

Defining Incident Management Processes for CSIRTs: A Work in Progress

Chris Alberts
Audrey Dorofee
Georgia Killcrece
Robin Ruefle
Mark Zajicek

October 2004

TECHNICAL REPORT
CMU/SEI-2004-TR-015
ESC-TR-2004-015



**Carnegie Mellon
Software Engineering Institute**

Pittsburgh, PA 15213-3890

Defining Incident Management Processes for CSIRTs: A Work in Progress

CMU/SEI-2004-TR-015

ESC-TR-2004-015

Chris Alberts
Audrey Dorofee
Georgia Killcrece
Robin Ruefle
Mark Zajicek

October 2004

Networked Systems Survivability Program

Unlimited distribution subject to the copyright.

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER



Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2004 Carnegie Mellon University.

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.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (<http://www.sei.cmu.edu/publications/pubweb.html>).

Table of Contents

Preface	ix
Acknowledgements	xiii
Abstract	xv
1 Introduction	1
1.1 Definition of a CSIRT	1
1.2 Definition of Incident Management	2
1.3 Who Performs Incident Management	5
1.4 A Process Model for Incident Management	8
1.5 Purpose of this Report	9
1.6 Scope of this Report	10
1.7 Intended Audience	11
1.8 Use of this Report	12
1.9 Structure of the Report	13
1.10 Reading and Navigating this Report	14
2 Incident Management Concepts and Processes	15
2.1 Incident Management Requirements	15
2.2 Overview of Incident Management Processes	16
2.3 Why We Chose These Processes	19
2.4 Incident Management Versus Security Management	23
2.5 Applying These Incident Management Concepts and Processes	27
2.6 Getting Started	34
2.7 Detailed Workflow Diagrams and Descriptions	35
3 Overview of Process Mapping	37
3.1 What is Process Mapping?	37
3.2 Applying Process Mapping to Incident Management	38
3.3 Our Process Mapping Methodology	39
3.3.1 Additional Uses for the Workflow Model	41

3.4	Guide to Reading the Incident Management Process Maps.....	42
3.4.1	Workflow Diagrams	42
3.4.2	Workflow Descriptions.....	46
4	Incident Management Process Workflows and Descriptions	49
4.1	Overview	49
4.2	Incident Management	50
4.2.1	PC: Prepare/Sustain/Improve Process (Prepare)	54
4.2.1.1	PC: Prepare/Sustain/Improve Workflow Diagram	56
4.2.1.2	PC: Prepare/Sustain/Improve Workflow Description	58
4.2.1.3	Handoff from Any Activity Inside or Outside CSIRT Process to PC: Prepare/Sustain/Improve	68
4.2.1.4	Handoff from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure	72
4.2.2	PI: Protect Infrastructure Process (Protect)	76
4.2.2.1	PI: Protect Infrastructure Workflow Diagram	80
4.2.2.2	PI: Protect Infrastructure Workflow Description.....	82
4.2.2.3	Handoff from Any Activity Inside or Outside CSIRT Process to PI: Protect Infrastructure	86
4.2.2.4	Handoff from PI: Protect Infrastructure to D: Detect Events	90
4.2.3	D: Detect Events Process	94
4.2.3.1	Reactive Detection	94
4.2.3.2	Proactive Detection	94
4.2.3.3	Detect Events Details	95
4.2.3.4	D: Detect Events Workflow Diagram.....	98
4.2.3.5	D: Detect Events Workflow Description	100
4.2.3.6	Handoff from Any Activity Inside or Outside of the Organization to D: Detect Events.....	104
4.2.3.7	Handoff from D: Detect Events to T: Triage Events	108
4.2.4	T: Triage Events (Triage) Process	112
4.2.4.1	T: Triage Events Workflow Diagram	116
4.2.4.2	T: Triage Events Workflow Description	118
4.2.4.3	Handoff from T: Triage Events to R: Respond	122
4.2.5	R: Respond Process	128
4.2.5.1	Technical Response	128
4.2.5.2	Management Response	129
4.2.5.3	Legal Response	129
4.2.5.4	Coordination of Response Activities	129
4.2.5.5	R: Respond Workflow Diagram	132
4.2.5.6	R: Respond Workflow Description	134
4.2.5.7	Handoff from R: Respond to PC: Prepare/Sustain/Improve	140

4.2.5.8	R1: Respond to Technical Issues Workflow Diagram.....	144
4.2.5.9	R2: Respond to Management Issues Workflow Diagram.....	148
4.2.5.10	R3: Respond to Legal Issues Workflow Diagram	152
5	Future Work.....	157
	Bibliography	161
Appendix A:	Context for Each of the Process Workflows.....	A-1
Appendix B:	Acronyms.....	B-1
Appendix C:	Glossary.....	C-1
Appendix D:	One-Page Versions of the Process Workflow Diagrams	D-1
	Incident Management Workflow Diagram	D-2
	PC: Prepare/Sustain/Improve Workflow Diagram	D-3
	PI: Protect Infrastructure Workflow Diagram.....	D-4
	D: Detect Events Workflow Diagram.....	D-5
	T: Triage Events Workflow Diagram	D-6
	R: Respond Workflow Diagram	D-7
	R1: Respond to Technical Issues Workflow Diagram	D-8
	R2: Respond to Management Issues Workflow Diagram.....	D-9
	R3: Respond to Legal Issues Workflow Diagram.....	D-10
Appendix E:	One-Page Versions of the Process Workflow Descriptions and Handoffs	E-1
	PC: Prepare/Sustain/Improve	E-2
	Handoff from Any Activity Inside or Outside CSIRT Process to PC: Prepare/Sustain/Improve	E-7
	Handoff from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure	E-8
	PI: Protect Infrastructure Workflow Description.....	E-9
	Handoff from Any Activity Inside or Outside CSIRT Process to PI: Protect Infrastructure	E-11
	Handoff from PI: Protect Infrastructure to D: Detect Events	E-12
	Detect Events Workflow Description.....	E-13
	Handoff from Any Activity Inside or Outside of the Organization to D: Detect Events	E-15
	Handoff from D: Detect Events to T: Triage Events	E-16
	T: Triage Events Workflow Description	E-17
	Handoff from T: Triage Events to R: Respond	E-19
	Respond Process Workflow Description	E-21
	Handoff from R: Respond to PC: Prepare/Sustain/ Improve	E-24

List of Figures

Figure 1:	CSIRT Services	4
Figure 2:	Defining the Relationship between Incident Response, Incident Handling, and Incident Management.....	4
Figure 3:	Five High-Level Incident Management Processes	18
Figure 4:	Operational Comparison of Incident and Security Management.....	25
Figure 5:	Overlap of Security Management, Incident Management, and IT Operations	26
Figure 6	Example of an Incident Management Workflow Diagram	27
Figure 7	Example of an Incident Management Workflow Description	28
Figure 8:	Example of Swim-Lane Chart Showing a Specific Instantiation of an Incident Handling Capability Derived from the Detect, Triage, and Respond Process Workflows and Descriptions	33
Figure 9:	Process Map Example	38
Figure 10:	Merging Workflows Triggering an Activity	45
Figure 11:	Separate Workflows Triggering an Activity	45
Figure 12:	Process Decisions and Alternative Branches	46
Figure 13:	Incident Management Workflow Diagram.....	52
Figure 14:	PC: Prepare/Sustain/Improve Workflow Diagram.....	56
Figure 15:	PI: Protect Infrastructure Workflow Diagram	80
Figure 16:	D: Detect Events Workflow Diagram	98
Figure 17:	T: Triage Events Workflow Diagram	116
Figure 18:	R: Respond Workflow Diagram	132
Figure 19:	R1: Respond to Technical Issues Workflow Diagram	146
Figure 20:	R2: Respond to Management Issues Workflow Diagram	150
Figure 21:	R3: Respond to Legal Issues Workflow Diagram	154

List of Tables

Table 1	Review of Incident Management Processes from Various Publications	20
Table 2:	Detect Events Workflow Example	32
Table 3:	Key to Incident Management Process Map Symbols	42
Table 4:	Incident Management Workflow Description Information Categories	47
Table 5:	Incident Management Handoff Description Information Categories	48
Table 6:	PC: Prepare/Sustain/Improve Workflow Description	58
Table 7:	Handoff from Any Activity Inside or Outside CSIRT Process to PC: Prepare/Sustain/Improve	70
Table 8:	Handoff from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure	74
Table 9:	PI: Protect Infrastructure Workflow Description	82
Table 10:	Handoff from Any Activity Inside or Outside CSIRT Process to PI: Protect Infrastructure	88
Table 11:	Handoff from PI: Protect Infrastructure to D: Detect Events	92
Table 12:	D: Detect Events Workflow Description	100
Table 13:	Handoff from Any Activity Inside or Outside of the Organization to D: Detect Events	106
Table 14:	Handoff from D: Detect Events to T: Triage Events	110
Table 15:	T: Triage Events Workflow Description	118
Table 16:	Handoff from T: Triage Events to R: Respond	124
Table 17:	R: Respond Workflow Description	134
Table 18:	Handoff from R: Respond to PC: Prepare/Sustain/Improve	142

Preface

Since its inception, the CERT[®] Coordination Center (CERT/CC) has had a strong commitment to transition lessons learned about computer security incident handling to the broader Internet community. The ultimate goal of this transition work is the development of a community equipped to recognize, prevent, and effectively respond to computer security risks and threats against their organizations.

To accomplish this transition work, our basic strategy is to develop a body of knowledge that will codify best practices for creating, managing, and sustaining incident management capabilities, based on the 15+ years of experience of the CERT/CC and other national and international teams. We then make this body of knowledge and resulting products available through publications, training courses, collaboration, and direct assistance to organizations interested in building or improving incident management capabilities.

Incident management capabilities¹ can take many forms—they can be an ad hoc group that is pulled together in a crisis, they can be a defined set of procedures that are followed when an incident occurs, or they can be a designated group of people assigned explicit responsibility for handling computer security incidents, generically called a computer security incident response team, or CSIRT.²

In our work, we are often asked for a “roadmap” or set of processes and templates that can be used by an organization to guide the development of their incident management capability. Correspondingly, we are asked how best to evaluate and measure the success and quality of an existing incident management capability. With these questions in mind and with an objective to continue our work in not only codifying best practices for incident management but also in building an overarching framework for our developing body of knowledge, we began a project to outline a methodology for planning, implementing, improving, and evaluating an incident management capability.

This methodology will identify key components for building consistent, reliable, and repeatable incident management processes. It will include a set of requirements or criteria against which an organization can benchmark its current incident management processes. The results

[®] CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

¹ The definition of incident management services and capabilities will be explored in the rest of this document.

² The term “CSIRT” is a generic, common name for an organization that provides services to a defined constituency to prevent and handle computer security incidents. Other synonymous names are discussed in Section 2.4, “What’s in a Name?” of the handbook *Organizational Models for CSIRTs* [Killcrece 03a].

of such benchmarking can help an organization identify gaps and problem areas in its incident prevention and handling processes and plans.

The incident management methodology, when completed, will provide a set of supporting materials that can be used by any organization. These materials will include various components and guides that will help organizations to

- identify the issues and decisions that must be addressed in planning a new or expanding an existing incident management capability
- identify the various components of such a capability and the various processes that should be in place to perform effective incident management
- benchmark the current state of incident management within the organization
- develop workflows and tasks that can be followed to implement or improve the capability

The methodology will also contain templates and checklists for developing incident management resources such as incident reporting forms, policies and procedures, incident tracking systems requirements, staff job descriptions, major event guidelines, and other similar items.

As a start on this work, we have chosen to focus on building one particular component. That component is the benchmarking mechanisms and corresponding set of criteria against which an organization can evaluate their incident management processes. To do this work, a multidisciplinary team was put together that includes members with expertise in the development and operation of incident management capabilities, along with members with expertise in risk analysis and process engineering and, more specifically, with expertise in implementing the Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE[®]) methodology at the Carnegie Mellon[®] Software Engineering Institute (SEISM).³

To begin this work, we defined and diagrammed the basic set of processes and activities involved with incident management functions in a series of incident management process maps. This report presents the initial incident management process definitions, workflow diagrams, and workflow descriptions and the corresponding process mapping methodology for our work to date. As we pursued this work, we realized that although we had started this project with the goal of developing an assessment mechanism, we had, in fact, created other useful products. The process maps themselves have provided us with a framework for incident management activities. There is still more work to be done to complete this framework as we

SM Operationally Critical Threat, Asset, and Vulnerability Evaluation and SEI are service marks of Carnegie Mellon University.

[®] OCTAVE and Carnegie Mellon are registered in the U.S. Patent & Trademark Office by Carnegie Mellon University.

SM Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

³ OCTAVE is a self-directed, risk-based strategic information security assessment and planning technique for security. You can read more about OCTAVE at <http://www.cert.org/octave/>.

continue to not only define these processes in more detail but also to develop methods to build, sustain, and evaluate the processes.

This report is not a “how to guide.” It is a vehicle to present the initial work we have done toward the development of the “roadmap” previously discussed. Organizations looking for assistance in building or improving incident management capabilities should look to our other publications and available training as outlined at our main web site for CSIRT Development, <http://www.cert.org/csirts/>.

Much of our initial work to date has been within the CSIRT community. This report, although applicable to broader incident management processes, is written from a CSIRT perspective. It approaches the process definitions from a CSIRT point of view, often addressing how CSIRTs fit into the overall incident management framework in their parent organizations or constituencies (hence the title of the report). However, many organizations do not have entities that they call CSIRTs; they have some other organizational structure or processes to handle this work. This report is still applicable to those organizations. It is useful outside of the CSIRT community and can be applied in any organization that deals with the handling and prevention of computer security incidents.

It should be pointed out, however, that the initial set of processes included here are more appropriate for internal incident management or CSIRT capabilities, as defined in our report *Organizational Models for CSIRTs* [Killcrece 03a]. An internal capability is one in which staff in the organization have been assigned the responsibility for incident management and the constituency being serviced is the parent organization. Future work will include applying these processes to other organizational models, particularly the Coordinating CSIRT model.

The terminology and variety of organizational structures involved in incident management today can often be confusing. We will begin to explore some of these areas of confusion in the material presented here. We will look at the difference and relationship between CSIRTs and incident management capabilities; we will also look at the difference and interrelationship between incident management and security management functions.

The material in this report is based on the information we have collected through our own experiences, discussions with and observations of other CSIRTs and incident management organizations, research and review of existing publications and literature related to CSIRTs and incident response, and from experience with risk analysis and process methodologies. We are very interested in receiving comments about this work from the CSIRT community. If you would like to share your opinions or suggest additions to this report, please contact us by sending email to csirt-info@cert.org.

Acknowledgements

We would like to express our deep appreciation to our colleagues in the incident handling and broader security community who reviewed this report. Their comments, recommendations, and suggestions helped us clarify our terms and ideas, think of our next steps, and make this report more useful and readable.

Julia Allen

Henk Bronk

Dawn Cappelli

Rich Caralli

Byron Collie

Katherine Fithen

Cristine Hoepers

Klaus-Peter Kossakowski

Barbara Laswell

Rob McMillan

Damon Morda

David Mundie

Sofie Nystrøm

Don Stikvoort

Moira West-Brown

Pamela Williams

We would like to acknowledge and thank the following people for their contributions, support, and assistance in the production of this document:

- Barbara Laswell – who not only provides us with the time, resources, and encouragement to continue our research and project work, but who also asks the hard questions that help us to crystallize our thoughts and ideas.
- William Wilson – for sharing with us the talents of Chris Alberts and Audrey Dorofee, the authors of *Managing Information Security Risks: The OCTAVE Approach*.
- Julia Allen and Rich Caralli – for sharing with us their ideas and evolving thoughts on enterprise security management and for exploring with us the synergies between that work and our CSIRT development work.

- Pamela Curtis – for guiding us through the technical editing process and formatting the first draft of our workflow diagrams and descriptions.
- Barbara White – for taking on the mammoth task of formatting all our workflow diagrams and workflow description tables so they could be included in this publication.
- David Biber – our graphics artist, who helped us visualize our ideas, concepts, and processes and who created additional graphics of the process map work for inclusion in slide sets and other publications.
- Kellie Short – for scheduling *all* those meetings.

All the other CSIRT organizations who shared their processes, problems, and experiences with us.

Abstract

This report presents a prototype best practice model for performing incident management processes and functions. It defines the model through five high-level incident management processes: Prepare/Sustain/Improve, Protect Infrastructure, Detect Events, Triage Events, and Respond. Workflow diagrams and descriptions are provided for each of these processes.

One advantage of the model is that it enables examination of incident management processes that cross organizational boundaries, both internally and externally. This can help computer security incident response teams (CSIRTs) improve their ability to collaborate with other business units and other organizations when responding to incidents.

Future reports will extend this work and provide additional guidance to enable both newly forming and existing incident management capabilities to use the model to determine where gaps exist in their current processes and to develop plans for creating, improving, or restructuring their incident management processes.

Although the processes defined in this document were originally developed for internal CSIRTs, the models and information presented here are applicable to other types of CSIRTs and other types of incident management and security management capabilities.

1 Introduction

This work showcases our evolving ideas and thoughts about computer security incident response team (CSIRT) processes and incident management processes in general. In our research and training work, we find incident management performed in a variety of ways across diverse organizations. This has led us to the conclusion that there is no standard method or staff structure that is used across all organizations for providing all the functions of incident management. If that is the case, then creating and applying standards and best practices in this domain can be complex and difficult.

To begin such a process, we believe you must look at all the processes involved in incident management and also ask the question, “Who performs incident management activities?” This question is one that is often asked by organizations as they plan their incident management strategy. They want to know what organizational units should be involved, what types of staff will be needed to perform the functions, and what types of skills that staff must have. They also want a way to identify which organizational units are already doing this type of work and to determine how to integrate new processes and functions with legacy ones. To do this, they want to be able to identify and understand the critical interfaces and interactions between different parts of the organization, different security functions, and the incident management process. These types of questions and needs have motivated us to pursue the work that we are documenting in this report.

To answer the question about who performs incident management activities, we must define what we mean by incident management and also what we mean by CSIRT, and how the two terms are related. We will begin with the definition of a CSIRT.

1.1 Definition of a CSIRT

We have defined a CSIRT in our previous publications and in our current training materials as “an organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents.” In our publication *Organizational Models for CSIRTs* [Killcrece 03a], we discuss various organizational models for structuring CSIRT functions. In that report, we make the following distinction between “security teams,” “internal” CSIRTs, and “coordinating CSIRTs”:

- In a security team, no group or section of the organization has been given the formal responsibility for incident handling activities. No CSIRT has been established; instead available personnel (usually system, network or security administrators) at the local or

division level handle security events on an ad hoc and sometimes isolated basis as part of their overall responsibilities or job assignments.

- An internal CSIRT is one in which a designated group of individuals has been assigned the responsibility for incident handling. This CSIRT is in the same organization as the constituency, such as a commercial CSIRT whose constituency is the commercial organization in which the CSIRT is located. For example, the Siemens commercial organization is the constituency for Siemens Computer Emergency Response Team (CERT).
- In the coordinating CSIRT model, the CSIRT coordinates and facilitates the handling of incidents, vulnerabilities, and general information across a variety of external and internal organizations, which can include other CSIRTs, vendor organizations, security experts, and even law enforcement agencies. The CERT/CC is a coordination center, as is the Australian Computer Emergency Response Team, AusCERT.

Although each of these organizational models provides some set of “CSIRT” services as outlined in our report *CSIRT Services* [Killcrece 02], the manner in which they provide the service and the extent of the service, or “level of service,” will be different. We have seen this work carried out through detailed sets of response plans; through emergency or crisis teams, which provide incident handling services in an ad hoc manner; through defined organizational entities such as a CSIRT, and through specialized CSIRT coordination centers, which focus on sharing information and guidance across a diverse constituency.

Because of the many ways that this work can be done, we do not believe the term “CSIRT,” as historically defined, encompasses all of these organizational structures. The “T” in “CSIRT” can often be too restrictive. We see the team as being more of a capability. Whatever structure the capability takes is suited to the needs of its “parent” or “hosting” organization or constituency. However, it should be reiterated, as described above, that a “security team” is not a CSIRT. It is another type of capability that may perform this work.

With these definitions in mind, our slightly modified definition of a CSIRT might now be “a capability or team that provides services and support to a defined constituency for preventing, handling and responding to computer security incidents.” Next, let’s move on to the definition of incident management.

1.2 Definition of Incident Management

Historically in the security and CSIRT community, people have used the term “incident response” and “incident handling” to define the activities of a CSIRT. We, however, consider those phrases also too narrow in scope to adequately address the wide range of work and services a CSIRT might provide. We believe that although incident handling and incident response are part of that work, the range of work that can be done actually encompasses a larger set of activities that we refer to as incident management. We see a defined difference in scope and leveling between the terms incident response, incident handling, and incident management.

We have outlined the differences between incident handling and incident response in our report *CSIRT Services* [Killcrece 02]. We define incident handling as one service that involves all the processes or tasks associated with “handling” events and incidents. Incident handling includes multiple functions:

- detecting and reporting – the ability to receive and review event information, incident reports, and alerts
- triage – the actions taken to categorize, prioritize, and assign events and incidents
- analysis – the attempt to determine what has happened, what impact, threat, or damage has resulted, and what recovery or mitigation steps should be followed. This can include characterizing new threats that may impact the infrastructure.
- incident response – the actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to prevent the incident from happening again

Incident response, as noted in the list above, is one process, the last step in incident handling. It is the process that encompasses the planning, coordination, and execution of any appropriate mitigation and recovery strategies and actions.

The term “incident management” expands the scope of this work to include the other services and functions that may be performed by CSIRTs, including vulnerability handling, artifact handling, security awareness training, and the other services outlined in the *CSIRT Services* list as shown in [Figure 1](#).⁴ The definition of this term to include this expanded set of services is important because incident management is not just responding to an incident when it happens. It also includes proactive activities that help prevent incidents by providing guidance against potential risks and threats, for example, identifying vulnerabilities in software that can be addressed before they are exploited. These proactive actions include training end users to understand the importance of computer security in their daily operations and to define what constitutes abnormal or malicious behavior, so that end users can identify and report this behavior when they see it.

⁴ Security Quality Management Services are services that augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT’s point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

Reactive Services 	Proactive Services 	Security Quality Management Services 
+ Alerts and Warnings + Incident Handling – Incident analysis – Incident response on site – Incident response support – Incident response coordination + Vulnerability Handling – Vulnerability analysis – Vulnerability response – Vulnerability response coordination + Artifact Handling – Artifact analysis – Artifact response – Artifact response coordination	○ Announcements ○ Technology Watch ○ Security Audit or Assessments ○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures ○ Development of Security Tools ○ Intrusion Detection Services ○ Security-Related Information Dissemination	✓ Risk Analysis ✓ Business Continuity & Disaster Recovery Planning ✓ Security Consulting ✓ Awareness Building ✓ Education/Training ✓ Product Evaluation or Certification

Figure 1: CSIRT Services

Figure 2 illustrates the relationship between the terms incident response, incident handling, and incident management. Incident response is one of the functions performed in incident handling; incident handling is one of the services provided as part of incident management.

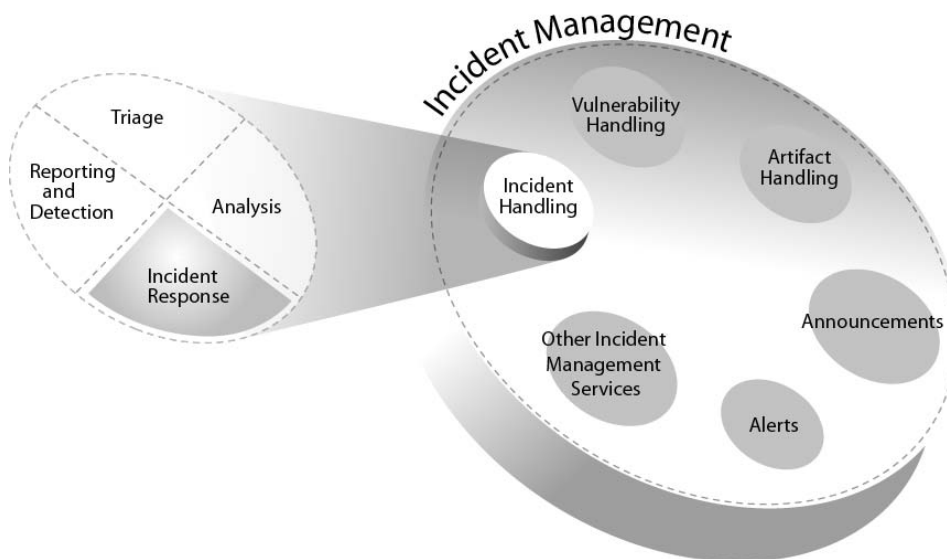


Figure 2: Defining the Relationship between Incident Response, Incident Handling, and Incident Management

As we have continued to work in the security community, we have seen that not all organizations provide the services we associate with CSIRT work or incident management activities through a defined CSIRT. In our experience and observations, we have seen these services distributed across various operational units of an organization. Sometimes these services are split between a CSIRT and these other divisions. This is especially true in organizations with

internal CSIRTs, such as commercial, military, government, and educational institutions. Coordinating CSIRTs are often an exception, as they usually do not spread their incident management functions across these types of business units.

Depending on the structure of an organization's incident management functions, we have seen certain functions performed by a CSIRT and in other cases these same functions performed by the information technology (IT) group, a security management team, or some other part of the organization. We have seen, for example,

- organizations in which all network monitoring and firewall and intrusion detection system (IDS) maintenance is handled by the IT or network group
- organizations in which CSIRT staff, rather than IT network operations staff, control perimeter defenses such as firewalls and intrusion detection systems and repair and recover affected systems
- organizations in which all security incidents are reported directly to the CSIRT
- organizations in which security incidents are reported to a centralized IT help desk and then passed to the CSIRT when appropriate
- situations in which no dedicated CSIRT has been established, but persons from IT and other business function units are given responsibilities to handle an incident once it is reported, based on the expertise required
- organizations in which CSIRTs perform vulnerability handling, scanning, and assessment services
- organizations in which vulnerability handling, scanning, and assessments are done by the audits, compliance, or IT operations group performing these functions

We have also seen various mixtures of services split between the CSIRT, IT and security groups, help desk, and compliance divisions. In many cases, some of these services are also outsourced to third-party managed security services providers (MSSPs).

1.3 Who Performs Incident Management

Let's return to the question of who performs incident management activities. Let us frame that question inside an organization with an internal CSIRT. Previously, many people might have answered, "The CSIRT, IT, or security group." However, more and more today we are seeing that effective incident management includes participants from outside these areas. For example, some very specific processes related to incident management may be performed by

- human resource personnel, who participate in removing an employee found to have been performing malicious computer activity
- legal council, who may provide interpretations of rules and regulations and their impact on implementing security policies and practices or who may be called in to help determine organizational liability when internal systems are being used for malicious activity

- the firewall manager, who puts certain filters in place to prevent a denial-of-service attack from continuing
- an outsourced service provider repairing systems that have been infected with a virus

We also often see the concept of extended teams, where a core group performs daily CSIRT activities and is supported, when necessary, by other experts throughout the organization or from external organizations. These people might have expertise in human resources (HR), media relations, specific activities performed by organizational business units, audits, risk management, network operations, or some other area. These types of staff members are often viewed as the “extended” team members of a CSIRT.

We also see that many factors not related to, or under the control of, a CSIRT affect and influence the level, type, and timing of the response. These factors might be in the form of business accessibility and operational requirements, financial decisions, laws and regulations, internal change management processes, or other organizational drivers. In light of these factors, our answer to the question “Who performs incident management activities?” has now evolved to the answer that incident management occurs across an organization, and in many cases includes participants from multiple divisions, who may have different organizational business drivers or missions. Balancing these different drivers effectively in the development and execution of an incident management plan can be challenging.

Enterprise security strategies are most effective when they strike a balance among competing and conflicting organizational drivers [Alberts 02]. An enterprise’s security strategy includes the set of security objectives, or mission, that must be achieved, as well as the organization’s approach for achieving that mission. In today’s competitive business environment, managers face many difficult decisions when developing security strategies. They are forced to balance the need for cost effectiveness with achieving the security mission of the enterprise. The path that is ultimately chosen might lead to centralizing some information-technology functions, including many security-related activities, across the enterprise to avoid costly duplication of tasks.

Management might also decide to outsource many information-technology and security-related activities, contracting with third parties to provide functions that are critical to achieving the enterprise’s security mission. This sets up an interesting situation. Managers are increasingly finding themselves in the unenviable position of having responsibility for ensuring the completion of an enterprise’s security mission while not directly controlling all of the resources needed to accomplish it. Contractual relationships, rather than direct reporting relationships within the enterprise’s management hierarchy, link participants from multiple enterprises, making the line of management authority unclear in many cases. Information sharing across business units or geographically distributed organizations can also complicate the matter.

Based on field work and observations done in the CSIRT community, we see that incident management is affected by these organizational tradeoffs. Balancing incident management

objectives and business drivers has led management in many organizations to distribute that capability across the organization and, in many cases, outsource much of it to third parties. This observation has led us to look at incident management outside of its historical boundaries within the IT department and instead see incident management as a distributed capability.

Just like a CSIRT, an incident management capability can take many forms. It can be a set of comprehensive policies and procedures for reporting, analyzing, and responding to computer security incidents. It can be an ad hoc or crisis team with defined roles and responsibilities that is called together when an incident occurs. It can also be an established or designated group that is given the responsibility for handling computer security events. So in essence, a CSIRT is one type of incident management capability.

To summarize this discussion of the definition of CSIRTs and incident management:

- Incident management activities and functions are broad based; they can involve not only incident analysis and response but also vulnerability analysis, artifact analysis, security awareness training, intrusion detection, public or technology monitoring, and other services as listed in the *CSIRT Services* list in [Figure 1](#).
- In a commercial, educational, military, or government organization where an internal CSIRT model would be appropriate, the incident management activities are often performed across multiple parts of the organization, including the CSIRT, as well as across multiple organizations such as contractors and service providers
- A capability for providing incident management activities can take many forms; a CSIRT is one type of incident management capability.

Often when working with a newly forming CSIRT or an organization wishing to develop an incident management capability, we discover that incident management activities are already occurring in other parts of the organization but are not identified as such. In our publications, we discuss how important it is to identify what types of incident management activities are already occurring and who is responsible for performing these activities as part of the planning and design process of building an incident management capability. This can help shape and structure the needed services. For example, if the organization is looking to create a CSIRT, then by looking at what is already in place, the interfaces required between the CSIRT and any other ongoing incident management activities can be defined. If certain functions are already being successfully handled, then perhaps the CSIRT can instead focus on those activities that are not being done. For example, if configuration management, vulnerability scanning, and security awareness training are already being done by an organization's IT department, it may be appropriate to have that area continue to provide those services while a new CSIRT concentrates on other services such as incident analysis, technology watch, vulnerability coordination, or incident response support and coordination.⁵ The main change to the existing functions is that there must be some type of formal mechanism or interface put into place and agreed to by both groups to provide coordination and information exchange between those IT (or other) functions and any new CSIRT functions.

⁵ For definitions of these services, see *CSIRT Services* at <http://www.cert.org/csirts/services.html>.

1.4 A Process Model for Incident Management

As mentioned previously, many organizations are looking for guidance on how to structure and implement an incident management capability. Also, many existing teams are looking for a way to benchmark their existing structure and processes and evaluate the quality of their incident management efforts. Our work and observations have led us to the belief that organizations need a framework or model for not only planning an incident management capability but for providing a methodology for evaluating its work. At the same time, the CSIRT community needs a framework to understand how CSIRTs fit into the overall incident management scheme and structure in their parent or hosting organizations.

This incident management model provides commonly accepted and practiced processes that outline the main functions and activities required for a successful incident management capability. The model, with the appropriate guidance and supporting materials, can then be used by an organization to plan a new capability, benchmark their current capability, and provide a path for improving and expanding the capability.

Because of the variety of ways that incident management capabilities can be organized and staffed, we decided that our starting point for building an incident management functional model would be to document all the processes we felt were involved in effective and efficient incident management work, regardless of where they occur across an organization or enterprise. An organization can then use this model to identify what processes they are already performing, what processes and process activities are being performed by whom (including third parties), what gaps exist in their processes, what part of the processes the CSIRT should perform, and then what interfaces need to exist between all the processes and all the participants.

The work documented in this report is an initial attempt to produce such a model or framework. This model documents a set of activities or functions that outline the various incident management processes. Based on this model, methodologies for assessing and benchmarking an organization's incident management processes can be developed. This methodology and resulting assessment instrument will enable organizations to evaluate their incident management performance and also allow CSIRTs to evaluate their performance for the following processes: Prepare/Sustain/Improve (Prepare), Protect Infrastructure (Protect), Detect Events (Detect), Triage Events (Triage), and Respond.⁶

It is important to point out that all parts of this model may not be applicable to all types of CSIRTs. For example, some of the processes may not be relevant to certain types of coordinating CSIRTs. But in general, we believe this model is a good starting point in providing a basic framework for most organizations.

⁶ The definition of these five processes and the rationale for choosing them is explained in Section 2.

In developing this model, we strived to ensure that our work complemented and conformed to other work going on in the CSIRT community and that it fit into a broader enterprise security framework.⁷ For example, we wanted to ensure that our work was also applicable to the Department of Defense (DoD) Computer Network Defense Service Provider (CNDSP) certification and accreditation metrics.

The U.S. Department of Defense established a directive and instruction whereby all DoD components are required to establish and provide for computer network defense services.⁸ The CNDSP is built around a framework of functional capabilities that are often provided by a CSIRT. Those CND services are defined as: Protect; Monitor, Analyze & Detect; and Respond. The primary goal of the DoD CNDSP certification and accreditation (C&A) process is to enhance the survivability of DoD information systems and computer networks through a standardized evaluation process. A secondary goal is to ensure a higher quality of protection through increased maturity and understanding of the services provided by the CNDSP. The DoD's evaluation process is used as a measurement of mission effectiveness, operational performance, and functional maturity through a number of critical success factors.

The functional model that we are presenting in this publication does not match process name to process name with the CNDSP metrics, but all the processes and functions outlined in the CNDSP metrics do match to a process area within our incident management process workflows.⁹

1.5 Purpose of this Report

This report documents the initial work done to date to define incident management processes. It is a first step in providing the framework for creating and operating incident management capabilities, including CSIRTs. As such it can be used as a foundational publication and reference to detail a best practice model for incident management processes.

One of the main purposes of the report is to outline the basic concepts and methodology behind the use of process mapping for defining incident management processes. Another purpose is to define the Prepare, Protect, Detect, Triage, and Respond processes at a detailed level in process workflows and corresponding descriptions and handoffs. The report also looks at the relationship CSIRTs have to the overall incident management functions, hence the name, *Defining Incident Management Processes for CSIRTs*. You will find that the majority of the details of the processes in the workflows and descriptions are from the CSIRT point of view.

⁷ Work is currently ongoing within the SEI's Networked Systems Survivability program to develop a framework for Enterprise Security Management (ESM). For more information on the evolving ESM work, see: http://www.cert.org/nav/index_green.html.

⁸ As outlined in DoD Directive O-8530.1, "Computer Network Defense," and DoD Instruction O-8530.2, "Support to Computer Network Defense."

⁹ The areas covered by the CNDSP C&A metrics are: Protection; Detection; Response; and CND Sustainment Functions.

This report documents and defines the “what” and “who” of incident management processes. It does not define the “how.” In that regard, this report is not a how-to guide or a step-by-step process for implementing, sustaining, or improving incident management processes and capabilities. Some of the “how to” information will come from additional materials that have yet to be developed and other information is already available in some of our existing publications. References to those publications are indicated where appropriate.

The greater part of the ideas and concepts presented here are contained in the process workflows and descriptions. This can make reading and interpreting the model quite difficult for the average reader because of the amount of information presented. This is another reason that additional supporting materials will need to be developed.

This report provides the building blocks for future work that will provide further definition and description of the model. Future work will also provide guidance and materials for applying the concepts detailed here. With these additional materials, organizations will be able to use the model as a framework for structuring initial incident management capabilities and sustaining and improving existing ones. Additional materials based on this work will provide a capacity and methodology for benchmarking existing incident management processes in an organization and identifying and prioritizing gaps and process work improvements.

1.6 Scope of this Report

This publication presents a process model for incident management functions. The model is a prototype, and it will continue to evolve. In fact, in future versions and supporting materials the layout of the information presented may be revised or modified, since we will continue to explore the best way to provide this content in a user-friendly manner.

The process workflow diagrams and descriptions included here represent the first level of processes for all main incident management functions. They also include various levels of subprocesses for some of these main functions.¹⁰

The first or top-level workflow diagram for the main incident management process areas includes

- Prepare/Sustain/Improve (Prepare)
- Protect Infrastructure (Protect)
- Detect Events (Detect)
- Triage Events (Triage)
- Respond (Respond)

¹⁰ The word “level” in this context relates to how far down a process has been detailed. At the top level, the main processes are shown. At the next level down, each process box activity is expanded into its main subprocesses, at the next level down, each subprocess box is broken down into its various subprocesses.

The scope of this report is the draft set of process flows that exist at the time of this report's publication. Future publications will document the final version of this work and all the corresponding subprocess mappings.

It must also be pointed out that in documenting the processes we focused on what were considered common best practices. We did not include exceptions or customized approaches or processes. Our intent is to provide this best practice set of materials to organizations in a way that they can modify or adapt to fit any specific needs, requirements, or considerations they may have.

The majority of the discussion throughout the rest of the report will be primarily geared to organizations in the commercial, educational, military, or government areas where an internal CSIRT model would be most appropriate. Not all of the processes detailed here may be applicable to other CSIRT models, particularly coordinating CSIRTs. However, many of the processes will indeed be appropriate. Future work may take a separate look at the set of processes for performing incident management activities in a coordinating CSIRT.

1.7 Intended Audience

The primary audience for this report is individuals tasked with creating, operating, benchmarking, or evaluating a CSIRT or incident management capability, including

- CSIRT development project team members
- CSIRT managers
- CSIRT staff
- internal, external, and third-party evaluators
- MSSPs
- regional or national initiatives seeking to build CSIRTs or incident management capabilities
- incident handling communities such as the Forum for Incident Response and Security Teams (FIRST)

Although the processes here are more aligned with functions performed by an internal CSIRT, the concepts, ideas, and framework defined will be applicable and of interest to all types of CSIRTs and incident management capabilities.

This report will also be of benefit to others who may want to gain a better understanding of incident management and CSIRT processes, functions, and interactions, including

- chief information officers (CIOs)
- chief security officers (CSOs)
- other C-level managers such as chief financial officers (CFOs) and chief risk officers (CROs)
- business function managers

This report can also be a useful reference for higher management levels, all CSIRT staff, and other individuals who interact with CSIRTs and who would benefit from an awareness of the interorganizational issues and processes related to incident management. These include

- members of the CSIRT constituency
- representatives from law enforcement
- representatives from media relations
- representatives from legal counsel
- others parts of the parent organization, including the IT department, physical security area, human resources, audits and compliance, risk management, and any investigative groups

Again it should be pointed out that because of the detailed nature of this report, some of these audiences may want to read only part of the report, as outlined in Section 1.10, “Reading and Navigating this Report.” Others may want to wait until additional materials, packaged in a more user-friendly manner, are available. These additional materials will explain how to apply the incident management process map model and corresponding framework.

1.8 Use of this Report

This report, *Defining Incident Management Processes for CSIRTs*, was developed for use as both a stand-alone document and as a companion document to these other CSIRT publications from the SEI:

- *Handbook for CSIRTs*, CMU/SEI-2003-HB-002 [West-Brown 03]
- *Organizational Models for CSIRTs*, CMU/SEI-2003-HB-001 [Killcrece 03a]
- *State of the Practice of CSIRTs*, CMU/SEI-2003-TR-001 [Killcrece 03b]

The framework that will result from this report and future supplemental materials can be used to meet a number of goals and objectives as a

- guide for mapping your own organizational incident management processes and work-flows
- best practice model for benchmarking your own incident management capability or identifying gaps in an existing capability
- guide for identifying all the incident management processes that occur outside the CSIRT and require coordination with any of your existing CSIRT activities
- map or reference in planning what specific processes will be done by which part of your organization

This document can be used in conjunction with the other three reports mentioned above to provide guidance for teams on the options for organizing and operating a CSIRT. It can be used at the early stage of CSIRT development to provide ideas for organizational structures

and service offerings. It can also be used to help gather management buy-in and support and, after support has been obtained, to strategically plan and develop a capability.

Use the *Handbook for CSIRTs* for specific in-depth guidance for issues relating to the establishment and operation of a CSIRT. Use *Organizational Models for CSIRTs* to understand the specific issues to be addressed when determining the model for your CSIRT. Use the *State of the Practice of CSIRTs* report for the historical background on the development of CSIRTs, for examples of what other teams are doing, and as a reference to existing articles, publications, books, laws, and training related to CSIRTs and incident management. Use the *Defining Incident Management Processes for CSIRTs* report to provide an overview of the processes and functions and supporting people, technology, and procedures that are involved in incident management.

Other SEI publications that this report may be used in conjunction with include some Security Improvement Modules available from the CERT/CC web site,¹¹ including

- *Responding to Intrusions*
<http://www.cert.org/security-improvement/modules/m06.html>
- *Detecting Signs of Intrusion*
<http://www.cert.org/security-improvement/modules/m09.html>
- *Outsourcing Managed Security Services*
<http://www.cert.org/security-improvement/modules/omss/index.html>

1.9 Structure of the Report

The remainder of this report will detail our progress to date in developing incident management process maps for CSIRTs.

Section 2, “Incident Management Concepts and Processes,” will expand on the ideas and concepts of the five top-level incident management processes. This discussion will include a rationale for including the processes we did, a discussion of incident management as it relates to the domain of security management, and an example of how we see this work being used in an organization.

Section 3, “Overview of Process Mapping,” will provide an explanation of what process mapping is and how it can be applied to incident management. This section also contains a description of the data elements or components of the process workflows and descriptions, along with a legend for reading and understanding the process workflow diagram symbols and drawings.

Section 4, “Incident Management Process Workflows and Descriptions,” contains the main content of this report. This section includes the process workflow diagrams and supporting descriptions in the form of process data and handoff templates. Preceding each workflow will

¹¹ Available at <http://www.cert.org/security-improvement/#modules>.

be a brief description of the process depicted. Future work and publications will provide a more in-depth discussion of each process and its corresponding subprocesses. This initial work presents the workflow diagrams and descriptions as is, with only a brief discussion of the issues involved with each process.

Section 5, “Future Work,” describes our next steps and the tasks we see that need to be done to complete this work. It also describes the types of supporting materials we feel will be needed to allow organizations to easily apply the concepts contained in this report.

There are four appendices included as part of this report:

- Appendix A – includes additional notes, called context, for each of the process workflows. This was information that was not included in the workflow descriptions but that helps explain our ideas and intent. This type of information will be used to expand the process workflows and descriptions in future work.
- Appendix B – lists acronyms used in this report
- Appendix C – includes a glossary of terms used in this technical report
- Appendix D – includes one-page versions of the process workflow diagrams that may be easier to handle for some readers, rather than the two-page versions included in the main content of the report
- Appendix E – includes one-page versions of the process workflow descriptions and handoffs

1.10 Reading and Navigating this Report

Because the main content of this report is contained in the process workflows and descriptions in Section 4, the presentation of this material can be daunting to review. As a reader interested in the incident management domain, you may find the following guidance helpful in deciding how to read and navigate this report.

If you want a simple overview of the basic concepts presented in this report, read Section 1, “Introduction,” and Section 2, “Incident Management Concepts and Processes.” Section 1 provides an overview of where the concept of this project came from and the overall framework that we are trying to build. It also includes a discussion of the definitions of CSIRT and incident management and how they relate to each other. Section 2 provides a more detailed discussion of the place that incident management holds in the security management arena, and discusses the five high-level processes of incident management and how they relate to one another. This section also discusses how this set of processes can be used to help create, sustain, and evaluate an incident management capability.

If you want to understand the five processes in more detail, read (along with Sections 1 and 2) Section 3, which provides guidance for reading and understanding the process workflows and descriptions, and Section 4, which contains the workflow processes and descriptions. For some basic context, also read Appendix A.

2 Incident Management Concepts and Processes

2.1 Incident Management Requirements

In our CSIRT-related publications and courses,¹² we describe the need for organizations to have a multilayered approach to secure and protect their critical assets and infrastructures. This multilayered strategy requires that not only technical but also organizational approaches be in place to manage computer security incidents as part of the goal of achieving an enterprise's business objectives in the face of risks and attacks. Organizations today want to not just survive attacks but to be resilient to whatever malicious activity may occur.¹³

Through our research in the area of incident management, we continue to evolve our understanding of its processes. In the early history of incident management, where most capabilities were established CSIRTs, the processes and functions performed by team members were primarily reactive in nature; actions were taken to resolve or mitigate an incident when it occurred.¹⁴ As teams increased their capability and scope, they began to expand their activities to include more proactive efforts. These efforts included looking for ways to

- prevent incidents and attacks from happening in the first place by securing and hardening their infrastructure
- training and educating staff and users on security issues and response strategies
- actively monitoring and testing their infrastructure for weaknesses and vulnerabilities
- sharing data where and when appropriate with other teams

As organizations become more complex and incident management capabilities such as CSIRTs become more integrated into organizational business functions, it is clear that incident management is not just the application of technology to resolve computer security events. It is also the development of a plan of action, a set of processes that are consistent, repeatable, of high quality, measurable, and understood within the constituency. To be successful this plan should

¹² These publications and courses are documented at <http://www.cert.org/csirts/>.

¹³ Resiliency in this context means the “the ability of the organization to withstand systemic discontinuities and adapt to new risk environments” [Starr 03].

¹⁴ For historical background on the development of CSIRTs, see the *State of the Practice of CSIRTs*, Section 2.3, “History and Development of CSIRT Capabilities.” This report is available at <http://www.cert.org/archive/pdf/03tr001.pdf>.

- integrate into the existing processes and organizational structures so that it enables rather than hinders critical business functions
- strengthen and improve the capability of the constituency to effectively manage security events and thereby keep intact the availability, integrity, and confidentiality of an organization's systems and critical assets, where required
- support, complement, and link to any existing business continuity or disaster recovery plans where and when appropriate
- support, complement, and provide input into existing business and IT policies that impact the security of an organization's infrastructure
- implement a command and control structure, clearly defining responsibilities and accountability for decisions and actions
- be part of an overall strategy to protect and secure critical business functions and assets
- include the establishment of processes for
 - notification and communication
 - analysis and response
 - collaboration and coordination
 - maintenance and tracking of records

2.2 Overview of Incident Management Processes

To implement such a plan, we believe organizations need to have quality strategies and processes in place to not only handle incidents that do occur but to prevent incidents from occurring or re-occurring. These include processes to

- plan and implement a computer security incident management capability
- secure and harden the enterprise infrastructure to help prevent incidents from occurring or to mitigate an ongoing incident
- detect, triage,¹⁵ and respond to incidents and events when they occur

These basic processes form the high-level processes in our incident management model documented in this report. We have defined these processes as follows:

- Prepare/Sustain/Improve (Prepare), which includes subprocesses to
 - plan and implement an initial incident management or CSIRT capability
 - sustain that capability
 - improve an existing capability through lessons learned and evaluation and assessment activities
 - perform a postmortem review of incident management actions when necessary
 - pass off infrastructure process improvements from the postmortem to the Protect process

¹⁵ Triage in incident management terms entails categorizing, correlating, prioritizing, and assigning computer security events and incidents.

- Protect Infrastructure (Protect), which includes subprocesses to
 - implement changes to the computing infrastructure to stop or mitigate an ongoing incident or to stop or mitigate the potential exploitation of a vulnerability in the hardware or software infrastructure
 - implement infrastructure protection improvements resulting from postmortem reviews or other process improvement mechanisms
 - evaluate the computing infrastructure by performing such tasks as proactive scanning and network monitoring, and by performing security and risk evaluations
 - pass off to the Detect process any information about ongoing incidents, discovered vulnerabilities, or other security-related events that were uncovered during the evaluation
- Detect Events (Detect), which includes subprocesses to
 - notice events and report those events¹⁶
 - receive the reports of events
 - proactively monitor indicators such as network monitoring, IDS, or technology watch functions
 - analyze the indicators being monitored (to determine any notable activity that might suggest malicious behavior or identify risk and threats to the enterprise infrastructure)
 - forward any suspicious or notable event information to the Triage process
 - reassign events to areas outside of the incident management process if applicable
 - close any events that are not forwarded to the triage process
- Triage Events (Triage), which includes subprocesses to
 - categorize and correlate events
 - prioritize events
 - assign events for handling or response
 - pass on relevant data and information to the Respond process
 - reassign events to areas outside of the incident management process if applicable
 - close any events that are not forwarded to the Respond process or reassigned to other areas
- Respond (Respond), which includes subprocesses to
 - analyze the event
 - plan a response strategy
 - coordinate and provide technical, management, and legal response, which can involve actions to contain, resolve, or mitigate incidents and actions to repair and recover affected systems
 - communicate with external parties

¹⁶ We have chosen to use the word “events” to describe the information and activity that are detected and triaged. We only use the word “incident” once it has been determined that a true computer security incident has occurred. Although this may happen in the Detect or Triage processes, it is often not until the Respond process that something is validated as a true incident. That is why the process names for “Detect Events” and “Triage Events” differ from “Respond.”

- reassign events to areas outside of the incident management process if applicable
- close response
- pass lessons learned and incident data to the Prepare function for use in a postmortem review

Figure 3 illustrates the relationship of these processes.

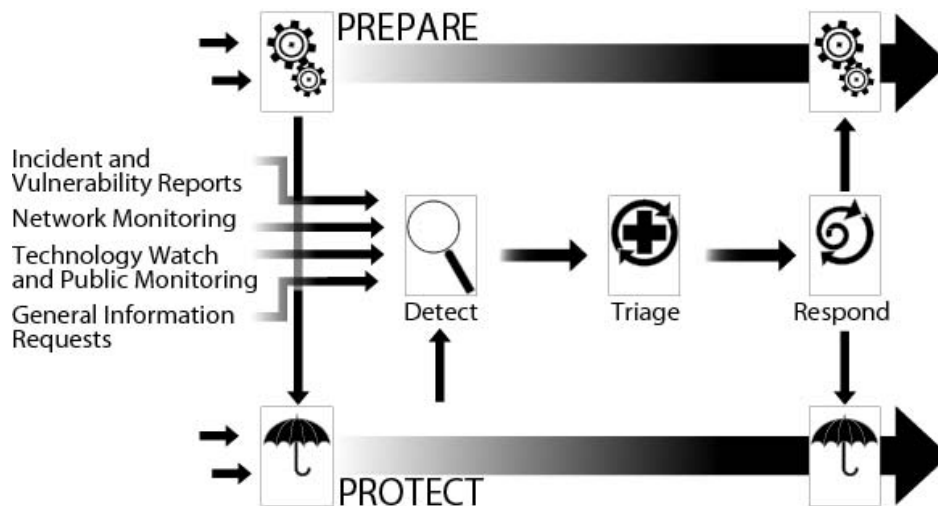


Figure 3: Five High-Level Incident Management Processes

The above diagram can be explained as follows:

- This diagram shows the Prepare and Protect processes as continuous ongoing processes. This is signified by the arrows going across the diagram and by having the icons for each at the beginning and end of the arrows. These processes involve putting into place all the necessary staff, technology, infrastructure, policies, and procedures for incident management activities to occur in a timely, coordinated, and effective manner. The use of the arrows surrounding the Detect, Triage, and Respond processes show that Prepare and Protect support and enable the other processes.
- The small arrows coming into the Prepare and Protect process indicate requirements, policies, or rules that will govern the structure and function of these processes. These arrows also indicate incoming process improvement recommendations.
- The line that goes from the Prepare to the Protect process signifies a handoff between these two processes. In this case, the information passed is process improvement recommendations for changes in the computing infrastructure that result from a postmortem review done in the Prepare process. These changes in the infrastructure, if implemented, will help harden and secure the infrastructure to help prevent similar incidents from happening and the same incident from re-occurring.
- The Detect, Triage, and Respond processes are shown in sequence as information coming into the Detect process is evaluated to determine if it is notable and needs to be passed on to the Triage process for further analysis and assessment. If in the Triage process the received information (whether it is an incident report, a vulnerability report, a general in-

formation request, or a suspicious event) requires a response, it is passed on to the Respond process.

- The arrow going from Protect to Detect indicates the passage of any incident or vulnerability reports that may result from infrastructure evaluations. It is possible that during an evaluation or assessment, a vulnerability, ongoing incident, or remnant of a past incident is discovered. This information needs to be passed to the Detect process.
- The arrows going from the Respond process to the Prepare process signify the handoff of process improvements and corresponding incident data or respond actions and decisions where appropriate. The handoff from Respond to Prepare passes this information to the postmortem review subprocess within the Prepare process.

2.3 Why We Chose These Processes

The above processes were chosen as our initial high-level model based on our own experience and observations in working with various CSIRTs and based on reviews of current incident management literature.

One of the main principles of our incident management process map work is to show that incident management is an enterprise-wide, distributed capability. In our experience we have seen a number of problems resulting in ineffective implementations of incident management capabilities and processes. These include capabilities

- that do not support the organizational mission, goals, or business drivers
- with no corresponding policies or procedures to govern their actions
- with no defined processes, accountability, or roles and responsibilities in place
- that provide redundant or duplicate services
- that were established without being integrated into existing processes, resulting in a lack of communication, coordination, and data sharing where needed

These common problems helped guide us to expand incident management capabilities to include strong processes for integration of the capability across the enterprise. We also looked at what others in the incident management field were saying about the processes that make up incident management.

In recent years a number of books and articles have been written about incident management and incident response activities. In 2002 and 2003, we did a literature review of a large number of these publications. In our report *The State of the Practice of CSIRTs* [Killcrece 03b] we detailed, in Appendix B, “Comparison of Incident Response Steps and Processes,” the basic set of activities or tasks each author outlined as a methodology for performing incident response. Some extracts from that literature review are shown in [Table 1](#).

Table 1 *Review of Incident Management Processes from Various Publications*

Title of Publication	Author(s)	Steps or Processes
<i>Computer Forensics, Incident Response Essentials</i>	Warren G. Kruse II and Jay G. Heiser [Kruse 02]	Discovery and Report Incident Confirmation Investigation Recovery Lessons Learned/Recommendations
<i>Incident Response</i>	Kenneth R. van Wyk and Richard Forno [van Wyk 01]	Identification Coordination Mitigation Investigation Education
<i>Incident Response: A Strategic Guide to Handling System and Network Security Breaches</i>	Eugene Schultz and Russell Shumway [Schultz 02]	Preparation Detection Containment Eradication Recovery Follow-up
<i>Incident Response: Investigating Computer Crime</i>	Kevin Mandia and Chris Prosise [Mandia 01]	Pre-incident preparation Detection Initial response Response strategy formulation Duplication (forensic backup) Investigation Security measure implementation Network monitoring Recovery Reporting Follow-up
<i>Advance Planning for Incident Response and Forensics</i>	Symantec Corp. [Symantec 01]	Identify vital assets Hire experienced staff Secure individual hosts Secure your network Monitor devices Establish a response strategy Establish policies and procedures
<i>Computer Security Incident Handling Step by Step</i>	The SANS Institute [SANS 03]	Preparation Identification Containment Eradication Recovery Follow-up
<i>Security Architecture and Incident Management for E-business</i>	Internet Security Systems - Marc S. Sokol and David A. Curry [Sokol 00]	Incident preparedness Alerting Report and notification Preliminary investigation Decision and resource allocation Response Recovery Lessons learned

Title of Publication	Author(s)	Steps or Processes
<i>Computer Security Incident Response Planning</i>	Internet Security Systems [ISS 01]	Alert Triage Response Recovery Maintenance
<i>Responding to Computer Security Incidents: Guidelines for Incident Handling</i>	E. Eugene Schultz, Jr., David S. Brown, Thomas A. Longstaff [Schultz 90]	Protection Identification Containment Eradication Recovery Follow-up
<i>The Methodology of Incident Handling</i>	Matthew McGlashan, Australian Computer Emergency Response Team ¹⁷	Identify scope and assess damage Communicate Collect and protect Apply short-term solutions Eliminate intruder access Return to normal operations Identify and implement lessons learned
<i>State of Vermont Incident Handling Procedure</i>	State of Vermont [Vermont 01]	Protect Identify Contain Eradicate Recover Follow-up
<i>RFC 2196 Site Security Handbook</i>	Barbara Fraser, Editor [Fraser 97]	Notification and exchange of information Protect evidence and activity logs Containment Eradication Recovery Follow-up
<i>Computer Incident Response Guidebook</i>	Naval Command, Control and Ocean Surveillance Center [Navy 96]	Preparation Identification Containment Eradication Recovery Follow-up

Although very few authors use the same terminology, it is apparent that a similar set of tasks are discussed. Most often those tasks include detecting and reporting events and incidents, containing and resolving incidents, and recovery of systems. Other steps that relate to these functions include identification, containment, eradication, investigation, and notification. At the top level of our process maps, the detect and reporting activities mentioned by these authors correspond to our Detect process. All the other tasks, such as identification, containment, eradication, investigation, notification, and recovery, are contained within our set of

¹⁷ McGlashan, Matthew. "The Methodology of Incident Handling." *InfoSecurity 2001 Conference Program*. Malaysian National Computer Confederation, 2001.

processes called Respond. These are generally the type of activities one thinks of when defining incident response and incident handling tasks.¹⁸

Some authors include a range of other tasks that we feel must be addressed. Schultz et al. and the State of Vermont, for example, include the process “protect.” SANS, Sokol et al., and the U.S. Navy include the process “prepare.” We too believe these processes should be included in any methodology or framework for modeling incident management work. Previously in our courses, we usually included both of these processes in one process called Prepare, but in our process mapping work, we have broken them out as separate processes: PC: Prepare/Sustain/Improve and PI: Protect Infrastructure.

Effective response starts long before an organization actually has an incident to handle. Being able to respond in an effective manner requires that an organization have an established response plan in place that is integrated into the enterprise strategy for protecting and securing critical business systems and assets. It requires the establishment of processes for notification, communication, collaboration, and coordination, along with processes for receiving, documenting, analyzing, and responding to computer security incidents. The appropriate communication channels must be established, incident handling tools must be obtained or developed and then tested, staff must be trained, and a secure infrastructure must be in place, along with processes and mechanisms for disseminating information and guidelines and processes for reporting incidents.

Because of the need to have preparations in place so that response actions can occur effectively, our definition of incident management has been broadened to include the processes for establishing and sustaining a CSIRT or incident management capability. This is the process we refer to as Prepare. This process provides for the establishment of incident management plans, the identification and training of staff to participate in these activities, and at a higher level the defining of a team or capability’s mission and services. It also includes those processes to actually build, staff, and equip the CSIRT or incident management capability. If this step is not done correctly and if the capability does not have the expertise, tools, resources, and supporting policies and procedures in place, the response may be delayed or fail altogether. We have also included processes related to the evaluation of the incident management capability to determine how well it is meeting its mission and performing its functions. Along with that we’ve included the process for performing a postmortem review after an incident has occurred. Out of the evaluation and the postmortem will come various process improvements that may impact this Prepare process by recommending changes to policies, procedures, workflows, staffing levels, communications channels, and equipment or infrastructure requirements.

In light of complex attacks that can occur in a matter of minutes and the need for an organization to implement best security practices for configuring and hardening systems, we believe that establishing a defense-in-depth protection scheme for an organization’s infrastructure is also an important proactive and preventative strategy that relates directly to incident man-

¹⁸ Although “identification” can also occur in the Triage process.

agement activities. Often the only way to combat malicious activity is to prevent its initial entry into an enterprise. As a result of lessons learned during an incident, organizations often have to make organizational and technical changes to their infrastructure to prevent attacks from successfully happening again. Other proactive protection activities, such as vulnerability scanning, penetration testing, network monitoring, public monitoring, and risk evaluation or assessment, relate directly to methods of detecting and reporting events, incidents, vulnerabilities, and other computer security related information. Protecting an organization's infrastructure becomes a strategy for not only preventing attacks but also for identifying, containing, and stopping malicious activity in a timely manner. The infrastructure defenses are one type of tool used to manage incident activity. Because of this multilevel connection between the protection of an organization's infrastructure and the resolution of incidents, we believe that the Protect function must be included as one of the activities in the broader scope of incident management.

One other process that we include and that is also mentioned by ISS [ISS 01] as being an important part of the incident management process is Triage. Some people see triage as being the first step in response (the Respond process), a method for performing an initial analysis of a report to determine what has happened and what the impact is, while also categorizing and prioritizing an event or incident. We have set Triage as a process separate from Respond, due to the fact that how triage is performed will depend heavily on who performs it. Triage can be handled in multiple ways. It can be done by an incident handler as part of the initial analysis of an event; it can be done by a help desk that handles general computer problems for an organization; it can be outsourced to a managed security service provider; or it can be handled by specific positions in an organization, such as an information security officer. When handled outside of a CSIRT, there are risks to the transfer of information from the triage role to the incident handling role that can occur. Triage is also important as a location where categorization and correlation of events can occur. As such, it is on the critical path to response and should be accorded an appropriate set of resources. For these many reasons, we believe Triage should stand alone as a process.

Depending on the type, structure, and mission of an incident management capability, some of these processes may not apply. For example, a coordinating CSIRT might not perform any type of Protect or even Detect functions. Various types of incident management capabilities may actually only focus on one part of these processes. In future reports, we hope to address some of these different types of capabilities and how their process workflows differ from the ones described here.

2.4 Incident Management Versus Security Management

Precisely defining incident management is difficult; the words mean different things to different communities. For example, in the Information Technology Infrastructure Library (ITIL), a best practice series of books providing guidance on developing and implementing

quality information technology (IT) services, “incident management” refers to the handling of any type of service disruption or interruption [OGC 03]. The scope of our definition of incident management¹⁹ is preventing and handling computer security incidents. This includes identifying and minimizing the impact of technical vulnerabilities in software or hardware that may expose computing infrastructures to attacks or compromise, thereby causing incidents. Part of the inherent difficulty in defining the term “incident management” is defining the term “incident,” which is often derived based on organizational requirements and specifications. For this report, the definition of a computer security incident is taken from RFC 2350: “any adverse event which compromises some aspect of computer or network security” [Brownlee 98]. Our definition of an “event” is taken from RFC 2828: “an occurrence in a system that is relevant to the security of the system...The term includes both events that are security incidents and those that are not” [Shirey 00]. We use the word “event” to describe activity that is computer security related but that has not yet been identified as an incident or a vulnerability.

The scope of incident management for this report is *computer security* incident management (shortened to “incident management”). Often we are asked to distinguish between security management and incident management, especially when our incident management scope includes processes for protecting infrastructures and detecting events using network monitoring and IDS. The boundary between the two is open to interpretation and can be confusing. The dividing line often depends on the structure of an organization’s security or incident management capabilities.

In our model and in keeping with other work within the SEI in the area of enterprise security management,²⁰ we view incident management as an integral component of security management. Security management encompasses all of the tasks and actions necessary to secure and protect an organization’s critical assets, and this is much broader in scope than incident management. It involves aligning and prioritizing security actions based on the organization’s mission and objectives and assessing security risks to achieving such objectives. It involves establishing, configuring, operating, and maintaining the organization’s computing infrastructure in a secure manner and as a continuous process. Security management includes risk management, audit, access control, account management, asset management, physical security, security policies, configuration management, change and patch management, disaster recovery, and business continuity. Security management applies risk management approaches to help choose the most effective course of action. Incident management may use many of these capabilities in the performance of its objectives, such as patch management, configuration management, or security policies. But incident management is not responsible for establishing and maintaining these capabilities. Incident management is a component of security

¹⁹ See the discussion of the definition of incident management in Section 1, “Introduction,” for more information.

²⁰ For more information on these initiatives, please see *The Challenges of Security Management*, available at <http://www.cert.org/archive/pdf/ESMchallenges.pdf>, and *Building a Practical Framework for Enterprise Security Management*, available at http://www.cert.org/archive/pdf/secureit_esm_allen_may0304.pdf.

management. Security management provides a framework within which the execution of incident management processes occurs.

If we examine the five high-level incident management processes, we see that some of them intersect and overlap with security management in some fashion. [Figure 4](#) shows how incident management processes fit into the scope of security management.

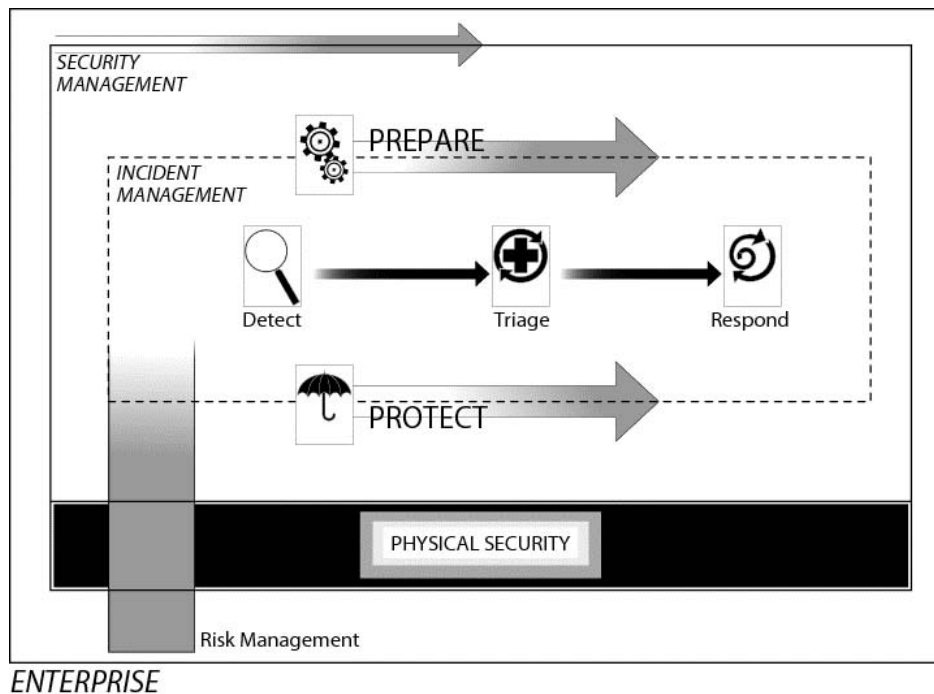


Figure 4: Operational Comparison of Incident and Security Management

In [Figure 4](#), the arrows show that Prepare and Protect processes are included in both incident management and security management. The incident management Protect process addresses infrastructure changes in response to current computer security threats, while the security management Protect process addresses a wider range of protection activities, including those necessary to configure and secure a computing infrastructure and maintain and monitor those configurations. The Detect, Triage, and Respond processes are totally within the scope of incident management, with regards to the treatment of computer security events and incidents.

Security management exercises physical security and risk management capabilities to protect critical assets at the enterprise level. Risk management also informs incident management by balancing incident response actions with business drivers and organizational mission. Applying risk management during incident response helps determine what actions should be taken based on the criticality of the asset (information, system, network) that is under threat of attack. Not all assets are equivalent and not all response efforts are cost effective in light of the organizational mission. For example, if a manufacturing organization finds that its computer infrastructure is propagating a harmless virus, it may keep its infected systems up and running rather than shut down production to remove the virus. If the organizational mission is to

keep production systems running and make money, then shutting them down could result in a higher risk (loss of revenue) than letting the virus propagate. Although this action may not be considered best practice, it reflects how tradeoffs may occur. Business and organizational drivers very often supersede recommended security and incident management actions.

Another way to clarify the distinction between incident management and security management is shown in [Figure 5](#). This figure notionally depicts the areas of intersection between security management, incident management, and IT operations. Prepare and Protect processes have actions in common with security management and IT operations, but there are also many Prepare/Protect process actions that are beyond the scope of incident management, as described above.

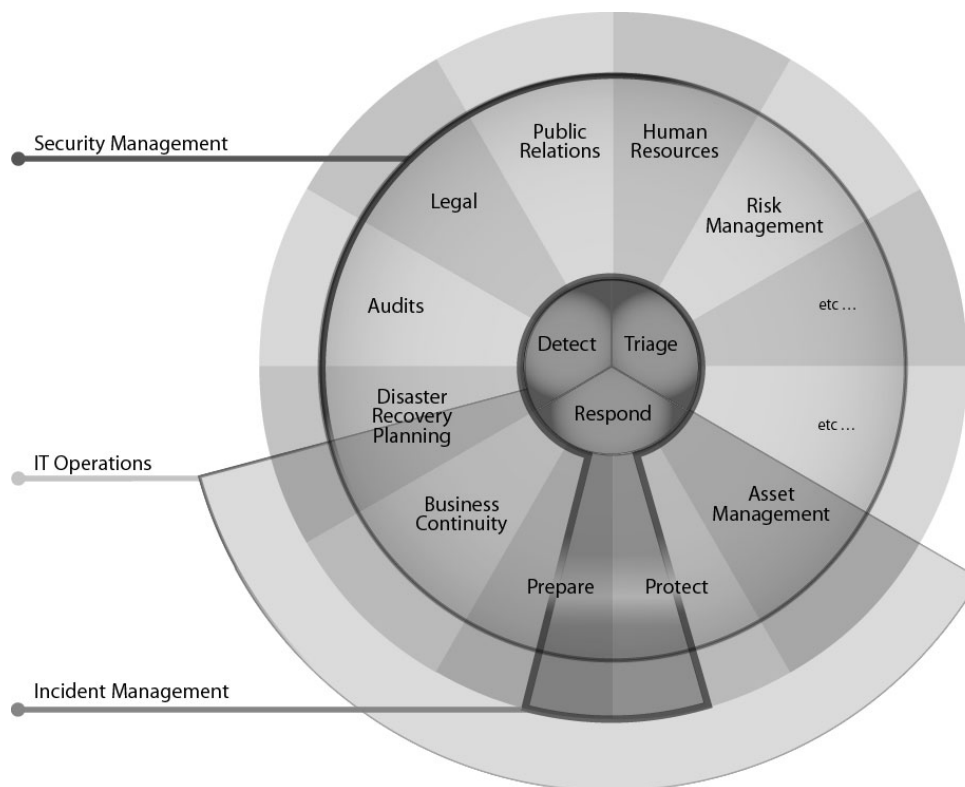


Figure 5: Overlap of Security Management, Incident Management, and IT Operations

Additionally, this diagram shows the need for coordination and information sharing between business capabilities such as legal, public relations (PR), and incident management. Incident management, as defined by the “keyhole” diagram in the middle of this diagram, touches many of the other functions, indicating the need for established channels of communication and collaboration.

2.5 Applying These Incident Management Concepts and Processes

The basic principles put forth in this report are that incident management processes are distributed in nature and should

- be enterprise driven
- have defined roles and responsibilities to ensure accountability
- have defined interfaces and communication channels with supporting policies and procedures for coordination across processes and process actors
- be integrated into other business and security management processes

The incident management processes described in this report can be used as a framework to help an organization meet the principles listed above.

This framework requires a best practice process model for incident management. That is what we have begun to develop with our new work. This report documents the initial details of that model. To develop this best practice incident management process model, we identified the processes, as described before, outlined each process via a workflow diagram, and provided the details and requirements of each process in a corresponding workflow description table.

In the following sections (3 and 4), we describe our incident management processes model in detail. The majority of the work is presented through figures called workflow diagrams that map the flow of incident management actions. These workflow diagrams and their supporting workflow descriptions and handoffs are included in Section 4, “Incident Management Process Workflows and Descriptions.” An example of a workflow is shown in [Figure 6](#). A readable version of the figure can be found in Section 4.2.3.4, “D: Detect Events Workflow Diagram.”

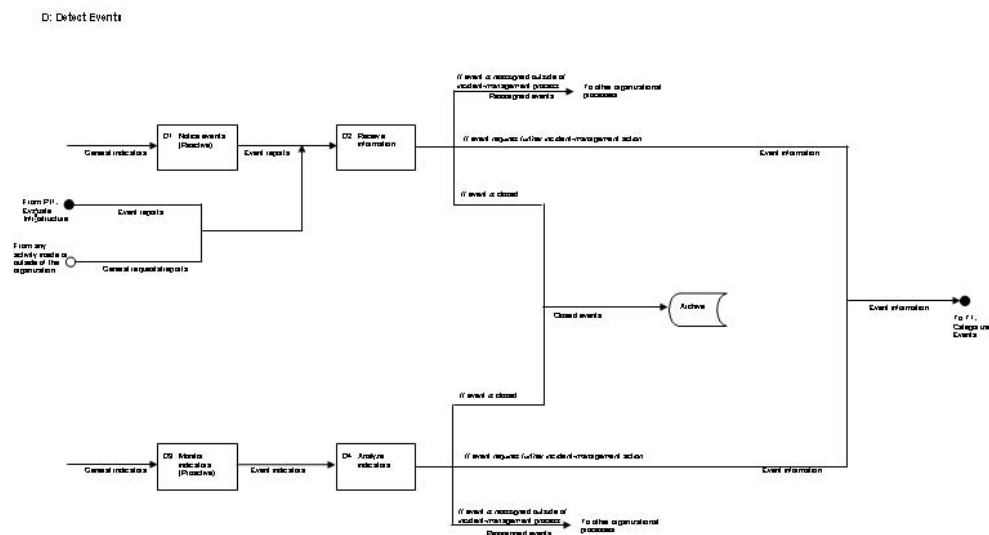


Figure 6 Example of an Incident Management Workflow Diagram

Most of the workflow diagrams have supporting information and explanations included in a multipage document called a workflow description. This workflow description includes information on the mission, triggers, completion criteria, inputs, outputs, subprocess requirements, associated written procedures to follow when performing the subprocess tasks, key people who could perform the tasks, technology used to perform the tasks, and any other general requirements. Figure 7 provides an example of a workflow description. The readable version of the figure can be found in Section 4.2.3.5, “D: Detect Events Workflow Description.”

D: Detect Events									
Mission Objectives		Triggers	Completion Criteria		Failures and Rules		General Requirements		
- To identify unusual activity that might compromise the mission of the CSRT - Identify and report CSRT - Identify and report CSRT - Identify and report CSRT		- When suspicious or unusual activity is noted - When suspicious activity is noted - When suspicious activity is noted	- When the mission is completed - When the mission is completed - When the mission is completed		- CSRTIT policies - Security-related policies, laws, guidelines, standards, and procedures - Operational security policies - Operational security policies - Operational security policies		- Operational personnel use appropriate procedures, technology, and other resources when handling information - Operational personnel receive appropriate training on procedures and technologies related to the tasks they are required to perform - Operational personnel (including personnel) receive training on CSRT and operational policies - Operational quality assurance checks are performed on submitted data - Operational personnel use appropriate procedures and security measures when configuring and securing submitted data		
Inputs									
Input	Description	Form	Decision	Output	Description	Form	Decision	Output	Description
General information	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events	Verbal, electronic, or physical	When the mission is completed	When the mission is completed	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events	Verbal, electronic, or physical	When the mission is completed	When the mission is completed	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events
General information	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events	Verbal, electronic, or physical	When the mission is completed	When the mission is completed	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events	Verbal, electronic, or physical	When the mission is completed	When the mission is completed	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events
General information	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events	Verbal, electronic, or physical	When the mission is completed	When the mission is completed	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events	Verbal, electronic, or physical	When the mission is completed	When the mission is completed	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events
General information	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events	Verbal, electronic, or physical	When the mission is completed	When the mission is completed	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events	Verbal, electronic, or physical	When the mission is completed	When the mission is completed	This information includes the following information: (1) mission or unusual activity noted for internal and external mission (2) data generated by CSRT, including information, computer activity, and other events
Subprocess									
Subprocess	Subprocess Requirements		Written Procedures		Key People		Technology		Other/Comments
D1: Detect events (events)	- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT		- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT		- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT		- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT		- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT
	- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT		- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT		- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT		- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT		- Operational personnel must report unusual activity and report to CSRT - Operational personnel must report unusual activity and report to CSRT

Figure 7 Example of an Incident Management Workflow Description

Mapping incident management processes helps an organization understand all the activities that are occurring and how they relate to and depend on one another. It also allows missing activities or activities with inherent weaknesses to be identified and targeted for improvement.

Incident management process maps are valuable for depicting these key items [Sharp 01]:

- roles – the actors or performers who participate in the process
- responsibilities – the tasks for which each actor is responsible
- routes – the workflows and decisions connecting tasks together and defining the path an individual work item takes through the process

Using the processes as a guide,²¹ an organization can map its own processes to create a workflow diagram that details its own current or “as-is” state. The fields in the workflow descriptions can be interpreted as questions for the organization to answer, such as “What is the mis-

²¹ It would be difficult to use the processes as presented here for this guidance, but future work products will be developed to help organizations apply these methodologies.

sion of the process?” and “Who performs the process?” The workflow descriptions included in our report list a fairly inclusive set of potential answers to each question. Therefore there are no real roles and responsibilities assigned to any one group in the workflow descriptions included here. When members of an organization would do such mappings themselves, they would streamline these descriptions to only include their particular arrangement or structure (i.e., the answers to the questions for their organization). When they were done mapping their current state, they would have a list of the processes and who was performing them. Accountability is very important to effective incident management.

Using this organization-specific information, the process workflow for an organization will look different from our generic workflow shown above in [Figure 6](#). It will show the workflow or routes of the work *and* who is responsible for performing the work. This type of diagram is called a “swimlane” diagram. More information about swimlane diagrams can be found in Section 3, “Overview of Process Mapping.”

To see an example of this mapping process and the resulting swimlane diagram, do the following:

1. Look at the Detect Events workflow diagram on page 98 and its corresponding workflow description on page 100.
2. An organization’s documentation of its own as-is process for Detect might result in the workflow description shown in [Table 2](#). Notice that instead of the multitude of key people or technologies that are listed in the generic Detect Events workflow diagram, this table only includes the actors performing each subprocess and the technologies currently being used to perform the process for this example organization.
3. When we actually map this process, knowing the responsible actors, we get the swimlane diagram depicted in [Figure 8](#), which shows the workflow and associated actor.²²

Once the as-is state is documented, and depending on the goal or outcome you are looking for in your process mapping work, you can benchmark your workflows against our best practice incident management process model to determine gaps and weaknesses. This is a traditional gap analysis. During this process, you would look for characteristics of the processes such as

- missing or poorly defined handoffs
- missing or poorly defined aspects of each process activity (e.g., no procedures in place or inadequate staff)
- bottlenecks in the process
- poorly defined activity flows (e.g., too much parallelism, too linear, too many handoffs)

²² Note that we only show the workflow description for Detect, but the swimlane diagram also includes the Triage and Respond processes. There would be a similar workflow description for Triage and Respond that would have been done, before the swimlane diagram was completed as shown here.

- single points of failure

You can also identify process improvements and create a new “to-be” or desired state workflow and use this as a map for implementing this new structure or process. In this case, you build the to-be state by modifying the as-is state. This will include

- identifying new activities
- identifying improvements to poor characteristics such as missing procedures or poorly trained staff
- streamlining inefficient flows
- redesigning bottlenecks

If you are planning an incident management capability from scratch, in theory you can use our generic model to help determine what functions you want to include and what procedures, staff, and technologies will be needed. We are piloting this work to test our theories. We are also looking for better tools and packaging of our workflows diagrams and descriptions, so they can be more easily used to perform this work.

Table 2: Detect Events Workflow Example

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
To identify unusual activity that might compromise the mission of the CSIRT constituency and/or the CSIRT	When suspicious or unusual activity is noticed	- When a decision about an event is made (i.e., forward to T: Triage Events, reassign to other processes, or close) - When outputs are ready to be passed to the next process	- CSIRT/IT policies - Security-related regulations and laws	- Note: no defined requirements for handling sensitive information - CSIRT staff and some IT staff receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Yearly quality assurance checks are performed on automated tools. - CSIRT and IT staff consider appropriate security measures when configuring and maintaining automated tools.

Inputs

Input	Description	Form
General indicators	This is data that is proactively gathered by IT staff, such as log information.	Electronic, or physical
Event reports	This includes reports of unusual or suspicious activity to the CSIRT identified by the organization's employees using the computing infrastructure.	Verbal, electronic, or physical

Outputs

Decision	Output	Description	Form
Event requires further incident management action (i.e., event is sent to T: Triage Events)	Event information	This includes all information that is passed to T: Triage Events for a given event. It can include the reported information and general indicators.	Electronic, or physical
Event report is closed	Closed reports	This includes all information related to an event that has been closed. It can include the reported information and general indicators. It can also include the rationale for closing the event.	Electronic, or physical

Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology
D1. Notice event (reactive)	- Computing infrastructure users notice suspicious or unusual activity and report it to the CSIRT. Inputs Outputs - Event reports	No written or formal procedures for organization's staff to follow when reporting events.	CSIRT constituency notice and report events to the Help Desk.	- CSIRT constituency uses the following technology when noticing and reporting events: - Communication channels (telephone, email, web)
D2. Receive report	- Help desk personnel review report information, verify it, and decide whether to forward an event report to T: Triage or close it. Inputs Outputs - Event reports - Event information* - Closed reports*	- Help Desk staff follow procedures for collecting required event information and sending it to T: Triage. - Help desk staff follow appropriate procedures for closing events.	Help desk personnel receive reported information from users of the organization's computing infrastructure	- Help desk personnel use the following technology when receiving, reviewing, and deciding what to do about reported information: - Communication channels (telephone, email, web)
D3. Proactive Detect	- IT staff proactively monitor indicators for potential events (e.g., log information). - IT staff analyze event indicators and decide whether to forward an event report to T: Triage. Inputs Outputs - General indicators* - Event reports	- IT staff follow operational procedures for monitoring and reviewing general indicators. - IT staff follow operational procedures when completing an event report and sending it to T: Triage.	IT staff perform proactive detect activities.	- Designated personnel can use the following technology when monitoring for general indicators: - System administration and security tools (e.g., logs and vendor applications) - Communication channels (e.g., email, web)

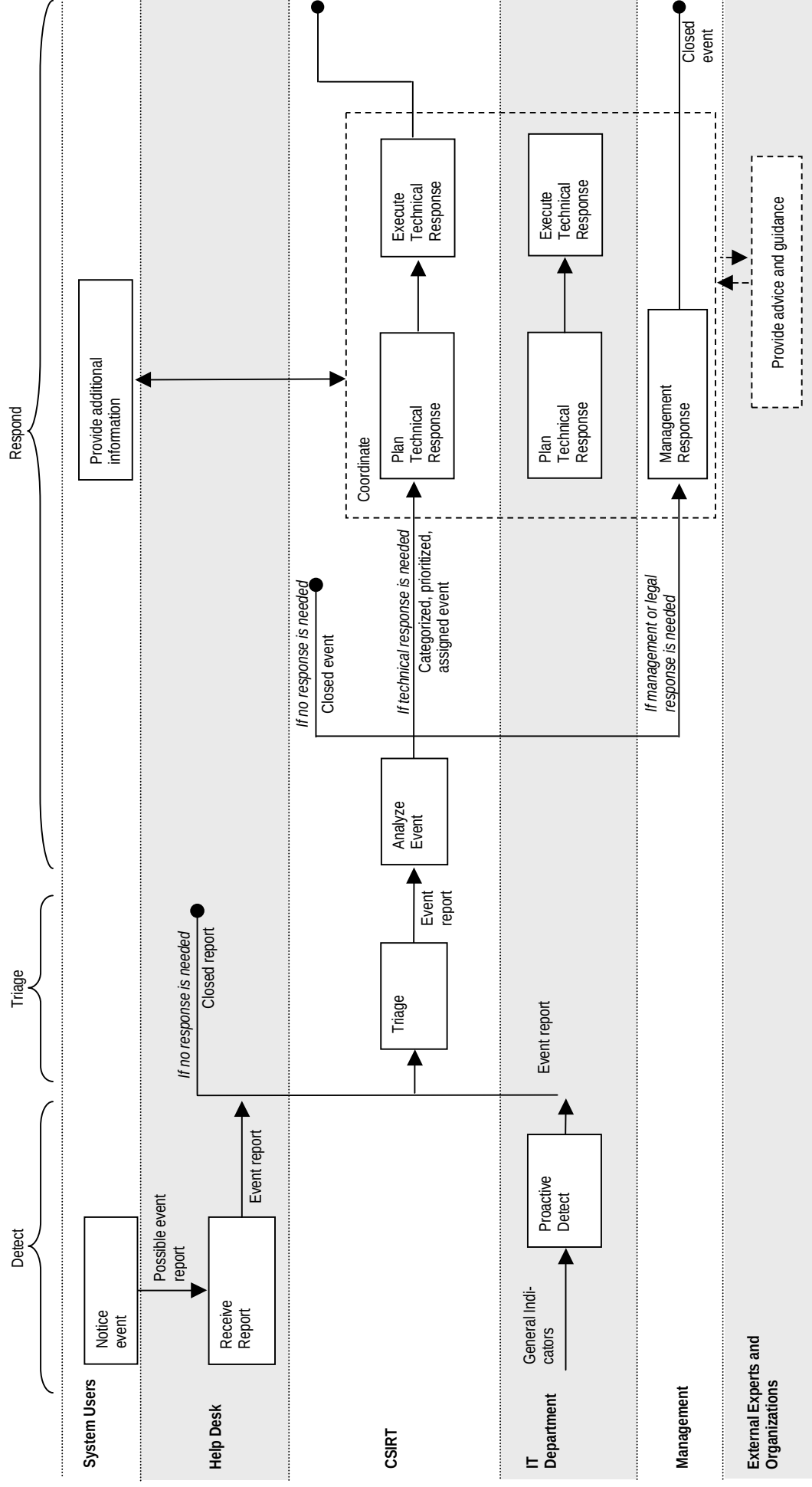


Figure 8: Example of Swim-Lane Chart Showing a Specific Instantiation of an Incident Handling Capability Derived from the Detect, Triage, and Respond Process Workflows and Descriptions

2.6 Getting Started

Although this report was not developed to be used as a guide for planning, implementing, and evaluating incident management capabilities, we understand that people may want to begin to use the ideas and concepts defined here to do just that, before supplemental materials are available to help apply these concepts.

While we are still developing and testing methods for using these process maps to establish or improve incident management capabilities, we can make a few suggestions for those who want to make use of the process maps now. These are suggestions only and your success will vary.

We have provided some ideas for where to begin for early adopters of this model and its supporting concepts. Basically, what you will be doing is identifying who does what activity and mapping that workflow.

To begin with, define what it is you want to accomplish: create an incident management capability, improve an existing one, or evaluate an existing one.

1. Collect information on what incident management processes are currently being performed in your organization. Use the high-level Incident Management Workflow Diagram on page 52 to provide a framework for the type of processes you should look for. Specific information would involve
 - functions and tasks being performed in the Prepare, Protect, Detect, Triage, and Respond processes
 - roles and responsibilities
 - supporting policies and procedures, mandates, regulations, or laws
 - technologies, equipment, and supporting infrastructures being used
 - handoffs or interfaces between processes and the actors and between business function units
2. Review the high-level Incident Management Workflow Diagram on page 52, keeping your own current situation in mind.
 - Are there any activities that are done by some other part of the organization? Then look at the handoff or interface with this group in detail to determine how well it is defined and how well it functions.
 - Is there any activity that you do not currently perform? Look at the details for this activity. Consider whether it is something you want to add and how much of it you can add.
 - Are there activities that you know are not currently being performed well? Look at the details for these activities and consider what might be missing (e.g., procedures, training, software, etc.) or need improvement.
 - If there are activities that you think you are doing well, you might check the details anyway and see if there are any hints for additional improvements. Or you can see if you can apply the related policies and procedures from those activities to other activities you are performing.

As you customize the workflows to match your processes, you may find that you drop large sections of the processes that do not apply to your organization. For example, as previously

mentioned, a coordinating CSIRT might have no Protect processes. But even in that case, there may be some aspect of Protect ongoing, even if it just relates to the maintenance and security of the systems and networks belonging to and being used by the CSIRT.

If you are creating a capability, you can use the information you have mapped to determine what functions and processes are already being performed, where gaps exist, and what functions your incident management capability requires to be successful.

If you are improving an existing capability, you can match your customized process workflow against the ones included in this report to determine where gaps exist and what improvements could be made.

If you are evaluating an existing capability, you would match your customized process workflow against our workflows and descriptions to determine what applicable processes, policies, procedures, staffing, and technology are missing. This is basically a gap analysis.

2.7 Detailed Workflow Diagrams and Descriptions

The remainder of the report provides an in-depth look at our process mapping methodology and at the five high-level processes described in this section and a number of the subprocesses for each that have been defined and mapped to date. As previously stated, there is still a lot of work to be done to fill out this model.

If you want to look at the detail for each process, then you may want to continue reading. Please remember that workflow diagrams by themselves may be difficult to understand. You will need to look at the supporting workflow descriptions to understand all the inputs, outputs, and interfaces.

3 Overview of Process Mapping

3.1 What is Process Mapping?

Process mapping is a common technique for describing a set of activities performed to accomplish a set goal or mission. There are many specific techniques for determining and documenting processes [Jackson 97, Kobiellus 97, Sharp 01]. Most techniques usually define not only the specific activities that take place but also the dependencies, interrelationships, and sequencing of the activities. Most also define various attributes such as inputs and outputs, who performs the activities, and other similar details.

Specifically, a good process map will include the following types of information:

- goals and objectives for the overall process and each activity
- processes and activities²³
- inputs and outputs of each activity
- roles and responsibilities of the people who perform the activities
- constraints on the activities, such as budget or schedule
- enablers, such as employee training
- supporting technology, such as an IT infrastructure
- procedures and documentation
- interfaces or handoffs between different activities (i.e., where one person must transfer or send their outputs as input to another person)
- interrelationships and dependencies (e.g., activity C depends on the successful completion of activity A, or activities D, E, and G must be performed in parallel)

Process mapping can be done to understand and document an existing process. But it is usually undertaken as part of a broader business process re-engineering effort.

A process is generally re-engineered to

- increase efficiency or effectiveness
- alter scope
- understand its weaknesses and strengths

²³ Although the level of detail in which a process is defined can vary.

- make other improvements

The steps followed in performing this business process re-engineering are to

- identify the core business processes
- map the as-is processes
- rethink the processes
- plan and map the to-be processes [Jackson 97, Kobiellus 97, Sharp 01]

Figure 9 provides a simple example of a process map for answering the phone.



Figure 9: Process Map Example

How to read and interpret this type of diagram will be explained in Section 3.3.

3.2 Applying Process Mapping to Incident Management

The same strategy for improving organizational business processes is also applicable to incident management and, as part of that, CSIRT operations. Mapping incident management processes helps an organization understand all the activities that are occurring and how they relate to and depend on one another. It also allows missing activities or those activities with inherent weaknesses to be identified and targeted for improvement. Risks that can affect a successful response to incidents can be recognized and mitigated. By understanding the whole set of processes and activities, improvements can be made in context, avoiding the waste of isolated fixes.

Mapping the incident management processes

- enables a comprehensive understanding of the current (as-is) state. Attributes that are detailed include process
 - activities
 - roles and responsibilities
 - technology used
 - interfaces
 - dependencies
- identifies risks to successful completion of the mission of the incident management capability

- supports decisions about improvements to incident management operations (the to-be state)

One way to accomplish this analysis is by using a general or standardized map²⁴ of incident management practices and comparing your version of these processes and activities to determine if there are any gaps or weaknesses. Next you would look at what types of strengths and other compensating factors might balance those gaps and weaknesses. In evaluating a process you would look at the

- completeness of the process—whether it is successfully meeting its mission
- strengths and weaknesses of the process
- risks to the process, including
 - environmental factors such as funding, organizational culture, access to data, geography and location
 - operational factors such as having the right staff that is adequately trained, the availability of supporting policies and procedures, and ongoing coordination and communication across the involved parties
- decision points in the process

This type of evaluation can provide a foundation on which a plan for short- and long-term improvements to the incident management capability can be made.

Process maps can also be used as a basis for evaluating the risks to successful incident management operations. In this case, the process map serves as a source of information or risk data for identifying risks. These risks are then analyzed and prioritized to produce strategies for mitigating the most important risks.

3.3 Our Process Mapping Methodology

The process mapping work grew out of a project aimed at assessing the effectiveness of CSIRTs. We had been chartered to develop a CSIRT assessment technique for specific customers and decided to incorporate a new risk analysis methodology being developed by the SEI. That risk analysis methodology is based on a process-mapping, or workflow-design, technique called swimlane diagramming. It also relies on several custom-developed data collection and risk analysis artifacts.

Process modeling techniques are useful for illustrating an abstraction of a business process, highlighting key activities and artifacts required to conduct the process. A workflow model is a specific type of process modeling technique, providing a description of how tasks are done, by whom, in what order, and how quickly. It differs from other modeling techniques, such as data flow diagrams and flow charts, because it specifically defines interrelationships and dependencies among tasks and activities; other modeling techniques do not provide this infor-

²⁴ “Map” in this context relates to the process workflow diagrams and supporting descriptions.

mation. Understanding interrelationships and dependencies among tasks and activities is important when analyzing the risk inherent in a business process, such as incident management. For this reason, workflow modeling became an integral part of our risk analysis work.

As indicated above, we specifically selected swimlane diagramming as our central modeling technique. (To see an example of a swimlane diagram, please refer to page 33.) Swimlane diagrams highlight relevant process variables—the “who, what, and when”—in a simple notation. They show an entire business process from beginning to completion and are valuable for understanding the as-is workflow, as well as for defining the to-be workflow. These diagrams are valuable for depicting the following key items [Sharp 01]:

- roles – the actors or performers who participate in the process
- responsibilities – the tasks for which each actor is responsible
- routes – the workflows and decisions connecting tasks together and defining the path an individual work item takes through the process

While workflow modeling provides several critical pieces of information vital to risk analysis, we needed to extend the technique to fully capture the broad range of information required. With respect to the swimlane diagrams, we followed the principles outlined in *Workflow Modeling* [Sharp 01]. We tried to keep the diagrams as simple as possible, which can be quite challenging for a process as complex as incident management. We limited our use of symbols, attempting to keep the diagrams readable by the widest audience possible. We also made liberal use of textual annotation in the diagrams to provide additional information about the process where appropriate. We used standard icons on the diagrams where appropriate. The primary reason for using annotation and icons in certain instances was to capture additional information related to the risk analysis technique. For example, we denoted the inputs and outputs related to each task directly on the swimlane diagram because this information is essential to analyzing risk. (For more information about swimlane diagrams and how to read them, refer to *Workflow Modeling* [Sharp 01].)

While the interrelationship, dependency, timing, and sequencing information illustrated by a swimlane diagram is necessary to conduct a risk analysis, additional data is required to ensure that the analysis is complete. Process risk also includes information related to *how* a work process is executed. Unfortunately, swimlane diagrams do not provide enough information about process execution, which led us to further extend the workflow modeling technique. We designed a table called a *process description* to document additional information about each process, including how the process is conducted, which procedures must be followed, and which technology supports the process. The information documented in swimlane diagrams and process descriptions provides sufficient data for the risk analysis.

Finally, to facilitate a risk analysis at a given site, we developed a generic incident management practice that could be easily tailored to that site. The generic practice provides the basis for the technical information presented in this report. As we began building the generic model, we realized how many variations existed with respect to roles and responsibilities for each incident management activity. For example, the people responsible for receiving infor-

mation reported by the constituency (from D2: Receive Information) can include the following:

- help desk staff
- CSIRT triage staff
- CSIRT hotline staff
- CSIRT manager
- incident handlers
- information security officer
- system and network administrators
- third-party answering service
- coordination center

Because of the sheer number of potential roles and responsibilities potentially associated with each incident management activity, we determined that our generic workflow diagrams had to differ from classic swimlane diagrams in one important respect. The large number of potential actors or performers for each activity, if included on the diagrams, precluded our ability to keep the diagrams simple and readable. We thus moved information about roles and responsibilities to the process descriptions and eliminated this information from the workflow diagrams. However, when performing a risk analysis for an organization, the first step is to determine precisely who is responsible for performing each incident management activity, enabling us to create a unique swimlane diagram for that organization.

3.3.1 Additional Uses for the Workflow Model

Upon developing the initial version of the incident management model, we saw how it could serve multiple purposes. It provides a needed structure for organizing the body of knowledge in the incident management domain, bringing with it the potential for influencing the development of future products and services. However, it is important to keep in mind the original intent of the model as you review the details presented in this report. Its format reflects our original purpose for creating it, which is assessing the effectiveness of CSIRTs or other incident management capabilities. You should view the model presented in the following pages as a prototype or work in progress rather than a final product.

Early feedback indicates that the prototype has uses far beyond what we imagined when we first began working on it. We now see the incident management model as a stand-alone product rather than simply part of an assessment. We intend to continue developing the model, improving its content based on input from the community and providing progressively more detail over time. As the model evolves, its format and content might change, reflecting its expanding role in our product suite.

3.4 Guide to Reading the Incident Management Process Maps

Incident management activities and functions are documented via the process mapping method in two forms: workflow diagrams and workflow descriptions. These workflows and descriptions can be found in Section 4. The components of the workflow diagrams and corresponding descriptions are outlined in the following sections.

3.4.1 Workflow Diagrams

The workflow diagrams are similar to other types of process workflows.²⁵ Processes are defined by both a short acronym and a descriptive phrase, such as R: Respond. Basic rules for interpretation are as follows:

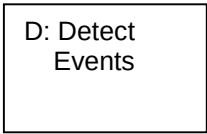
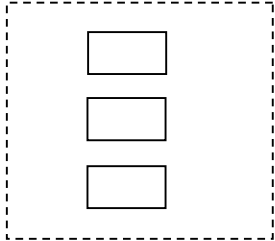
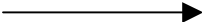
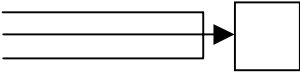
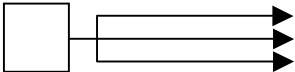
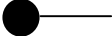
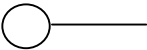
- Flows are read from left to right.
- Lines and arrows indicate flow between activities in a workflow or the completion of a workflow. *It is important to note that work flows only in the direction depicted by an arrow.*
- Each box on a workflow diagram can be expanded into another graphic depicting a greater level of detail. This expansion occurs when the additional level of detail is required to fully understand the process.
- A handoff basically details the workflow of an interaction between the major processes. Handoffs occur when work is passed between actors (e.g., the actor(s) responsible for completing R: Respond pass infrastructure protection improvements to the actor(s) responsible for completing PI: Protect Infrastructure when appropriate).

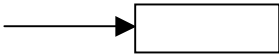
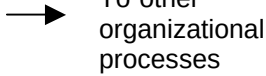
The symbols, lines, and labels used on the incident management workflow diagrams for CSIRTs are interpreted according to [Table 3](#).

Table 3: Key to Incident Management Process Map Symbols

Symbol	Meaning	Example
Process title	Freestanding name in the upper left corner of the diagram indicates the name of the <i>process</i> depicted in the flow diagram.	Incident Response
Solid-line box	An <i>activity</i> within the process.	

²⁵ In this report the processes documented reflect general good practices for CSIRTs. Any organization could tailor these process maps to indicate how they conduct these processes.

Symbol	Meaning	Example
Box labels	The name of the activity. A short acronym for the activity is first, followed by the complete name.	
Dashed-line box	Represents coordination type of activity that encompasses other activities. This indicates that some degree of coordination must occur among the contained activities. This coordination often requires multiple, unpredictable feedback loops among the contained activities.	
Basic line	Lines indicate inputs to an activity and outputs from an activity. They also connect activities that have dependencies.	
Forked set of lines, left side of a box	Indicates a set of alternative inputs to an activity. Only one of the set is required to initiate the activity.	
Forked set of lines, right side of a box	Indicates a set of alternative outputs from an activity. One or more of the outputs may occur.	
Plain text line label	Indicates the output that is being sent from one activity to another.	Event Information
Italicized line label	Indicates a choice or alternative route to be taken if a condition is true.	<i>If closed incidents are documented</i>
Line termination: line ends without a terminating symbol	Indicates the end of a workflow without specifying any additional information or context (i.e., there is no stipulation of the final form of the output or of any destinations of the output external to the process being studied).	
Line initiation: line flows from a closed, filled circle	Indicates that an input originates from a specific activity elsewhere within the process being studied.	From R: Respond 
Line initiation: line flows from an open circle	Indicates that an input can originate from multiple activities elsewhere within the process being studied or from activities external to the process being studied. The label provides additional context about where the input can originate.	From any activity... 

Symbol	Meaning	Example
Line initiation: flow begins without an initiating symbol	Indicates the input flows from an unspecified source that is outside the scope of the process being studied. Lines only flow in one direction.	
Line termination: line ends at a closed, filled circle	Indicates that an output flows to a specific activity elsewhere within the process being studied.	 To P1: Protect Infrastructure
Line termination: line ends at an icon	Indicates the end of a workflow while also specifying the form of the output (e.g., document, archive).	
Line termination: line ends at a label	Indicates the end of a workflow within the scope of the process being studied. The label provides additional context about the output (e.g., what other organizational processes use it next, the audience that requires it)	

Keep in mind a couple of subtleties when reading the diagrams in this report. The first is related to merging workflows. [Figure 10](#) illustrates a case in which two workflows join together as they enter an activity. When the two flows meet, the workflow represented by the bottom line is joining the flow represented by the top line. Notice that the direction of the top flow is toward process R1.4: Close Technical Response. Because workflows are unidirectional, the merged flows must move in the direction of process R1.4, not away from it.

A second subtlety that can easily be overlooked is the number of branches flowing into an activity. Processes are generally triggered when their inputs arrive. When two workflows merge before reaching a process, as illustrated in [Figure 10](#), only one of the input streams is needed to trigger the process. By contrast, both input streams illustrated in [Figure 11](#) must arrive at process PI2: Determine Infrastructure Protection Requirements before that process can be executed. Note that the two flows do not merge; they flow into the activity separately, indicating that both inputs are required to initiate the process.

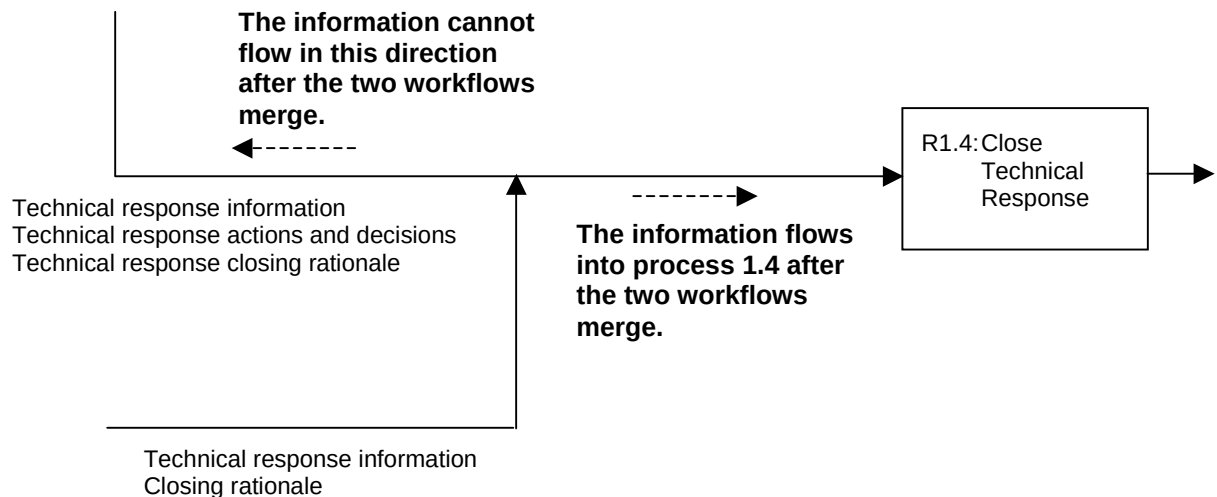


Figure 10: Merging Workflows Triggering an Activity

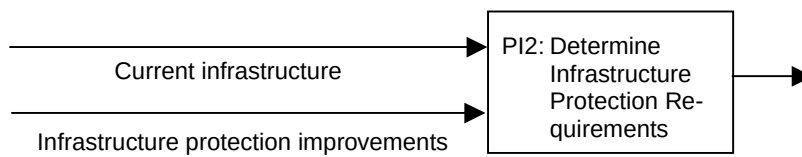


Figure 11: Separate Workflows Triggering an Activity

Finally, incident management is complex, requiring many decisions to be made at various times throughout the process. Decision points are represented on diagrams using distinct branches, with each branch having a unique “if” statement annotated above it. For example, [Figure 12](#) illustrates that a decision must be made during process D2: Receive Information. The people responsible for executing process D2 must determine what to do with the reports they receive. They have the following three choices:

1. An event can be reassigned outside of the incident management process.
2. Event information can be forwarded to T1: Categorize and Correlate Events if an event requires further incident management action.
3. An event can be closed and archived, indicating that no further action will be taken to address it.

In [Figure 12](#), the annotated statement for a given branch indicates the condition in which that path will be followed. For some processes, multiple paths can be followed at the conclusion of the process, because more than one of the conditions can be true at any given time.

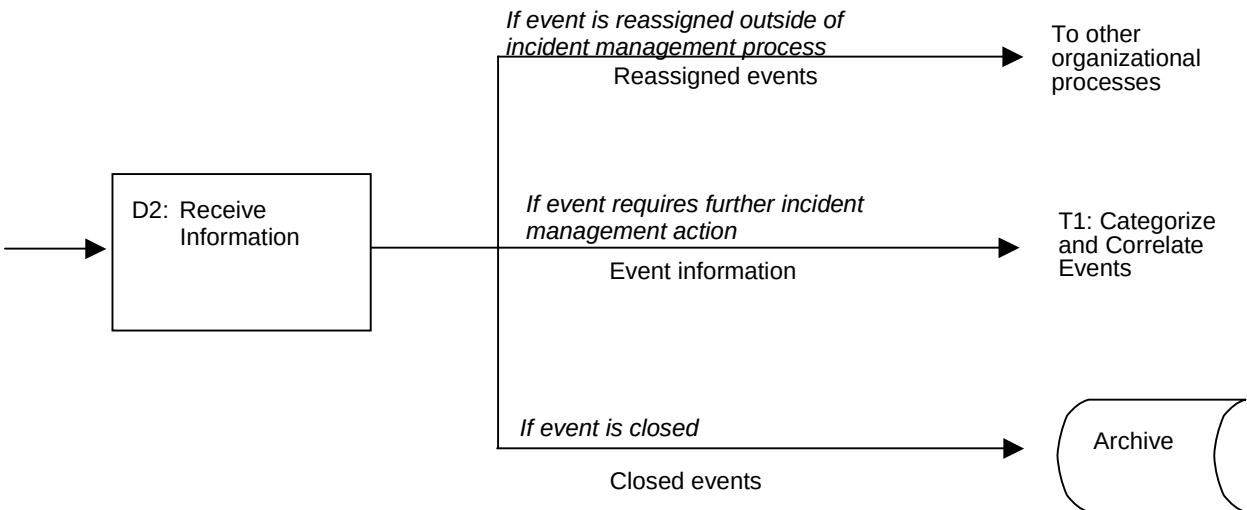


Figure 12: Process Decisions and Alternative Branches

3.4.2 Workflow Descriptions

The workflow descriptions are contained in tables describing details about multiple aspects of each process and its activities. Separate descriptions are also provided for each handoff.

These tables include a wide range of information that reflects good practices, as well as a list of possibilities for some categories, such as Key People. For example, in the workflow diagram for PI: Protect Infrastructure on page 80 we can see that in the first subprocess, PI1: Evaluate Infrastructure, the key people who might be involved in this activity are listed as IT staff, audit staff, risk management staff, third-party managed security service providers, or CSIRT staff. Depending on the organizational structure and procedures, any of these people might perform this work. That is why several people are listed. It does not mean that for any given organization, all these people would perform this work.

Any organization tailoring these descriptions would select from the presented choices to indicate precisely who, in their organization, performs these tasks. Once those roles and responsibilities were established, necessary interactions and interfaces with other parts of the incident management capability would then be outlined and, where appropriate, put in place. For example, if the evaluation of the incident management capability was to be done by the audit staff, then according to the processes outlined in PI1: Evaluate Infrastructure, the audit staff would need to know how to report any indication of incidents or other problems they may uncover. This would mean that policies and procedures and supplemental materials such as incident reporting forms would need to be created and a formalized process put in place to hand off the discovered incidents to whoever has been designated as the receipt contact point for incident and event reports in the Detect process.

Handoffs are exchanges between actors (e.g., from one person to another or even from a technology to a person, or a person to a technology) and occur between the major processes such as

Detect to Triage, Triage to Respond, etc. Another term for handoff is interface; this is usually for system-to-system types of exchanges. The categories of information provided in each process description and handoff description are defined according to [Table 4](#) and [Table 5](#).

Table 4: Incident Management Workflow Description Information Categories

Information Category	Description
Mission/objectives	The goals for this process. Defines what should be accomplished by the successful completion of the process activities.
Triggers	Activities that initiate the process. This could be an event or an input.
Completion criteria	Conditions that must be met for the process to be successfully completed.
Policies and rules	Any policies, laws, regulations, rules, etc. that govern this process or its outputs.
General requirements	Any type of supporting information, procedures, or technology that may be needed to successfully perform activities associated with this process.
Inputs	The required inputs for this process.
Input name	The name of the input.
Input description	A short description of the input, including the sending process.
Input form	The form of the input (usually verbal, electronic, and/or physical).
Outputs	The possible outputs of this process.
Output decision	Any relevant decisions that will produce one output vs. another.
Output name	The name of the output.
Output description	A short description of the output, including its destination.
Output form	The form of the output (usually verbal, electronic, and/or physical).
Subprocess	All of the subprocesses or activities for this process.
Subprocess name and diagram	The acronym (e.g., D1 for the first subprocess of Detect), the name (e.g., Notice Events), and a simple diagram indicating the relevant box on the process flow as a visual reference for the reader.
Subprocess requirements	The requirements for this subprocess, namely what must occur for this subprocess to be successful. Also included are any inputs/outputs related to these subprocess requirements.
Written procedures	Any procedures that must be followed by those conducting this subprocess.
Key people	The types of key people who may conduct this subprocess or who need to be involved in any discussions or decisions.
Technology	The types of supporting technology that may be needed to successfully perform this subprocess.
Other/miscellaneous	Any other relevant items for this subprocess.

Table 5: Incident Management Handoff Description Information Categories

Information Category	Description
Mission/objectives	The goals for this handoff. Defines what should be accomplished by the successful completion of the handoff.
Triggers	Activity that initiates this process. This could be an event or an input.
Completion criteria	What constitutes success for this handoff.
Policies and rules	Any policies, laws, regulations, rules, etc. that govern this handoff.
Processes involved	Identifies the processes on either side of this handoff or interface.
Sending process	The acronym and name of the process sending the objects being transmitted.
Receiving process	The acronym and name of the process receiving the objects being transmitted.
Objects being transformed/transmitted	The objects being exchanged between the sending and receiving processes.
Object name	The name of the object being transmitted.
Object description	A short description of the object being transmitted.
Handoff descriptions	Set of descriptive information for each possible type of handoff (person to person, person to technology, technology to person, technology to technology).
Handoff requirements	Any specific requirements governing how the handoff is to be conducted.
Written procedures	Any procedures that must be followed by people or associated technology to successfully complete this handoff.
Sending actor	Possible types of sending actors.
Receiving actor	Possible types of receiving actors.
Transmission/transportation modes	Relevant modes of transportation that can be used (usually verbal, electronic, and/or physical).
Transmission/transportation mechanisms	Relevant types of transportation mechanisms that can be used (e.g., phone, email, etc.).
Other/miscellaneous	Any other relevant characteristics of this handoff.

4 Incident Management Process Workflows and Descriptions

4.1 Overview

This section provides detailed information on the incident management processes and sub-processes we have defined to date. Included for each process—Prepare, Protect, Detect, Triage, and Respond—are

- a brief overview of the process
- the workflow diagrams showing a visual representation of the process and its inputs, outputs, and relationships with other processes
- the workflow descriptions, which are corresponding tables that outline the supporting components of the workflows, including the mission of the process, general requirements, triggers, subprocess requirements, written procedures that may guide the process, key personnel who may perform the process, and technologies used to perform the process, along with other descriptive information
- any corresponding handoffs, which detail how information is passed from one process to another

Handoffs included and described are listed below:

- Handoff from Any Activity Inside or Outside the CSIRT Process to PC: Prepare/Sustain/Improve
- Handoff from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure
- Handoff from Any Activity Inside or Outside the CSIRT Process to PI: Protect Infrastructure
- Handoff from PI: Protect Infrastructure to D: Detect Events
- Handoff from Any Activity Inside or Outside of the Organization to D: Detect Events
- Handoff from D: Detect Events to T: Triage Events
- Handoff from T: Triage Events to R: Respond
- Handoff from R: Respond to PC: Prepare/Sustain/Improve

More information about how each process can be built, sustained, and evaluated will be developed in future reports.

The rest of this section presents a lot of detail in the form of diagrams and tables. Reading through these process maps can take a lot of time and can be a daunting task. If you want only an overview of our process map work, you may want to stop reading at this point. If you are interested in the subprocess components of each high-level process and the details of those subprocesses, you may want to continue reading.

The process workflows and descriptions are written in a standardized way, so they can become very repetitive if you review them at one sitting. If you want to apply the concepts behind the incident management process maps, you may want to wait until we release more user-friendly documentation that provides guidance for implementing and applying this information.

The workflow diagrams and descriptions are formatted to spread over two pages, so they all start on a left-hand page. As a result, there are a number of blank pages in this section.

A set of the process map workflow diagrams and descriptions and handoffs formatted on single pages is included in Appendix D, “One-Page Versions of the Process Workflow Diagrams,” and Appendix E, “One-Page Versions of the Process Workflow Descriptions and Handoffs.”

4.2 Incident Management

This is the top level of the process maps, identifying the five main processes of the incident management activity that were described in the previous section: Prepare, Protect, Detect, Triage, and Respond.

As described before, the Prepare process defines all the prework that has to occur to enable quick response to any risks, threats, or attacks. This means having in place the required people, policies, procedures, equipment, and infrastructure to perform the assigned tasks. The Prepare process also contains the subprocesses for evaluating the incident management capability and for performing a postmortem review of any incidents, vulnerabilities, or response actions where appropriate. Any outputs from the evaluation or postmortem that result in improvements to CSIRT processes are passed back to the planning and design processes. Any outputs that result in needed changes to the infrastructure to harden/secure systems and networks in order to prevent future incidents are passed from Prepare to Protect.

The Protect process relates to changes in the computing infrastructure to respond to or prevent attacks or malicious activity. These changes may result from information gained during the handling and analysis of an incident, artifact, or vulnerability. This process involves improving the infrastructure based on known threats, recommended best practices, and mitigation strategies. Process improvement can come from the Respond process as a reactive step in handling an ongoing attack or potential threat. It can also come as a best practice improvement from any other process inside or outside the incident management capability as a proactive step to prevent incidents from happening. The Protect process also contains a subprocess

for performing an infrastructure evaluation, such as a vulnerability scan or assessment. In that evaluation, a potential vulnerability, ongoing malicious activity, or the remnants of an intruder compromise or attack may be discovered. If such things are discovered they are passed to the Detect process, as an incident or vulnerability report.

The Detect process is triggered when general security information is received or suspicious activity is observed. Events that require further action are forwarded to Triage, where they are sorted according to predefined categories and priorities²⁶ to maximize the effectiveness of the response. Any notable events, incidents, vulnerabilities, and other information is forwarded to the Respond process., where the appropriate response action is taken.

Note that sometimes a report or an event will be determined to be outside the scope of the incident management process. In that case, the information may be passed to another organizational unit for handling or closed because no further action will be taken. This can occur in the Detect, Triage, or Respond process. Who makes this determination will depend on who is actually performing the process in question. An event might also be closed because it is determined to be a “non-event.” In this case, it may not be related to computer security activities and therefore requires no further handling. For example, a help desk may receive a wrong number phone call. This event may be tracked to gather information on the total number of calls coming in, but will be immediately closed.

In reviewing the diagram shown in [Figure 13](#), it is important to note that the outputs listed to the right of the process boxes relate to the context of the subprocesses for those high-level processes. Although you are seeing the outputs, their corresponding source may not be as readily apparent.

Also note that the straight black arrows at the far right of the process boxes signify the end of the process (or rather that the process is ongoing at that point).

²⁶ Priorities and any related criteria are defined by the organization or corresponding CSIRT.

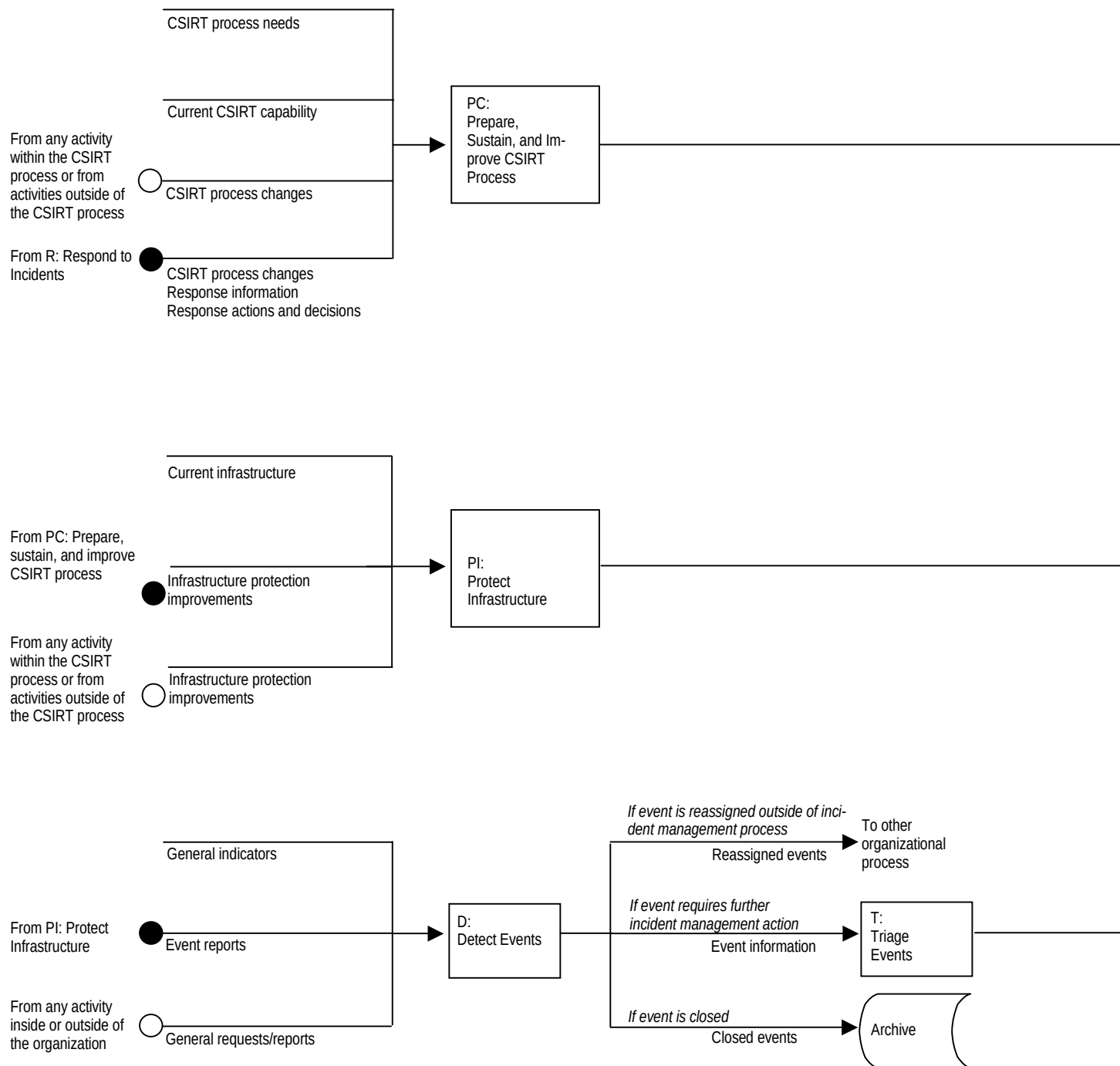
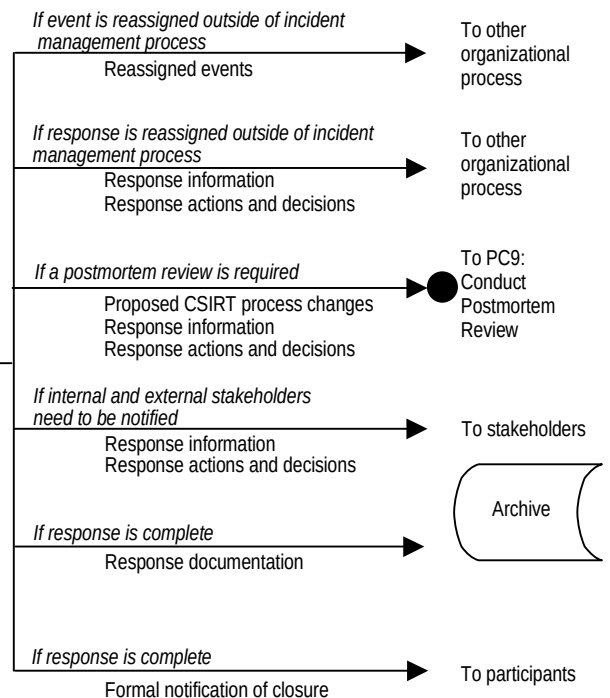
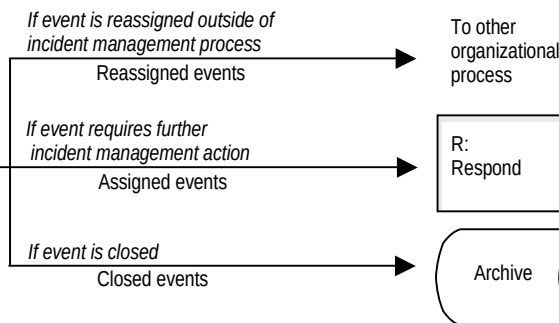
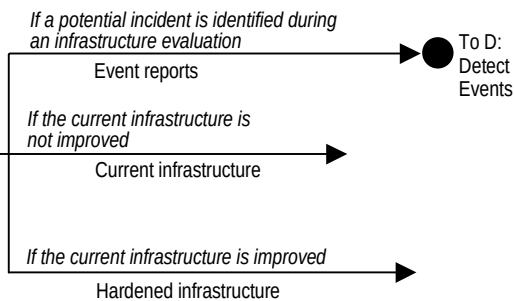
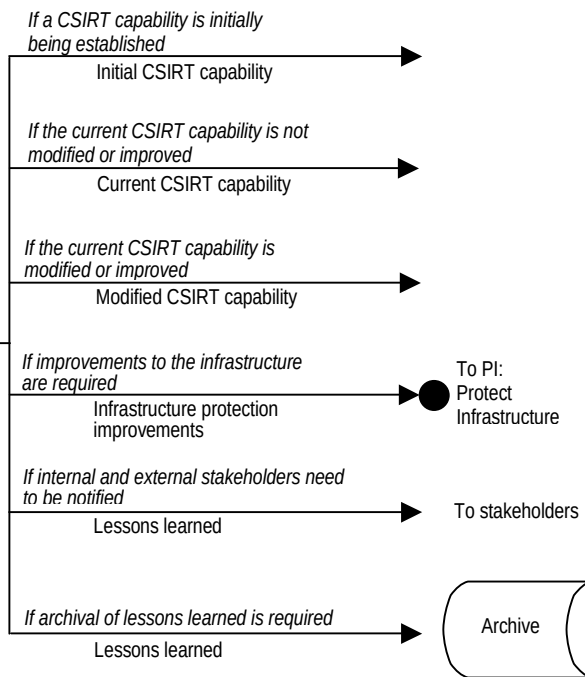


Figure 13: Incident Management Workflow Diagram



4.2.1 PC: Prepare/Sustain/Improve Process (Prepare)

The Prepare process outlines what needs to be in place for incident management to occur in a timely and effective manner. This can include what

- staff is required and what training they will need to adequately perform their job
- tools, equipment, and supporting infrastructure will be required, such as secure communications mechanisms and network connections, incident tracking databases, online incident reporting forms, or analysis tools
- policies and procedures will govern the operation of the incident management capability and its interactions with any other part of the enterprise or constituency. This might include information disclosure policies, standard operating procedures, or any service level agreements in place.

One part of this process involves the building of the initial CSIRT or incident management capability. If a new capability is to be formed, the main subprocesses break down into two basic areas:

- coordinating the planning and design of the capability (PC1 – PC3)
- coordinating the implementation (PC5 – PC7)

In the planning and design phase, a needs analysis and requirements definition are performed to define what the CSIRT capability is to be (PC1). Requirements may come from a wide variety of sources. These can include interviews and discussions with stakeholders, existing policies and guidelines, business needs, and regulations or laws related to the establishment of an incident management capability. For example, the Federal Information Security Management Act (FISMA) [FISMA 02] requires all U.S. federal civilian agencies to have a response capability. Requirements can also come in the form of reporting guidelines; for example, critical infrastructures in the United States must report any incidents. Requirements may also be industry- or organization-specific and derived. In addition, some organizations may look to International Standards Organization (ISO) standards or other best practice approaches for guidance in building effective incident management capabilities. This guidance then provides them with specific requirements for compliance.

The requirements definition is used to outline a CSIRT vision (PC2), which defines the mission, constituency, services, organizational model, and resources for the capability. A parallel process obtains sponsorships and funding for the CSIRT (PC3).

From this initial work, an implementation plan is developed (PC4), and this is used to build, staff, and equip the CSIRT (PC5–PC7). Processes PC5–PC7 are not sequential and can occur in parallel. Written procedures that may already be in place and able to provide organization-specific guidelines for performing these processes include any change or process management procedures; any legislative, regulatory, sector, or business policies, laws, or require-

ments; any human resource policies regarding hiring and training staff; and any network policies for developing and deploying computer resources.

The Prepare process includes subprocesses for sustaining and improving an existing capability. Once a CSIRT or incident management capability is established, or if a capability already exists, it can be evaluated (PC8). If at the end of the Respond process (See [Figure 18, R: Respond](#) on page 132), it is determined that a postmortem should be performed, this activity will occur as part of the Prepare process (PC9). Process improvements resulting from either an evaluation or a postmortem or from any other part of any other process are then reviewed, and any process modifications are determined (PC10) and implemented (PC11).

Related workflow diagrams, descriptions, and handoffs that detail the Prepare process in the following pages include

- PC: Prepare/Sustain/Improve Workflow Diagram ([Figure 14](#))
- PC: Prepare/Sustain/Improve Workflow Description ([Table 6](#))
- Handoff from Any Activity to PC: Prepare/Sustain/Improve ([Table 7](#))
- Handoff from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure ([Table 8](#))

Resources available from the CERT/CC that provide more information about designing, implementing, and sustaining a CSIRT or incident management capability include

- *Creating a CSIRT: A Process for Getting Started*
<http://www.cert.org/csirts/Creating-A-CSIRT.html>
- *The Handbook for CSIRTs*
<http://www.cert.org/archive/pdf/csirt-handbook.pdf>
- *Organizational Models for CSIRTs*
<http://www.cert.org/archive/pdf/03hb001.pdf>
- *The State of the Practice of CSIRTs*
<http://www.cert.org/archive/pdf/03tr001.pdf>
- *CSIRT Services*
<http://www.cert.org/csirts/services.html>
- *Staffing Your CSIRT: What Basic Skills Are Needed?*
<http://www.cert.org/csirts/csirt-staffing.html>

Various courses are also offered by the CERT/CC related to this topic. You can find information about these courses at http://www.cert.org/nav/index_gold.html.

Future work will detail methodologies for evaluating and assessing incident management capabilities and corresponding processes.

4.2.1.1 PC: Prepare/Sustain/Improve Workflow Diagram

Trigger 1

When a CSIRT capability is initially being established, processes PC1 through PC7 are completed.

Trigger 2

When changes or improvements to an existing CSIRT capability have been identified through means other than an evaluation, processes PC10 and PC11 are completed. PC9 is optional. It is completed only when a postmortem review is needed to identify CSIRT process improvements.

Trigger 3

When an existing CSIRT capability is evaluated, PC8 is conducted. PC10 and PC11 may also be completed, depending on the results of the evaluation.

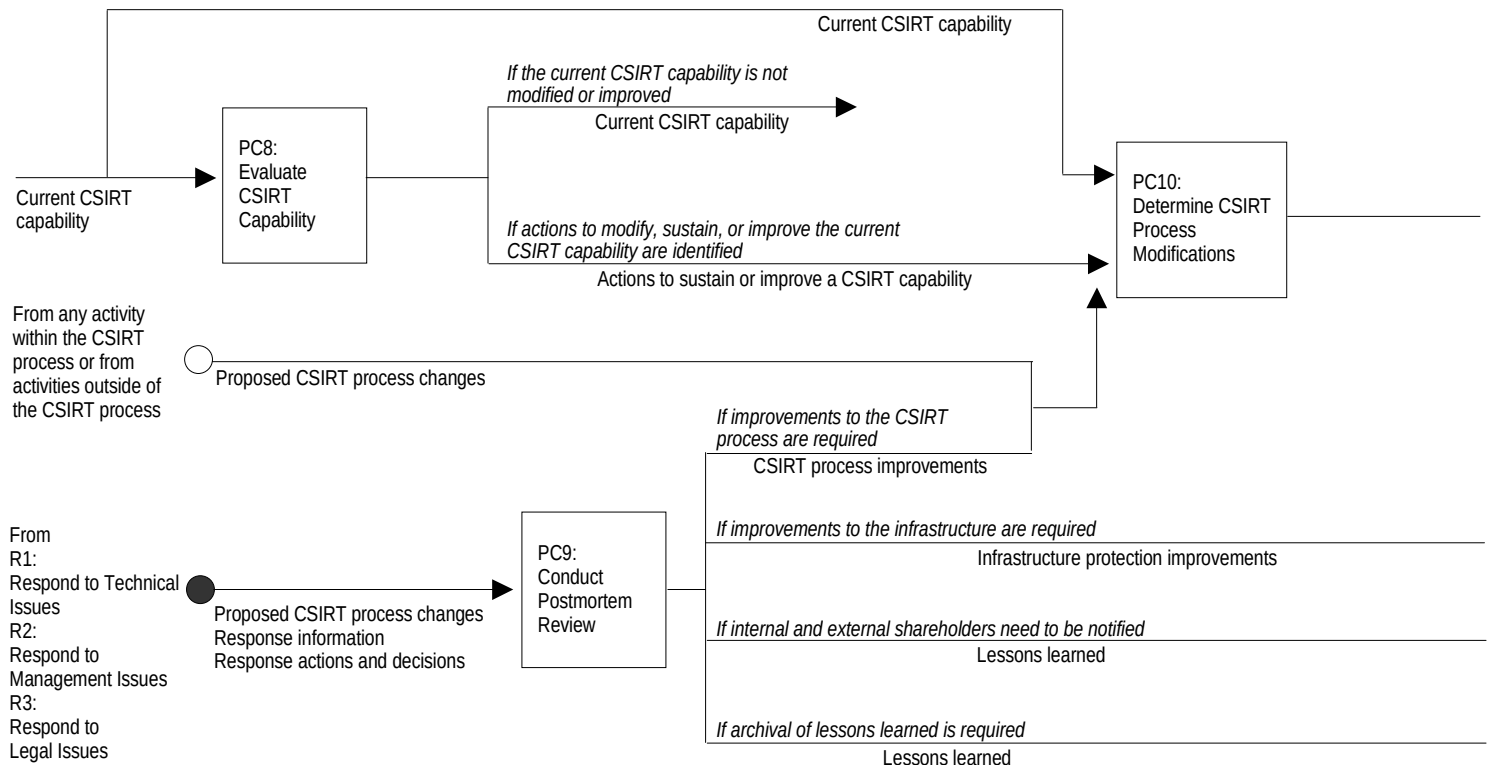
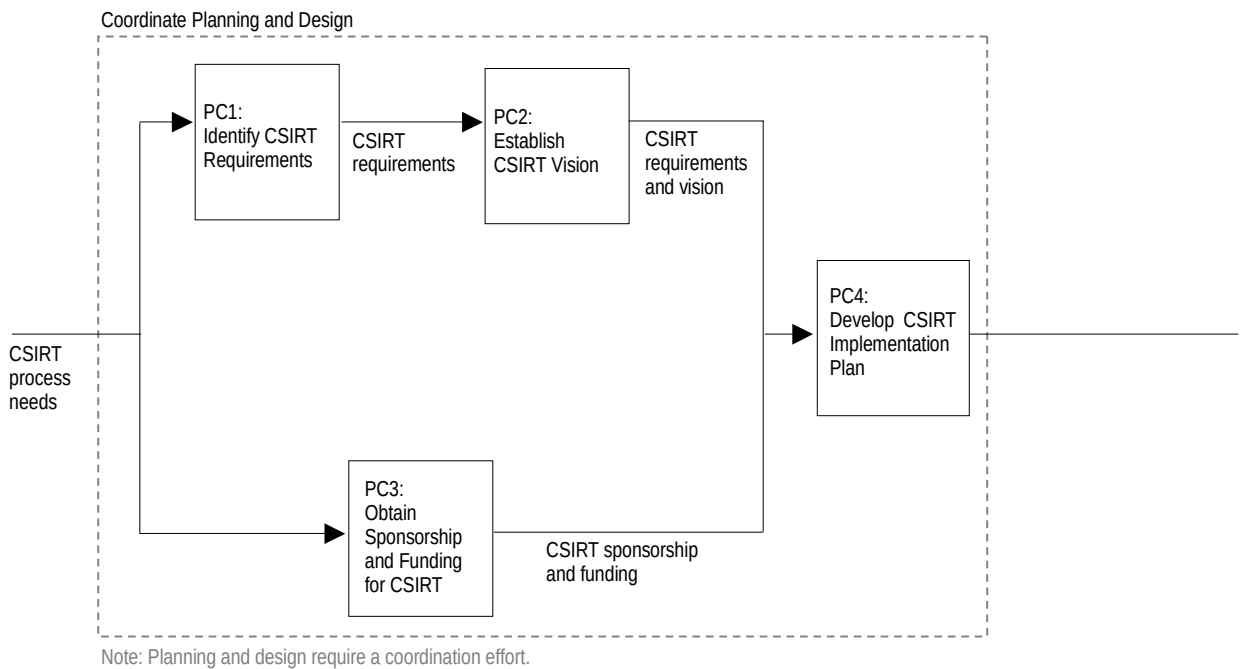
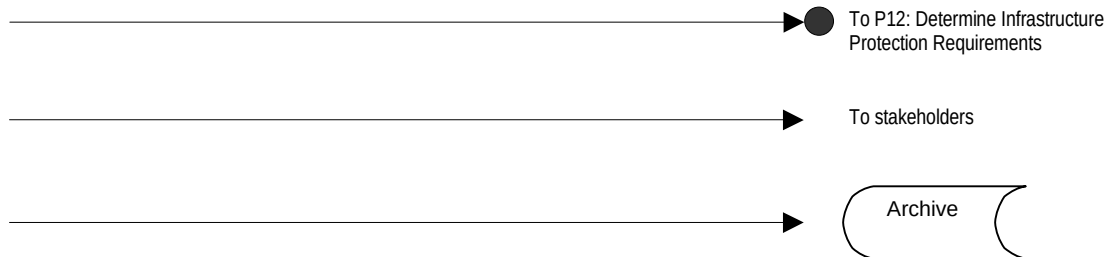
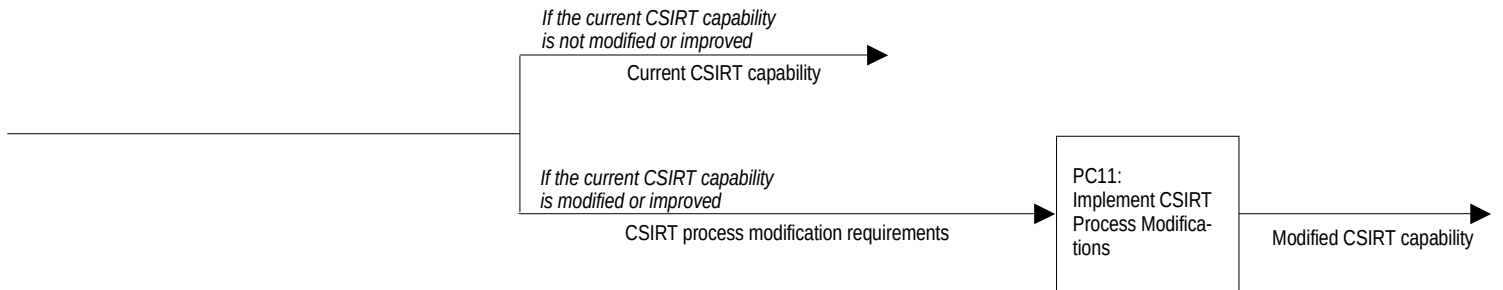
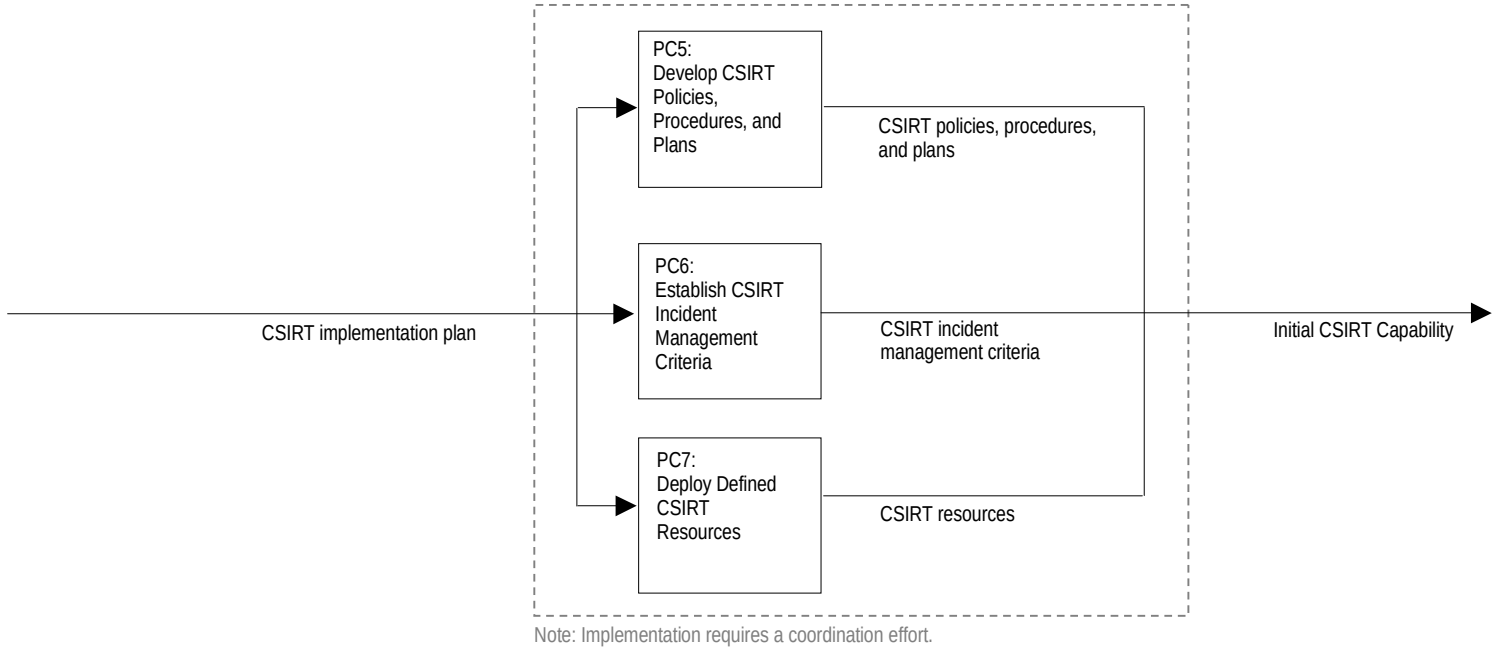


Figure 14: PC: Prepare/Sustain/Improve Workflow Diagram

Coordinate Implementation



4.2.1.2 PC: Prepare/Sustain/Improve Workflow Description

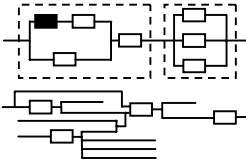
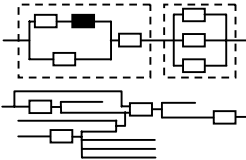
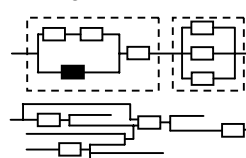
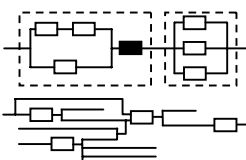
Table 6: PC: Prepare/Sustain/Improve Workflow Description

Mission/Objectives	Triggers
- To create a formalized CSIRT capability that supports the mission and goals of the constituency - To improve an existing CSIRT capability that supports the mission and goals of the constituency	- When an organizational entity decides or is mandated to create a formalized incident management capability - When an organizational entity decides or is mandated to evaluate an existing CSIRT capability - When changes or improvements to an existing CSIRT capability have been identified through means other than an evaluation (i.e., through activities within or outside of the CSIRT process)

Inputs		
Input	Description	Form
CSIRT process needs	This includes the drivers and conditions that indicate the need for a CSIRT capability when one does not currently exist. CSIRT process needs can come from a variety of sources, including local, state, federal, and international laws and regulations; relevant standards; site-security, IT, and organizational policies; general information collected as part of a CSIRT development project; and having suffered through an incident.	Verbal, electronic, or physical
Current CSIRT capability	This includes the existing resources (people, processes, and technologies) available to provide CSIRT services to a defined constituency.	People, processes, and technologies
Proposed CSIRT process changes	This includes projected modifications to an existing CSIRT process. These changes can come from many different sources, including - proposed improvements resulting from observations about where the CSIRT process has failed (from R: Respond as well as from any activity within the CSIRT process) - modifications directed by an organization's management (e.g., changes to the funding profile, decision to outsource part of the process, change in mission, new requirements, change in services) - modifications mandated by laws and regulations	Verbal, electronic, or physical
Response information	This includes all relevant response-related data required to conduct a postmortem review.	Verbal, electronic, or physical
Response actions and decisions	This includes the following data about the response: - technical, management, or legal actions taken - technical, management, or legal decisions made	Verbal, electronic, or physical

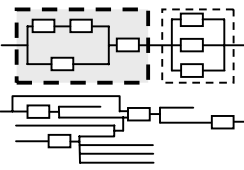
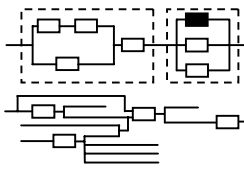
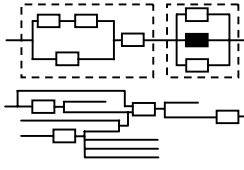
Completion Criteria	Policies and Rules	General Requirements
- When CSIRT formalized process, capability, or team is established (both short-term CSIRT operations as well as long-term CSIRT sustainment) - When CSIRT process is improved or enhanced	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Designated personnel model the CSIRT process after relevant standards, guidelines, and practices. - Designated personnel document and track results in accordance with CSIRT and organizational policies.

Outputs			
Decision	Output	Description	Form
A CSIRT capability is initially being established	Initial CSIRT capability	This includes the initial set of resources (people, processes, and technologies) required for the incident management process and deployed for that purpose. A CSIRT capability includes the following elements: - mission - constituency - set of services - defined organizational model or framework - assigned resources with designated roles and authority - appropriate equipment for performing incident management functions - secure physical and electronic infrastructures	People, processes, and technologies
The current CSIRT capability is not modified or improved	Current CSIRT capability	This includes the existing resources (people, processes, and technologies) available. There is no change to the current capability.	People, processes, and technologies
The current CSIRT capability is modified or improved	Modified CSIRT capability	This builds on the current CSIRT capability by incorporating changes identified through various means. The end result is a modified set of resources (people, processes, technologies) available to improve or modify the incident management process.	People, processes, and technologies
Improvements to the infrastructure are required	Infrastructure protection improvements	Infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure. During PC: Prepare/Sustain/Improve, these proposed improvements are identified during postmortem reviews and then forwarded to PI: Protect Infrastructure.	Verbal, electronic, or physical
Internal and external stakeholders need to be notified Archival of lessons learned is required	Lessons learned	Lessons learned are a summary of how well the incident management process worked based on how well a specific response worked. These lessons are the result of either a formal or informal review of the actions, decisions, and occurrences related to the response.	Verbal, electronic, or physical

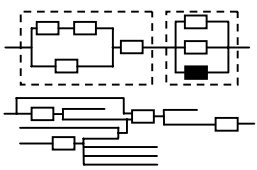
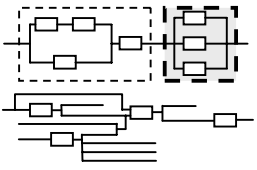
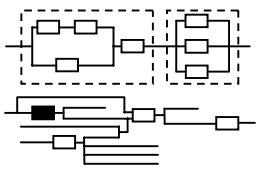
Subprocess	Subprocess Requirements	Written Procedures				
PC1: Identify CSIRT Requirements 	- Designated personnel collect and review CSIRT process needs and determine requirements for the CSIRT capability. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - CSIRT process needs* </td><td> - CSIRT requirements </td></tr></table>	Inputs	Outputs	CSIRT process needs*	CSIRT requirements	- Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when identifying CSIRT requirements. - Designated personnel follow organizational or CSIRT change management processes or guidelines.
Inputs	Outputs					
CSIRT process needs*	CSIRT requirements					
PC2: Establish CSIRT Vision 	- Designated personnel define the CSIRT vision, which includes the CSIRT mission, constituency, services, organizational framework, and resources. - Designated personnel obtain approval of CSIRT vision. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - CSIRT requirements </td><td> - CSIRT requirements and vision </td></tr></table>	Inputs	Outputs	CSIRT requirements	CSIRT requirements and vision	- Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when establishing the CSIRT vision. - Designated personnel follow organizational or CSIRT change management processes or guidelines.
Inputs	Outputs					
CSIRT requirements	CSIRT requirements and vision					
PC3: Obtain Sponsorship and Funding for CSIRT 	- Designated personnel obtain sponsorship and funding for establishing the CSIRT process. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - CSIRT process needs* </td><td> - CSIRT sponsorship and funding </td></tr></table>	Inputs	Outputs	CSIRT process needs*	CSIRT sponsorship and funding	- Designated personnel follow organizational guidelines for obtaining funding and sponsorship. - Designated personnel follow budgetary guidelines for acquiring and implementing project funding.
Inputs	Outputs					
CSIRT process needs*	CSIRT sponsorship and funding					
PC4: Develop CSIRT Implementation Plan 	- Designated personnel develop the CSIRT implementation plan. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - CSIRT requirements and vision - CSIRT sponsorship and funding </td><td> - CSIRT implementation plan </td></tr></table>	Inputs	Outputs	- CSIRT requirements and vision - CSIRT sponsorship and funding	CSIRT implementation plan	- Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when developing the CSIRT implementation plan. - Designated personnel follow organizational or CSIRT change management processes or guidelines.
Inputs	Outputs					
- CSIRT requirements and vision - CSIRT sponsorship and funding	CSIRT implementation plan					

Note: An asterisk (*) after an input to or an output of a subprocess listed in this table indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Key People	Technology	Other/Miscellaneous
- Designated personnel for identifying CSIRT requirements can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development subject matter experts (SMEs)	- Designated personnel can use the following technology when identifying CSIRT requirements: - documentation and publication technologies - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web)	---
- Designated personnel for establishing and refining the CSIRT vision can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development SMEs	- Designated personnel can use the following technology when establishing the CSIRT vision: - documentation and publication technologies - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - decision support systems	---
- Designated personnel for obtaining sponsorship and funding for CSIRT can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - CSIRT manager - CSIRT sponsor - marketing and business development staff	- Designated personnel can use the following technology when obtaining sponsorship and funding for CSIRT: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - financial and accounting systems	---
- Designated personnel for developing the CSIRT implementation plan can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development SMEs - CSIRT manager - CSIRT sponsor	- Designated personnel can use the following technology when establishing the CSIRT vision: - project planning and management software - documentation and publication technologies - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web)	---

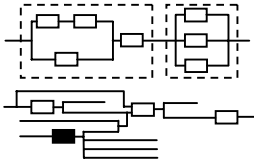
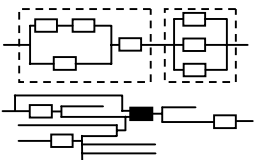
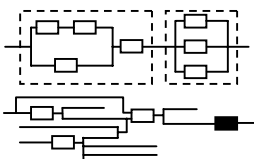
Subprocess	Subprocess Requirements	Written Procedures				
Coordinate Planning and Design 	- Designated personnel coordinate planning activities when establishing the CSIRT process. <table><tr><td>Shared Information</td></tr><tr><td> - CSIRT requirements and vision - CSIRT sponsorship and funding </td></tr><tr><td>Output</td></tr><tr><td> - CSIRT implementation plan </td></tr></table>	Shared Information	- CSIRT requirements and vision - CSIRT sponsorship and funding	Output	CSIRT implementation plan	- Designated personnel follow procedures required for identifying CSIRT requirements, establishing the CSIRT vision, obtaining sponsorship and funding for the CSIRT, and developing the CSIRT implementation plan. - Designated personnel follow appropriate procedures for coordinating the planning and design of the CSIRT capability. - Designated personnel follow organizational or CSIRT change management processes or guidelines. - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when coordinating the planning and design of the CSIRT capability.
Shared Information						
- CSIRT requirements and vision - CSIRT sponsorship and funding						
Output						
CSIRT implementation plan						
PC5: Develop CSIRT Policies, Procedures, and Plans 	- Designated personnel define core CSIRT policies, procedures, and plans consistent with the implementation plan and document the results. - Designated personnel obtain consensus and approval of CSIRT policies, procedures, and plans. <table><tr><td>Inputs</td><td>Outputs</td></tr><tr><td> - CSIRT implementation plan </td><td> - CSIRT policies, procedures, and plans </td></tr></table>	Inputs	Outputs	CSIRT implementation plan	CSIRT policies, procedures, and plans	- Designated personnel follow organizational procedures for documenting, verifying, and institutionalizing CSIRT policies, procedures, and plans. - Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when developing CSIRT policies, procedures, and plans.
Inputs	Outputs					
CSIRT implementation plan	CSIRT policies, procedures, and plans					
PC6: Establish CSIRT Incident Management Criteria 	- Designated personnel develop appropriate guidelines for supporting the CSIRT processes as specified in the implementation plan, such as - categories - priorities - triage strategies - response strategies - notification lists - escalation process <table><tr><td>Inputs</td><td>Outputs</td></tr><tr><td> - CSIRT implementation plan </td><td> - CSIRT incident management criteria </td></tr></table>	Inputs	Outputs	CSIRT implementation plan	CSIRT incident management criteria	Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when developing the CSIRT incident management criteria.
Inputs	Outputs					
CSIRT implementation plan	CSIRT incident management criteria					

Key People	Technology and Information	Other/Miscellaneous
• Designated personnel for coordinating planning and design can include – key people involved in identifying CSIRT requirements, establishing the CSIRT vision, obtaining sponsorship and funding for the CSIRT, and developing the CSIRT implementation plan	• Designated personnel can use the following technology when coordinating planning activities: – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) – documentation and publication technologies	• ---
• Designated personnel for developing CSIRT policies, procedures, and plans can include – policy and standards development staff – organizational CSIRT development project team – executive managers (i.e., any C-level manager) – business function managers – IT operations – representatives from administrative operations (e.g., legal, HR, PR, compliance) – representatives from constituency – third-party MSSP personnel – CSIRT development SMEs – CSIRT staff – technical writers	• Designated personnel can use the following technology when developing CSIRT policies, procedures, and plans: – documentation and publication technologies – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) – project planning and management software	• ---
• Designated personnel for establishing CSIRT incident management criteria can include – organizational CSIRT development project team – executive managers (i.e., any C-level manager) – business function managers – IT operations – representatives from administrative operations (e.g., legal, HR, PR, compliance) – representatives from constituency – representatives from law enforcement – representatives from critical infrastructures – third-party MSSP personnel – CSIRT development SMEs – CSIRT staff	• Designated personnel can use the following technology when establishing CSIRT incident management criteria: – documentation and publication technologies – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) – project planning and management software	• ---

Subprocess	Subprocess Requirements	Written Procedures								
PC7: Deploy Defined CSIRT Resources 	- Designated personnel identify and organize resources (e.g., staff, equipment, and infrastructure) as specified in the implementation plan when establishing the CSIRT process. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - CSIRT implementation plan </td><td> - CSIRT resources </td></tr></table>	Inputs	Outputs	CSIRT implementation plan	CSIRT resources	- Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when implementing CSIRT resources. - Designated personnel follow human resource policies and procedures for hiring and training staff. - Designated personnel follow organizational purchasing guidelines or procedures. - Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow security policies and best current practices when setting up resources, equipment, and infrastructure.				
Inputs	Outputs									
CSIRT implementation plan	CSIRT resources									
Coordinate Implementation 	- Designated personnel coordinate implementation activities when establishing the CSIRT process. <table><tr><th colspan="2">Shared Information</th></tr><tr><td colspan="2"> - CSIRT policies, procedures, and plans - CSIRT incident management criteria - CSIRT resources </td></tr><tr><th colspan="2">Output</th></tr><tr><td colspan="2"> - Initial CSIRT capability* </td></tr></table>	Shared Information		- CSIRT policies, procedures, and plans - CSIRT incident management criteria - CSIRT resources		Output		Initial CSIRT capability*		- Designated personnel follow procedures required for developing CSIRT policies, procedures, and plans, establishing CSIRT incident management criteria, and implementing CSIRT resources. - Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when coordinating the implementation of the CSIRT capability. - Designated personnel follow organizational or CSIRT change management processes or guidelines.
Shared Information										
- CSIRT policies, procedures, and plans - CSIRT incident management criteria - CSIRT resources										
Output										
Initial CSIRT capability*										
PC8: Evaluate CSIRT Capability 	- Designated personnel evaluate or assess the capability of the CSIRT and decide what to do (i.e., improve the current capability or make no improvements to the current capability). <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Current CSIRT capability* </td><td> - Current CSIRT capability* - Actions to sustain or improve a CSIRT capability </td></tr></table>	Inputs	Outputs	Current CSIRT capability*	- Current CSIRT capability* - Actions to sustain or improve a CSIRT capability	- Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when evaluating a CSIRT capability. - Designated personnel follow organizational procedures and methodologies for conducting assessments.				
Inputs	Outputs									
Current CSIRT capability*	- Current CSIRT capability* - Actions to sustain or improve a CSIRT capability									

Note: An asterisk (*) after an input to or an output of a subprocess listed in this table indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Key People	Technology and Information	Other/Miscellaneous
• Designated personnel for identifying and organizing resources can include – organizational CSIRT development project team – executive managers (i.e., any C-level manager) – business function managers – IT operations – representatives from administrative operations (e.g., legal, HR, PR, compliance) – representatives from constituency – representatives from law enforcement – representatives from critical infrastructures – third-party MSSP personnel – CSIRT development SMEs – CSIRT manager – CSIRT staff	• Designated personnel can use the following technology when identifying and organizing resources: – documentation and publication technologies – HR systems – purchasing systems – systems and networking technology required to establish and operate a CSIRT capability – physical security systems – communication channels, encrypted when appropriate (email, videoconferencing, groupware) – project planning and management software	• ---
• Designated personnel for coordinating implementation activities when establishing the CSIRT capability can include – key people involved in developing CSIRT policies, procedures, and plans, establishing CSIRT incident management criteria, and implementing CSIRT resources	• Designated personnel can use the following technology when coordinating implementation activities: – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) – documentation and publication technologies	• ---
• Designated personnel for assessing the capability of the CSIRT can include – organizational CSIRT development project team – executive managers (i.e., any C-level manager) – business function managers – representatives from constituency – third-party MSSP personnel – CSIRT development SMEs – auditors, risk management staff, compliance staff – third-party or independent evaluators	• Designated personnel can use the following technology when assessing the capability of the CSIRT: – electronic evaluation or assessment tools – report writing systems – database system – communication channels, encrypted when appropriate (email, videoconferencing, groupware) – incident tracking system – trouble ticket system	• ---

Subprocess	Subprocess Requirements	Written Procedures				
PC9: Conduct Postmortem Review 	- Designated personnel conduct a formal or informal postmortem review to determine what was learned from a response and decide if any improvements need to be implemented. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Proposed CSIRT process changes* - Response information* - Response actions and decisions* </td><td> - CSIRT process improvements - Infrastructure protection improvements* - Lessons learned* </td></tr></table>	Inputs	Outputs	- Proposed CSIRT process changes* - Response information* - Response actions and decisions*	- CSIRT process improvements - Infrastructure protection improvements* - Lessons learned*	- Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when conducting a postmortem review. - Designated personnel follow organizational or CSIRT change management processes or guidelines.
Inputs	Outputs					
- Proposed CSIRT process changes* - Response information* - Response actions and decisions*	- CSIRT process improvements - Infrastructure protection improvements* - Lessons learned*					
PC10: Determine CSIRT Process Modifications 	- Designated personnel review proposed CSIRT process changes and improvements and decide what to do with them (i.e., develop requirements to implement proposed modifications or take no further action). <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Current CSIRT capability* - CSIRT process changes* - Actions to sustain or improve a CSIRT capability - CSIRT process improvements </td><td> - Current CSIRT capability* - CSIRT process modification requirements </td></tr></table>	Inputs	Outputs	- Current CSIRT capability* - CSIRT process changes* - Actions to sustain or improve a CSIRT capability - CSIRT process improvements	- Current CSIRT capability* - CSIRT process modification requirements	- Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when determining how to modify the CSIRT capability. - Designated personnel follow organizational or CSIRT change management processes or guidelines.
Inputs	Outputs					
- Current CSIRT capability* - CSIRT process changes* - Actions to sustain or improve a CSIRT capability - CSIRT process improvements	- Current CSIRT capability* - CSIRT process modification requirements					
PC11: Implement CSIRT Process Modifications 	- Designated personnel acquire and organize resources (e.g., staff, equipment, and infrastructure) for implementing the requirements for modifying the CSIRT process. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - CSIRT process modification requirements </td><td> - Modified CSIRT capability* </td></tr></table>	Inputs	Outputs	CSIRT process modification requirements	Modified CSIRT capability*	- Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when implementing changes to the CSIRT capability. - Designated personnel follow organizational or CSIRT change management processes or guidelines. - Designated personnel follow security policies and best current practices when implementing changes to resources, equipment, and infrastructure.
Inputs	Outputs					
CSIRT process modification requirements	Modified CSIRT capability*					

Note: An asterisk (*) after an input to or an output of a subprocess listed in this table indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Key People	Technology and Information	Other/Miscellaneous
- Designated personnel for conducting a postmortem review can include - CSIRT staff - CSIRT manager - IT staff - IT manager - third parties (e.g., service providers) - business function managers - CSIRT constituency - representatives from administrative operations (e.g., legal, HR, PR, compliance) - auditors, risk management staff, compliance staff	- Designated personnel can use the following technology when conducting postmortem reviews: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - database system - incident tracking system - trouble ticket system	---
- Designated personnel for determining CSIRT process modification requirements can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development SMEs - CSIRT manager - CSIRT staff	- Designated personnel can use the following technology when determining CSIRT process modification requirements: - communication channels, encrypted when appropriate (email, videoconferencing, groupware)	---
- Designated personnel for implementing CSIRT process modifications can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development SMEs	- Designated personnel can use the following technology when implementing CSIRT process modifications: - documentation and publication technologies - HR systems - purchasing systems - systems and networking technology - physical security systems - communication channels, encrypted when appropriate (email, videoconferencing, groupware)	---

4.2.1.3 Handoff from Any Activity Inside or Outside CSIRT Process to PC: Prepare/Sustain/Improve

Table 7 describes the handoff requirements and transactions that occur when process changes and improvements are passed from any activity to the Prepare process. Process changes are proposed modifications to an existing CSIRT or incident management process. These changes can come from many different sources, including

- improvement recommendations resulting from observations about where the process has failed or where the process was successful during the handling of an incident. This type of recommendation can come from any activity within the incident management process. For example, if during the Triage process it was noted that a new policy and procedure needed to be created for escalating the handling of life-threatening incidents, this improvement recommendation could be passed on to the Prepare process. Who these recommendations are passed on to and how they are reviewed and implemented will depend on the evaluation and improvement process in place in the corresponding organization or constituency. Recommendations can also be passed directly from the Respond process. This happens when a decision is made to hold a postmortem of any incident management actions taken. This particular situation is discussed in Section 4.2.5.7, Handoff Improvements from R: Respond to PC: Prepare/Sustain/Improve.
- modifications directed by an organization's management (for example, budgetary modifications, a decision to outsource part of the process, or other similar changes). In this case, management may make a direct decision to change a process, and these changes are passed on to those responsible for making improvements to the incident management processes.
- modifications mandated by laws and regulations. Such modifications could include changes in reporting requirements or data protection requirements, or even changes in how the organization might contact and work with law enforcement. For example, implementation of FISMA, in the United States, required federal agencies to implement some type of capability for responding to computer security incidents [FISMA 02].

Implementation of any process improvements might involve many different types of people, depending on how the process is being changed and who the primary actors are who are responsible for the process. Changes might be needed in technical areas such as CSIRT or IT operations, in management units such as human resources or media relations, or in operations such as business unit functions or divisions.

Table 7 defines the sending and receiving process and the key people who might receive the process improvements.

Table 7: Handoff from Any Activity Inside or Outside CSIRT Process to PC: Prepare/Sustain/Improve

Mission/Objectives	Triggers
- To successfully send CSIRT process changes from any activity to PC: Prepare/Sustain/Improve - within defined time constraints - while handling information within the appropriate security context - while tracking the handoff in an appropriate manner	When CSIRT process changes are ready to be passed to PC: Prepare/Sustain/Improve

Processes Involved	
Sending Process	Receiving Process
Any activity	PC10: Determine CSIRT Process Modifications

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor
- Designated personnel in any activity send CSIRT process changes to designated personnel in PC: Prepare/Sustain/Improve. - Designated personnel in PC: Prepare/Sustain/Improve provide confirmation that CSIRT process changes were received. - Designated personnel in any activity and PC: Prepare/Sustain/Improve verify the integrity of transmitted CSIRT process changes.	Designated personnel follow operational procedures for sending and receiving CSIRT process changes.	Any personnel involved in the sending activity

Completion Criteria	Policies and Rules	General Requirements
- When CSIRT process changes have been sent to PC: Prepare/Sustain/Improve - When CSIRT process changes have been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Objects Being Transported/Transmitted	
Object	Description
Proposed CSIRT process changes	This includes projected modifications to an existing CSIRT process. These changes can come from many different sources, including - proposed improvements resulting from observations about where the CSIRT process has failed (from R: Respond as well as from any activity within the CSIRT process) - modifications directed by an organization's management (e.g., changes to the funding profile, decision to outsource part of the process, change in mission, new requirements, change in services) - modifications mandated by laws and regulations

Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
- Designated personnel in PC: Prepare/Sustain/Improve who receive CSIRT process changes can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development SMEs - CSIRT manager - CSIRT staff	Verbal	- Phone - Face-to-face communication	---
	Electronic	- Email - Fax - Electronic reporting system	
	Physical	Hard copy passed from one person to another	

4.2.1.4 Handoff from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure

This handoff details the requirements and transactions to send infrastructure protection improvements successfully from the Prepare to the Protect process. These infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure for the general organization or for any CSIRT that maintains its own separate network and supporting infrastructure.

There are two ways in which infrastructure protection improvements might be developed:

- During the original design of the incident management capability or CSIRT, various infrastructure and equipment requirements are implemented. This occurs in process PC7 as described in [Table 6](#), “PC: Prepare/Sustain/Improve Workflow Description.” Any special infrastructure protection specifications required to support the incident management process would be passed on to the Protect process for implementation.
- Outcomes from any postmortem review of incident activity or response actions may provide specific recommendations for improving the security of the existing infrastructure. For example, it could be discovered that a particular malicious worm or virus was able to penetrate the existing infrastructure because certain ports were not properly filtered at the firewall. Learning this from the postmortem review and then making a change to block these ports can increase the chance that a similar occurrence will not happen again.

[Table 8](#) defines the sending and receiving process and the key people who might receive the infrastructure protection improvements.

Table 8: Handoff from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure

Mission/Objectives	Triggers
- To successfully send infrastructure protection improvements from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure – within defined time constraints – while handling information within the appropriate security context – while tracking the handoff in an appropriate manner	- When the decision to improve the infrastructure is made - When infrastructure protection improvements are ready to be passed to PI: Protect Infrastructure

Processes Involved	
Sending Process	Receiving Process
PC9: Conduct Postmortem	PI2: Determine Infrastructure Protection Requirements

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor
- Designated personnel in PC: Prepare/Sustain/Improve send infrastructure protection improvements to designated personnel in PI: Protect Infrastructure. - Designated personnel in PC: Prepare/Sustain/Improve provide confirmation that infrastructure protection improvements were received. - Designated personnel in PC: Prepare/Sustain/Improve and PI: Protect Infrastructure verify the integrity of transmitted infrastructure protection improvements.	- Designated personnel follow operational procedures for reporting infrastructure protection improvements from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure. - Designated personnel follow organizational or CSIRT change management processes or guidelines. - Designated personnel follow organizational project management and implementation guidelines or procedures.	- Designated personnel in PC: Prepare/Sustain/Improve who send infrastructure protection improvement requirements can include – CSIRT staff – CSIRT manager – IT staff – IT manager – third parties (e.g., service providers) – business function managers – CSIRT constituency – representatives from administrative operations (e.g., legal, HR, PR, compliance) – auditors, risk management staff, compliance staff

Completion Criteria	Policies and Rules	General Requirements
- When infrastructure protection improvements have been sent to PI: Protect Infrastructure - When infrastructure protection improvements have been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Objects Being Transported/Transmitted	
Object	Description
Infrastructure protection improvements	Infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure. During PC: Prepare/Sustain/Improve, these proposed improvements are identified during postmortem reviews and then forwarded to PI: Protect Infrastructure.

Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
- Designated personnel in PI: Protect Infrastructure who receive infrastructure protection improvement requirements can include - IT staff (e.g., network information center (NIC) staff, network operations center (NOC) staff, security operations center (SOC) staff, system and network administrators) - third parties (e.g., MSSPs, Internet service providers [ISPs], SMEs) - auditors, risk management staff, compliance staff - CSIRT staff	Verbal	- Phone - Face-to-face communication	---
	Electronic	- Email - Fax - Electronic reporting system	
	Physical	Hard copy passed from one person to another (e.g., change management forms and reports)	

4.2.2 PI: Protect Infrastructure Process (Protect)

In today's world of rapidly spreading attacks via viruses, worms, and remote exploitations of vulnerable software, one of the most important actions an organization can take is to proactively prevent malicious activity from happening. In cases such as the Slammer or Sobig worms of 2003, the attacks happened before a normal response was possible. In situations such as this, the only true "response" is to prevent the attack from happening at all. Anything after that is really cleaning up and recovering from the propagating malicious code, or possibly stopping it from propagating further.

The Protect process in our incident management model relates to activities involved with preventing attacks from happening and mitigating the impact of those that do occur. We will take a look at the activities involved in mitigation first.

To begin with, often, as part of a response to an ongoing incident or to mitigate a discovered vulnerability, changes in the enterprise infrastructure must be made. These changes could include

- changes in filters on firewalls, routers, or mail servers to prohibit malicious packets from entering the infrastructure
- updates to IDS to include new signatures
- changes in system configurations to turn off default services
- installation of patches to vulnerable software
- updates to virus scanning software to include new signatures for new threats

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

Prevention can take many forms. It can involve

- performing security audits, vulnerability assessments, and other infrastructure evaluations to determine any weaknesses or exposure that could be exploited, resulting in successful attacks or compromises in the enterprise
- providing input from any existing CSIRT or incident management capability to those responsible for the overall development and maintenance of the infrastructure on precautions to take based on current risks and threats. Any incident management capability can be seen as a provider of authentic risk data, due to the information derived from analyzing the types of incidents and vulnerabilities they have handled in the organizational infrastructure. This information can be used to determine what protection strategies are needed.
- following standards and best practices recognized as methods for preventing and mitigating incidents and discovered vulnerabilities

This last point is basically the implementation of best practices for the protection of systems and networks based on the relevant standard of due care, be it ISO 17799 or other standards or regulatory requirements. Theoretically, improved protection of systems reduces the number of incidents that must be handled.

In this process more than any other, the crossover between incident management activities and normal security management activities is apparent. All of the above cases involve working with any existing configuration, patch, and change management systems. These are usually part of security management operations or IT operations. This highlights the importance of coordination between any of these operations and any existing CSIRT or other incident management capability. Not only is it helpful for the system and network administrators responsible for the development and maintenance of the computing infrastructure to benefit from the expertise of those involved in incident management, but conversely it is important that the CSIRT be on the receiving end of these processes to ensure that the team is sufficiently aware of infrastructure changes and to synchronize joint improvements. Also, if during an infrastructure evaluation, a new vulnerability, an ongoing incident, or the remnants of an unreported incident are discovered, this information must be passed to the Detect process as an appropriate incident or vulnerability report.

The Protect process, outlined in the workflow diagrams and descriptions that follow, contains subprocesses that describe the activities mentioned above. These include subprocesses to evaluate the current infrastructure (PI1) or receive infrastructure protection improvements from any process within the incident management functions or outside those functions. Once the infrastructure protection improvements are reviewed, the modifications that need to be made are determined (PI2) and implemented as appropriate (PI3). The implementation would include taking any actions to harden and secure the infrastructure. Such actions could include the addition of or modification to defenses such as firewalls, network monitoring, and IDS; configuration changes to hosts, servers, routers, firewalls, and other infrastructure components; or changes in policies and procedures related to acceptable use, account management, physical security, human resources, or other similar areas.

Resources available from the CERT/CC that provide more information about activities in the Protect process include

- *The CERT Guide to System and Network Security Practices*
http://www.cert.org/homeusers/cert_guide.html
- *The Challenge of Security Management*
<http://www.cert.org/archive/pdf/ESMchallenges.pdf>
- *Building a Framework for Enterprise Security Management*
http://www.cert.org/archive/pdf/secureit_esm_allen_may0304.pdf
- *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management*
<http://www.cert.org/archive/pdf/04tr010.pdf>

- *Securing Networks Systematically – the SKiP Method*
<http://www.cert.org/archive/pdf/SKiP.pdf>
- *Survivable Functional Units: Balancing an Enterprise’s Mission and Technology*
<http://www.cert.org/archive/pdf/04tn004.pdf>
- *Outsourcing Managed Security Services*
<http://www.cert.org/security-improvement/modules/omss/index.html>
- *Securing Desktop Workstations*
<http://www.cert.org/security-improvement/modules/m04.html>
- *Securing Network Services*
<http://www.cert.org/security-improvement/modules/m10.html>
- *Deploying Firewalls*
<http://www.cert.org/security-improvement/modules/m08.html>
- *Securing Public Web Servers*
<http://www.cert.org/security-improvement/modules/m11.html>
- *The OCTAVE Methodology*
<http://www.cert.org/octave/>
- *Which Best Practices Are For Me?*
http://www.cert.org/archive/pdf/secureit_bestpractices.pdf
- *The Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices*
<http://www.isalliance.org/news/requestform.cfm>

The following list is a sampling of some of the available standards and best practices that provide guidance to organizations for proactively securing and hardening the enterprise infrastructure.²⁷ Much work has been done in this area, and we do not want to repeat that work here.

- ISO 17799/British Standards Institute 7799 Part 2
- Control Objectives for Information and related Technology (COBIT)
- Federal Financial Institutions Examination Council (FFIEC) Handbooks
- International Information Systems Security Certification Consortium ((ISC)²) Certified Information Systems Security Professional (CISSP) Body of Knowledge
- Information Security Forum Best Practices
- Information Systems Security Association; Generally Accepted Information Security Principles (ISSA GAISP)
- Information Technology Governance Institute (ITGI) sources
- Information Technology Infrastructure Library (ITIL)

²⁷ Whatever standard is chosen is at the discretion of the organization.

- National Institute of Standards and Technology (NIST) (selected SP 800 series); Federal Information Processing Standards (FIPS) 199
- National CyberSummit Task Force reports (draft)
- SEI body of work including Capability Maturity Model (CMM[®]), Capability Maturity Model Integration (CMMI),²⁸ OCTAVE, the Security Knowledge in Practice (SKiPSM) method, CERT Security Practices²⁹

Related workflow diagrams, descriptions, and handoffs that detail the Protect process in the following pages include

- PI: Protect Infrastructure Workflow Diagram ([Figure 15](#))
- PI: Protect Infrastructure Workflow Description ([Table 9](#))
- Handoff from Any Activity Inside or Outside CSIRT Process to PI: Protect Infrastructure ([Table 10](#))
- Handoff from PI: Protect Infrastructure to D: Detect Events ([Table 11](#))

[®] CMM and CMMI are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

²⁸ For information on CMM or CMMI, see <http://www.sei.cmu.edu/cmm/cmms/cmms.html>.

SM SKiP is a service mark of Carnegie Mellon University.

²⁹ For information on CERT/CC Security Practices, see http://www.cert.org/nav/index_green.html.

4.2.2.1 PI: Protect Infrastructure Workflow Diagram

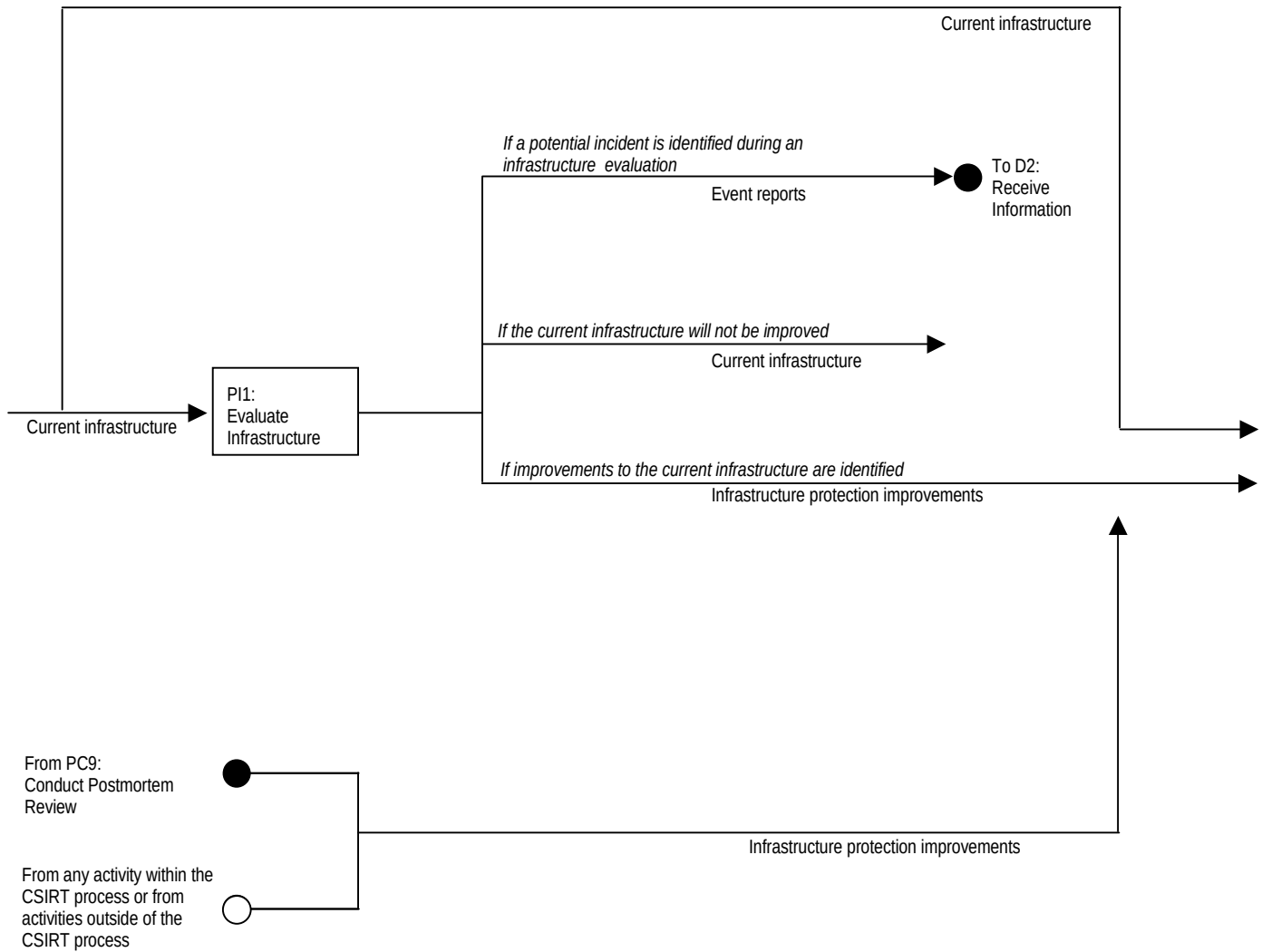


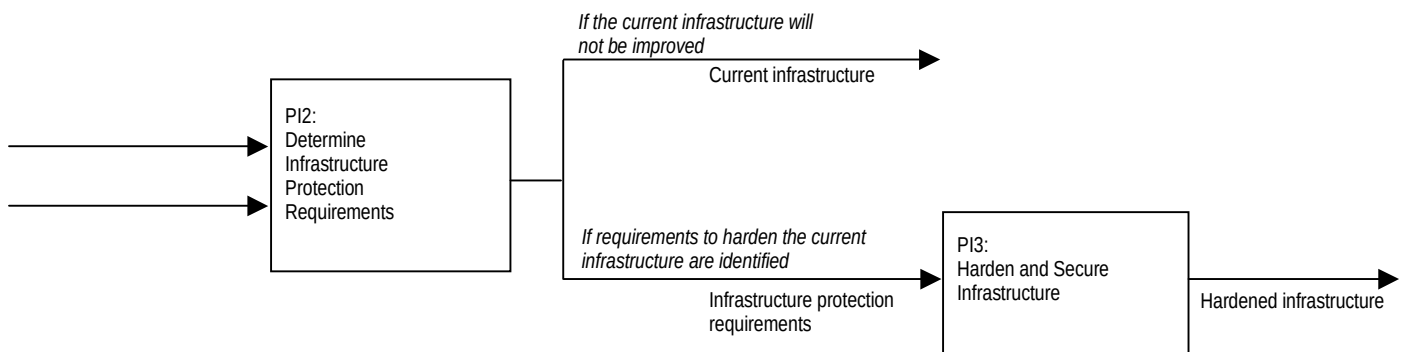
Figure 15: PI: Protect Infrastructure Workflow Diagram

Trigger 1

When the current infrastructure is evaluated, P11 is conducted. P12 and P13 may also be completed, depending on the results of the evaluation.

Trigger 2

When improvements to the current infrastructure have been identified through means other than an evaluation, processes P12 and P13 are completed.



4.2.2.2 PI: Protect Infrastructure Workflow Description

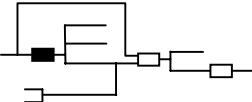
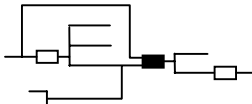
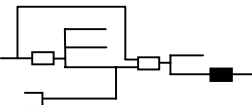
Table 9: PI: Protect Infrastructure Workflow Description

Mission/Objectives	Triggers
• To adequately protect and secure critical data and the computing infrastructure of the CSIRT and its constituency – in response to current risk, threats, attacks – in response to proposed improvements – based on a predetermined schedule – while handling information within the appropriate security context	• When lessons learned from a postmortem review of a computer security incident require improvements to the computing infrastructure • When an organizational entity decides or is mandated to evaluate, manage, and improve the security of its computing infrastructure • When improvements to the security of the computing infrastructure have been identified through means other than an evaluation (i.e., through activities within or outside of the CSIRT process)

Inputs		
Input	Description	Form
Current infrastructure	This is the existing configuration of the computing infrastructure and its susceptibility to cyber and physical attacks. <i>Note:</i> The current infrastructure comprises the people, processes, and technologies needed to support an organization's computing capability.	People, processes, and technologies
Infrastructure protection improvements	Infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure. These improvements come from many different sources, including • enhancements stemming from formal and informal postmortem reviews conducted as part of PC: Prepare/Sustain/Improve • changes resulting from observations about problems with the security of the computing infrastructure (from any activity within the CSIRT process or from activities outside of the CSIRT process) • improvements directed by mandates, best practices, standards, or an organization's management	Verbal, electronic, or physical

Completion Criteria	Policies and Rules	General Requirements
When the security of the computing infrastructure is improved or enhanced	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Designated personnel document results in accordance with organizational policies. - Designated personnel stay abreast of current methods, tools, and technologies for protecting the infrastructure.

Outputs			
Decision	Output	Description	Form
The current infrastructure is improved	Hardened infrastructure	This builds on the current infrastructure configuration by incorporating improvements identified through various means. The end result is a computing infrastructure that is less vulnerable to cyber and physical attacks. The hardened infrastructure meets or exceeds all infrastructure protection requirements.	People, processes, and technologies
The current infrastructure is not improved	Current infrastructure	This is the existing configuration of the computing infrastructure. Its susceptibility to cyber and physical attacks is unchanged. <i>Note:</i> The current infrastructure comprises the people, processes, and technologies needed to support an organization's computing capability.	People, processes, and technologies
A potential incident is identified during the evaluation	Event reports	This includes reports of unusual or suspicious activity identified during infrastructure evaluations that are forwarded to D: Detect Events.	Verbal, electronic, or physical

Subprocess	Subprocess Requirements	Written Procedures				
PI1: Evaluate Infrastructure 	- Designated personnel evaluate the computing infrastructure for vulnerability or risk and decide what to do (i.e., improve the current infrastructure, make no improvements to the current infrastructure, or send an event report to D: Detect Events when a potential incident is identified). <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Current infrastructure* </td><td> - Infrastructure protection improvements - Current infrastructure* - Event reports* </td></tr></table>	Inputs	Outputs	Current infrastructure*	- Infrastructure protection improvements - Current infrastructure* - Event reports*	- Designated personnel follow organizational procedures and methodologies for conducting vulnerability and risk assessments. - Designated personnel follow third-party best practice guidelines, procedures, standards, or regulations for protecting or securing a computing infrastructure. - Designated personnel follow organizational or CSIRT change management processes or guidelines.
Inputs	Outputs					
Current infrastructure*	- Infrastructure protection improvements - Current infrastructure* - Event reports*					
PI2: Determine Infrastructure Protection Requirements 	- Designated personnel review proposed improvements to the computing infrastructure and decide what to do with them (i.e., develop requirements to implement proposed improvements or take no further action). <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Current infrastructure* - Infrastructure protection improvements* </td><td> - Current infrastructure* - Infrastructure protection requirements </td></tr></table>	Inputs	Outputs	- Current infrastructure* - Infrastructure protection improvements*	- Current infrastructure* - Infrastructure protection requirements	- Designated personnel follow operational procedures for documenting infrastructure protection requirements. - Designated personnel follow third-party best practice guidelines, procedures, standards, or regulations for protecting or securing a computing infrastructure. - Designated personnel follow organizational or CSIRT change management processes or guidelines. - Designated personnel follow organizational criteria for prioritizing infrastructure requirements.
Inputs	Outputs					
- Current infrastructure* - Infrastructure protection improvements*	- Current infrastructure* - Infrastructure protection requirements					
PI3: Harden and Secure Infrastructure 	- Designated personnel implement appropriate infrastructure protection requirements for improving the security of the computing infrastructure. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Infrastructure protection requirements </td><td> - Hardened infrastructure* </td></tr></table>	Inputs	Outputs	Infrastructure protection requirements	Hardened infrastructure*	- Designated personnel follow operational procedures for configuring and maintaining the computing infrastructure. - Designated personnel follow third-party best practice guidelines, procedures, standards, or regulations for protecting or securing a computing infrastructure. - Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow organizational or CSIRT change management processes or guidelines.
Inputs	Outputs					
Infrastructure protection requirements	Hardened infrastructure*					

Note: An asterisk (*) after an input to or an output of a subprocess listed in this table indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Key People	Technology	Other/Miscellaneous
• Designated personnel for assessing the computing infrastructures can include – IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) – auditors, risk management staff, compliance staff – third-party or independent evaluators – CSIRT staff	• Designated personnel can use the following technology when assessing the computing infrastructures: – vulnerability assessment or scanning tools (e.g., network scanners) – risk assessment tools (e.g., decision support tools) – tracking and compliance database/archive system – communication channels (email, videoconferencing, groupware, web)	• ---
• Designated personnel for determining infrastructure protection requirements can include – IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) – third parties (e.g., MSSPs, ISPs, SMEs) – auditors, risk management staff, compliance staff – CSIRT staff	• Designated personnel can use the following technology when determining infrastructure protection requirements: – communication channels (email, videoconferencing, groupware, web)	• ---
• Designated personnel for hardening and securing the computing infrastructure can include – IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) – third parties (e.g., MSSPs, ISPs, SMEs) – CSIRT staff	• Designated personnel can use the following technology when hardening and securing the computing infrastructure: – system and network administration tools – database/archive system – communication channels (email, videoconferencing, groupware, web)	• ---

4.2.2.3 Handoff from Any Activity Inside or Outside CSIRT Process to PI: Protect Infrastructure

Generally, infrastructure protection improvements result from postmortem reviews of incident handling activities, but infrastructure protection improvements can sometimes be suggested in other parts of the incident management process or even from outside of the process. [Table 10](#) illustrates the transfer of those recommendations and suggestions to the Protect process.

Infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure. These improvements come from many different sources, including

- direct observation of a problem, flaw, or hole in the computing infrastructure that puts the infrastructure at risk to computer security threats and attacks. It is possible that this observation can occur from within any process at any time and be conveyed to the key people responsible for the corresponding part of the infrastructure. In this case, the recommendation does not have to wait until a postmortem review is done to be conveyed to the appropriate personnel. For example, in the Triage process, a message could come in from another part of the organization that has observed that certain ports are not turned off that would allow malicious activity into the infrastructure. Although this message may be passed to the Respond process for verification and evaluation, it could also be passed to those responsible for firewall maintenance. Those responsible for the firewall may evaluate the need to implement the recommendations, while those involved in the incident management process would still review the message and look for any evidence of exploitation of the open ports.
- mandates, best practices, and standards that define network and system configurations or network monitoring methods that enhance the security of the infrastructure and can prevent or mitigate malicious activity and exploitation of known vulnerabilities. These types of mandates, best practices, and standards can come from known standards bodies, computer security experts external to the organization, or even from the organization's executive management staff.

[Table 10](#) defines the sending and receiving process and the key people who might receive the infrastructure protection improvements.

Table 10: Handoff from Any Activity Inside or Outside CSIRT Process to PI: Protect Infrastructure

Mission/Objectives	Triggers
- To successfully send infrastructure protection improvements from any activity to PI: Protect Infrastructure - within defined time constraints - while handling information within the appropriate security context - while tracking the handoff in an appropriate manner	When infrastructure protection improvements are ready to be passed to PI: Protect Infrastructure

Processes Involved	
Sending Process	Receiving Process
Any activity inside or outside the CSIRT process	PI2: Determine Infrastructure Protection Requirements

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor
- Designated personnel in any activity send infrastructure protection improvements to designated personnel in PI: Protect Infrastructure. - Designated personnel in PI: Protect Infrastructure provide confirmation that infrastructure protection improvements were received. - Designated personnel in any activity and PI: Protect Infrastructure verify the integrity of transmitted infrastructure protection improvements.	Designated personnel follow operational procedures for reporting infrastructure protection improvements from any activity to PI: Protect Infrastructure.	Any personnel involved in the sending activity

Completion Criteria	Policies and Rules	General Requirements
- When infrastructure protection improvements have been sent to PI: Protect Infrastructure - When infrastructure protection improvements have been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Objects Being Transported/Transmitted	
Object	Description
Infrastructure protection improvements	Infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure. These improvements come from many different sources, including - changes resulting from observations about problems with the security of the computing infrastructure (from any activity within the CSIRT process or from activities outside of the CSIRT process) - improvements directed by mandates, best practices, standards, or an organization's management

Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
- Designated personnel in PI: Protect Infrastructure who receive infrastructure protection improvement requirements can include - IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) - third parties (e.g., MSSPs, ISPs, SMEs) - auditors, risk management staff, compliance staff - CSIRT staff	Verbal	- Phone - Face-to-face communication	---
	Electronic	- Email - Fax - Electronic reporting system	
	Physical	Hard copy passed from one person to another	

4.2.2.4 Handoff from PI: Protect Infrastructure to D: Detect Events

Part of the Protect process includes a subprocess for performing an evaluation of the infrastructure (PI1). This evaluation could include proactive security assessments such as a risk analysis, penetration testing, or vulnerability scanning. During the evaluation process, it is possible that a suspicious event or information is discovered that may indicate a security breach or other malicious activity. This handoff, as shown in [Table 11](#), describes the requirements and transactions that occur to pass the suspicious event information to the Detect Events process.

Examples of events that might be found during an evaluation could include

- artifacts such as toolkits, output from intruder tools, malicious code, or changes in configuration files indicating the compromise of a system
- strange or abnormal network activity such as broadcasts on ports identified with intruder behavior
- an unpatched vulnerability on a number of host systems
- a new vulnerability in mission-critical software

Information can be passed from Protect to Detect in a number of ways, including

- a vulnerability report
- an incident report
- a general email
- a phone call

From Detect, the information would be forwarded to Triage for assessment and then, if requiring action, to the Respond process.

Table 11: Handoff from PI: Protect Infrastructure to D: Detect Events

Mission/Objectives	Triggers
- To successfully send event reports from PI: Protect Infrastructure to D: Detect Events - within defined time constraints - while handling event reports within the appropriate security context - while tracking the handoff in an appropriate manner	- When an event has been detected during an evaluation and needs to be reported - When the event report is ready to be passed to D: Detect Events

Processes Involved	
Sending Process	Receiving Process
PI1: Evaluate Infrastructure	D2: Receive Information

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor
- Designated personnel in PI: Protect Infrastructure send event reports to designated personnel in D: Detect Events. - Designated personnel in D: Detect Events provide confirmation that event reports were received. - Designated personnel in PI: Protect Infrastructure and D: Detect Events verify the integrity of transmitted event reports.	- Designated personnel follow operational procedures for sending and receiving event reports. - Designated personnel follow any applicable special reporting procedures.	- Designated personnel in PI: Protect Infrastructure who send event reports can include - IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) - auditors, risk management staff, compliance staff - third-party or independent evaluators - CSIRT staff

Completion Criteria	Policies and Rules	General Requirements
- When event report has been sent to D: Detect Events - When event report has been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Objects Being Transported/Transmitted	
Object	Description
Event reports	This includes reports of unusual or suspicious activity to the CSIRT identified during infrastructure evaluations performed as part of PI: Protect Infrastructure. Event reports received from PI: Protect Infrastructure can include the following security-related items: specific signs of intrusion, configuration errors, and artifacts.

Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
- Designated personnel in D: Detect Events who receive event reports can include - help desk staff - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - incident handlers - information security officer - system and network administrators - third-party answering service - coordination center	Verbal	- Phone - Face-to-face communication	---
	Electronic	- Email - Fax - Electronic reporting system - Database system	
	Physical	Hard copy passed from one person to another	

4.2.3 D: Detect Events Process

The Detect process is often thought of as just the activities associated with intrusion detection or network monitoring. This is much too narrow of a definition for Detect. Detect in regards to incident management actually involves any observation of malicious or suspicious activity and any gathering of information that provides insight into current security threats or risks.

In the Detect process, information about potential incidents, vulnerabilities, or other computer security or incident management information is gathered either reactively (received from internal or external sources in the form of reports or notifications) or proactively (monitoring indicators of possible incidents or the exploitation of vulnerabilities through mechanisms such as network monitoring or IDS). The activity or information, once detected, is passed on to the Triage process as a report, alert, or similar notification.

Depending on the structure and staffing of an organization's Detect process, passing information from Detect to Triage can occur in minutes or days—it's a measure of the efficiency of the team and the maturity of their operational processes. If the same staff members perform both Detect and Triage functions, these two processes may happen almost simultaneously.

Note that there are two parallel paths for Detect in the workflow diagram in [Figure 16, D: Detect Events](#).

4.2.3.1 Reactive Detection

In reactive detection, information can be detected and reported from two main sources:

- Those using the computer facilities of the organization may notice some unusual or malicious activity and report this to the appropriate contact point. The reporting may involve submitting an incident reporting form or calling the appropriate point of contact, such as a help desk or a CSIRT hotline.
- Other computer security experts, such as an external CSIRT, coordinating CSIRT, or a security organization may send an alert or notification that must be assessed to see if there is a potential threat to the receiver's infrastructure. For example, AusCERT might receive reports of a new worm propagating in the Asia Pacific area. They would create an advisory or alert and send it out to a subscriber mailing list. Another CSIRT on this list, or even a security management team on this list, would receive the alert via email.

Staff members receive the information and reports and pass them to the Triage process (D2).

4.2.3.2 Proactive Detection

The second path requires proactive action by the designated staff to identify suspicious activity. Staff proactively monitor a variety of data (such as host logs, firewall logs, and netflows) and use intrusion detection software to monitor network behavior, looking for indications of

suspicious activity (D3). The data are analyzed and any unusual or suspicious event information is forwarded to the Triage process.

Staff performing such activity may be within or outside of a CSIRT function. Very often it is the IT operations staff that performs this function and passes on any suspicious activity or relevant incident or vulnerability information to the Triage process. In such cases it is important to have procedures already established for passing on this information. Staff doing this monitoring will have some criteria to follow to help them determine what type of alerts or suspicious activity should be passed on as a report to Triage. This occurs in process D4: Analyze Indicators, as shown in the D: Detect Events workflow diagram. If a possible event is indicated, the event information is sent to the Triage process. If the information does not indicate an event that needs action, the event is closed.

Proactive detection also includes technology watch or public monitoring functions. These activities are defined as services in *CSIRT Services* [Killcrece 02]. These services involve looking at available security resources such as mailing lists, web sites, articles, or news reports that are available publicly for free or from a commercial service for a fee. Staff performing technology watch functions can include actual CSIRT staff, network operations staff, other systems and network administrators, or even outsourced contractors. Information sought and passed to Triage could include new vulnerabilities, new attack types and threats, new recommendations and solutions for preventing incidents, or general political, social, or sector-related information that may have relevance to any ongoing or potential malicious activity.

Each organization will have its own set of guidelines and rules to determine what constitutes an incident or potential threat. These guidelines will be used to decide what will be passed on to Triage, what will be closed as no action is required, and what will be passed to another part of the organization for handling. Detect includes only the first order of information gathering. If additional information is required or further analysis is required, it is addressed in the Triage or Respond process, not in Detect.

4.2.3.3 Detect Events Details

Related workflow diagrams, descriptions, and handoffs that detail this process in the following pages include

- D: Detect Events Workflow Diagram ([Figure 16](#))
- D: Detect Events Workflow Description ([Table 12](#))
- Handoff from Any Activity Inside or Outside the Organization to D: Detect Events ([Table 13](#))
- Handoff from D: Detect Events to T: Triage Events ([Table 14](#))

Resources available from the CERT/CC that provide more information about activities in the Detect process include

- *CSIRT Services*
<http://www.cert.org/csirts/services.html>
- *Detecting Signs of Intrusion*
<http://www.cert.org/security-improvement/modules/m09.html>

4.2.3.4 D: Detect Events Workflow Diagram

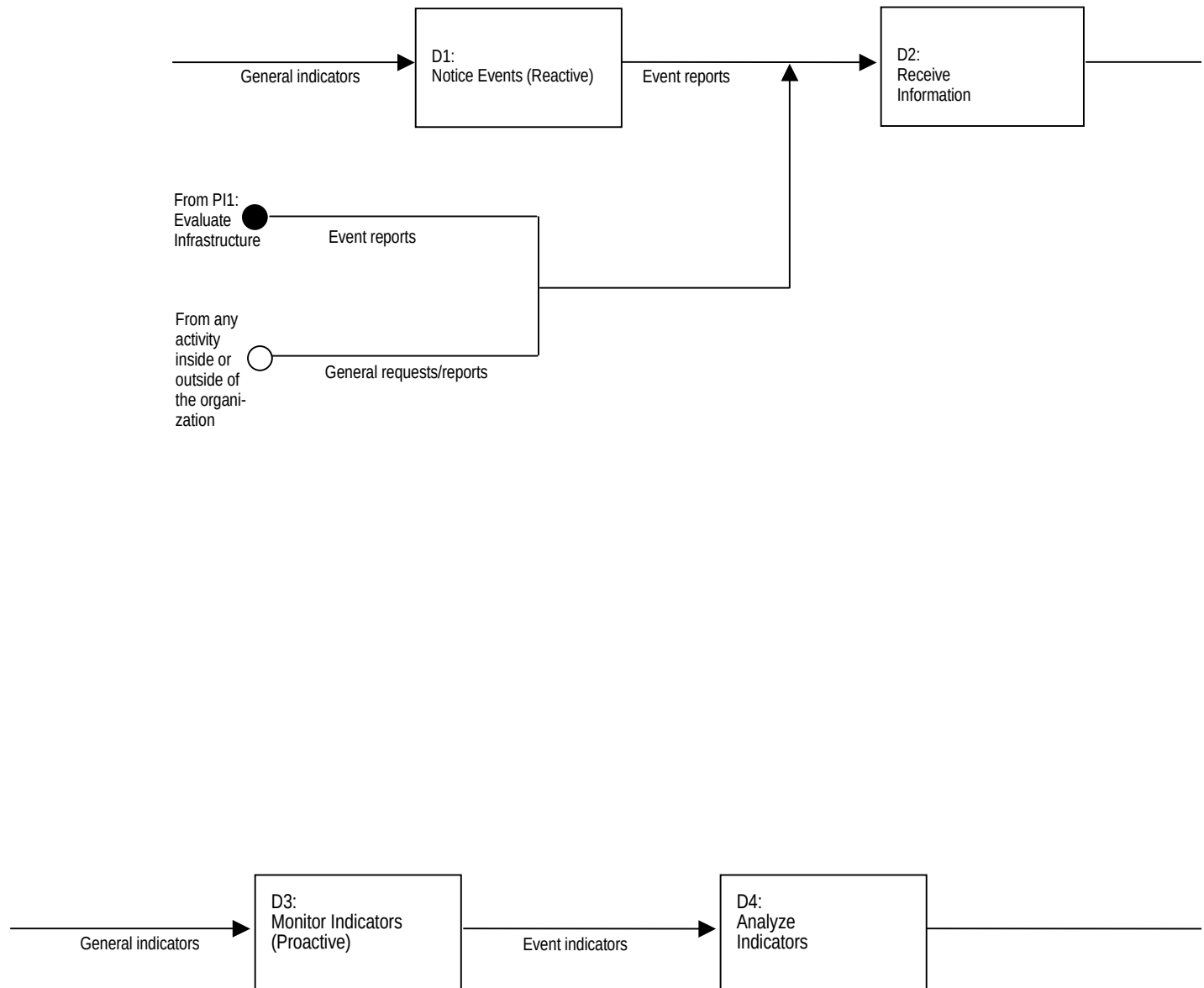
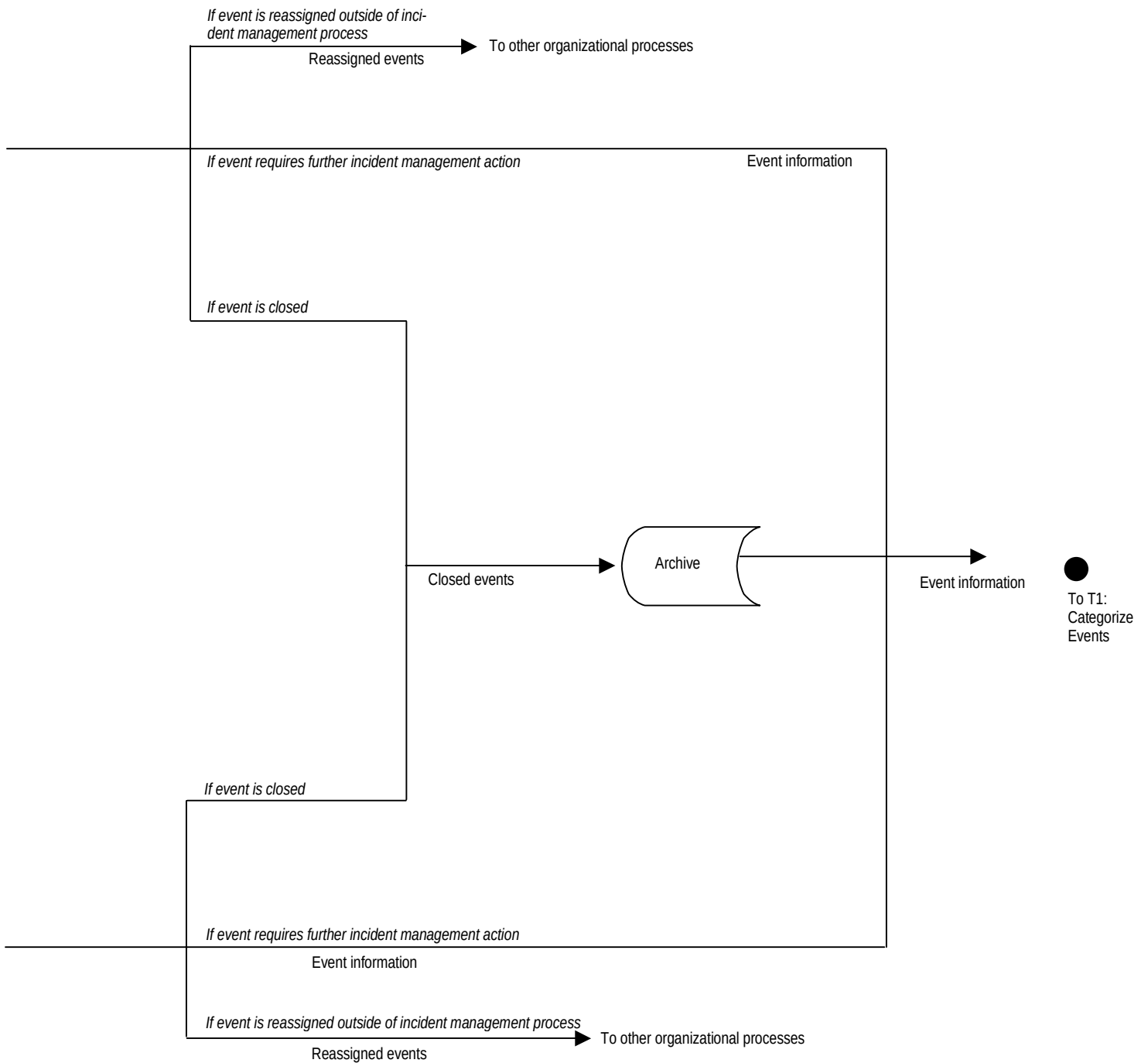


Figure 16: D: Detect Events Workflow Diagram



4.2.3.5 D: Detect Events Workflow Description

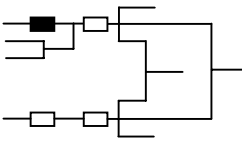
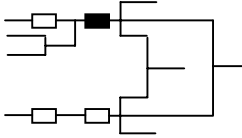
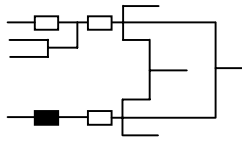
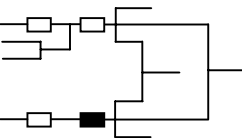
Table 12: D: Detect Events Workflow Description

Mission/Objectives	Triggers	Completion Criteria
• To identify unusual activity that might compromise the mission of the CSIRT constituency and/or the CSIRT – within defined time constraints – while handling information within the appropriate security context	• When suspicious or unusual activity is noticed • When advisories, alerts, and other information reports or requests arrive	• When a decision about an event is made (i.e., forward to T: Triage Events, reassign to other processes, or close) • When outputs are ready to be passed to the next process

Inputs		
Input	Description	Form
General indicators	This information includes the following security-related items: (1) suspicious or unusual activity noticed by internal and external sources and (2) data proactively gathered by the CSIRT, including log information, computer security news, and current events.	Verbal, electronic, or physical
Event reports	This includes reports of unusual or suspicious activity to the CSIRT identified during infrastructure evaluations performed as part of PI: Protect Infrastructure. Event reports received from PI: Protect Infrastructure can include the following security-related items: specific signs of intrusion, configuration errors, and artifacts.	Verbal, electronic, or physical
General requests/reports	This includes non-incident information (e.g., general information about CSIRT, general security questions, speaker requests).	Verbal, electronic, or physical

Policies and Rules	General Requirements
- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Designated personnel document and track results in accordance with CSIRT and organizational policies. - Periodic quality assurance checks are performed on automated tools. - Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools.

Outputs			
Decision	Output	Description	Form
Event requires further incident management action (i.e., event is sent to T: Triage Events)	Event information	This includes all information that is passed to T: Triage Events for a given event. It can include the reported information and general indicators received by D: Detect Events, any preliminary analysis performed on the information, and the decision rationale for forwarding the information to T: Triage Events.	Verbal, electronic, or physical
Event is reassigned outside of the incident management process	Reassigned events	This includes all information related to an event that has been reassigned outside of the incident handling process. It can include the reported information and general indicators received by D: Detect Events, as well as any preliminary analysis performed on the information. It can also include the rationale for reassigning the event.	Verbal, electronic, or physical
Event is closed	Closed events	This includes all information related to an event that has been closed. It can include the reported information and general indicators received by D: Detect Events, as well as any preliminary analysis performed on the information. It can also include the rationale for closing the event.	Verbal, electronic, or physical

Subprocess	Subprocess Requirements	Written Procedures				
D1: Notice Events (Reactive) 	- Designated personnel notice suspicious or unusual activity and report it to the CSIRT. - Trusted external groups send advisories and alerts to the CSIRT. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - General indicators* </td><td> - Event reports </td></tr></table>	Inputs	Outputs	General indicators*	Event reports	- Designated personnel follow incident reporting guidelines for reporting information to the CSIRT. - Trusted external groups follow operational procedures and watch procedures for reporting information to the CSIRT.
Inputs	Outputs					
General indicators*	Event reports					
D2: Receive Information 	- Designated personnel review reports, verify them, and decide what to do with them (i.e., forward to T: Triage Events, reassign to other processes, or close). - Automated tools receive reports and forward them to T: Triage Events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Event reports from D1: Notice Events - Event reports from PI: Protect Infrastructure* - General requests/ reports* </td><td> - Event information* - Reassigned events* - Closed events* </td></tr></table>	Inputs	Outputs	- Event reports from D1: Notice Events - Event reports from PI: Protect Infrastructure* - General requests/ reports*	- Event information* - Reassigned events* - Closed events*	- Designated personnel follow report collection procedures for reviewing and verifying reports and deciding what to do about them. - Designated personnel follow appropriate procedures for reassigning and closing events. - Automated tools are designed to follow report collection procedures for receiving and forwarding reports.
Inputs	Outputs					
- Event reports from D1: Notice Events - Event reports from PI: Protect Infrastructure* - General requests/ reports*	- Event information* - Reassigned events* - Closed events*					
D3: Monitor Indicators (Proactive) 	- Designated personnel proactively monitor a variety of sources for indications of potential events (e.g., log information, computer security news, current events). - Automated tools monitor systems and networks for general indicators. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - General indicators* </td><td> - Event indicators </td></tr></table>	Inputs	Outputs	General indicators*	Event indicators	- Designated personnel follow operational procedures for monitoring and reviewing general indicators. - Automated tools are designed to follow operational procedures for monitoring systems and networks for general indicators.
Inputs	Outputs					
General indicators*	Event indicators					
D4: Analyze indicators 	- Designated personnel review and analyze event indicators and decide what to do with the information (i.e., forward to T: Triage Events, reassign to other processes, or close). - Automated tools analyze event indicators and determine when to forward them to T: Triage Events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Event indicators </td><td> - Event information* - Reassigned events* - Closed events* </td></tr></table>	Inputs	Outputs	Event indicators	- Event information* - Reassigned events* - Closed events*	- Designated personnel follow operational procedures for reviewing and analyzing event indicators and deciding what to do with them. - Designated personnel follow appropriate procedures for reassigning and closing events. - Automated tools are designed to follow operational procedures for analyzing event indicators and determining when to forward them to T: Triage Events.
Inputs	Outputs					
Event indicators	- Event information* - Reassigned events* - Closed events*					

Note: An asterisk (*) after an input to or an output of a subprocess indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Key People	Technology	Other/Miscellaneous
- Designated personnel for noticing and reporting events can include - CSIRT - CSIRT constituency - victim or involved sites - general external groups (third-party reporters, MSSPs, media, law enforcement) - trusted external groups (other CSIRTs, vendors, etc.) - IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) - coordination center	- People can use the following technology when noticing and reporting events: - security tools (e.g., IDS, encryption) - desktop workstations - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web)	---
- Designated personnel for receiving reported information can include - help desk staff - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - incident handlers - information security officer - system and network administrators - third-party answering service - coordination center	- Designated personnel can use the following technology when receiving, reviewing, and deciding what to do about reported information: - security tools (whois, port number lists, encryption, etc.) - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - database system - decision support tools - Automated receiving and forwarding tools can be used to automatically receive events and forward them to T: Triage Events.	---
- Designated personnel for proactive monitoring can include - IT staff (e.g., NIC staff, NOC staff, system and network administrators) - selected members of the CSIRT staff - third parties (e.g., regulatory bodies, MSSPs, collaborators, ISPs, trusted SMEs) - coordination center	- Designated personnel can use the following technology when monitoring for general indicators: - security tools (e.g., IDS, vendor applications) - data manipulation tools - Internet search engines - communication channels, encrypted when appropriate (e.g., email, mailing lists, newsgroups, web) - database/archive system - Automated detection agents or sensors can be used to automatically monitor systems and networks for general indicators.	---
- Designated personnel for analyzing indicators can include - IT staff (e.g., NIC staff, NOC staff, system and network administrators) - selected members of the CSIRT staff - third parties (e.g., regulatory bodies, MSSPs, collaborators, ISPs, trusted SMEs) - coordination center	- Designated personnel can use the following technology when reviewing, analyzing, and deciding what to do about event indicators: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - database system - decision support tools - knowledge bases (e.g., CERT/CC, CVE³⁰) - Automated detection agents or sensors can be used to automatically analyze event indicators and determine when to forward them to T: Triage Events.	---

³⁰ Common Vulnerabilities and Exposures, <http://www.cve.mitre.org/>.

4.2.3.6 Handoff from Any Activity Inside or Outside of the Organization to D: Detect Events

This table describes the handoff requirements and transactions that occur when general requests or reports are passed from any activity inside or outside the organization to the Detect process. General requests and reports are non-incident information that may be sent to a CSIRT or incident management capability. This could include

- general information security questions
- questions dealing with CSIRT or incident management procedures, reporting requirements, organizational structure, publications, or services
- requests for speakers
- request for media interviews
- general information about newly available tools related to incident or vulnerability handling
- security conference announcements
- requests for services that may be delivered for a fee

This handoff description is necessary because, depending on services provided, an incident management capability might have issues to respond to other than reports of vulnerabilities or malicious, suspicious, or intruder activity. Handling these types of requests and reports can often consume considerable effort and should be recognized as an activity that is part of the incident management process.

Table 13 defines the sending and receiving process and the key people who might receive the general requests and reports.

Table 13: Handoff from Any Activity Inside or Outside of the Organization to D: Detect Events

Mission/Objectives	Triggers	Completion Criteria
- To successfully send general requests or reports from any activity to D: Detect Events - within defined time constraints - while handling information within the appropriate security context - while tracking the handoff in an appropriate manner	When general requests or reports are ready to be passed to D: Detect Events	- When general requests or reports have been sent to D: Detect Events - When general requests or reports have been received (optional)

Processes Involved	
Sending Process	Receiving Process
Any activity inside or outside of the organization	D2: Receive Information

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor
- Designated personnel in any activity send general requests or reports to designated personnel in D: Detect Events. - Designated personnel in D: Detect Events provide confirmation that general requests or reports were received. - Designated personnel in any activity and D: Detect Events verify the integrity of transmitted general requests or reports.	Designated personnel follow operational procedures for sending and receiving general requests or reports.	Any personnel involved in the sending activity

Policies and Rules	General Requirements
- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Objects Being Transported/Transmitted	
Object	Description
General requests/reports	This includes non-incident information (e.g., general information about CSIRT, general security questions, speaker requests).

Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
- Designated personnel in D: Detect Events who receive event reports can include the following people: - help desk staff - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - incident handlers - information security officer - system and network administrators - third-party answering service - coordination center	Verbal	- Phone - Face-to-face communication	---
	Electronic	- Email - Fax - Electronic reporting system	
	Physical	Hard copy passed from one person to another	

4.2.3.7 Handoff from D: Detect Events to T: Triage Events

The handoff shown in [Table 14](#) details the requirements and transactions to send event information successfully from the Detect process to the Triage process. Information passed includes all data for a given event, such as any incident or vulnerability reports and any general indicators showing abnormal or suspicious network or system behavior received by the Detect process, any preliminary analysis performed on the information, and the decision rationale for forwarding the information to the Triage process.

It is important to have this handoff process properly documented through policies and procedures when the Detect and Triage functions are performed by different parts of an organization (for example, if in the reactive parts of Detect, incident, vulnerability, and event reports are received by a centralized help desk and then forwarded to a CSIRT for Triage). This also holds true if proactive detection activities such as technology watch, public monitoring, network monitoring, intrusion detection, and vulnerability assessment and scanning are done by the IT operations and potential threats, malicious activity, or general computer security information that is discovered is then sent to the CSIRT for Triage.

Proper documenting of the handoff process will help to ensure that the correct information is passed and received in the most appropriate and timely manner and that all required pieces of information have been sent. A failure in this handoff could significantly delay the proper response, causing a greater impact to business operations if an ongoing incident or discovered vulnerability is not handled in a timely manner.

Table 14: Handoff from D: Detect Events to T: Triage Events

Mission/Objectives	Triggers
- To successfully send event information from D: Detect Events to T: Triage Events - within defined time constraints - while handling information within the appropriate security context - while tracking information in an appropriate manner	- When event information meets the criteria for being passed to T: Triage Events - When event information is ready to be passed to T: Triage Events

Processes Involved	
Sending Process	Receiving Process
D2: Receive Information D4: Analyze Indicators	T1: Categorize and Correlate Events

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor
- Designated personnel in D: Detect Events send event information to designated personnel in T: Triage Events. - Designated personnel in T: Triage Events provide confirmation that event information was received. - Designated personnel in D: Detect Events and T: Triage Events verify the integrity of event information.	Designated personnel follow operational procedures for sending and receiving event information.	- Personnel in D: Detect Events who send event information can include the following: - help desk staff - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - incident handlers - information security officer - system and network administrators - IT staff (e.g., NIC staff, NOC staff, system and network administrators) - third parties (e.g., answering service, regulatory bodies, MSSPs, collaborators, ISPs, trusted SMEs) - coordination center

Completion Criteria	Policies and Rules	General Requirements
- When event information has been sent to T: Triage Events - When event information has been received and its contents verified (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Periodic quality assurance checks are performed on automated tools. - Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools.

Objects Being Transported/Transmitted	
Object	Description
Event information	This includes all information that is passed from D: Detect Events to T: Triage Events for a given event. It can include the reported information and general indicators received by D: Detect Events, any preliminary analysis performed on the information, and the decision rationale for forwarding the information to T: Triage Events.

Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
- Personnel in T: Triage Events who receive event information can include the following: - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - help desk staff - incident handling staff - IT staff - information security officer - coordination center	Verbal	- Phone - Face-to-face communication	---
	Electronic	- Email - Fax - Electronic reporting system	
	Physical	- Hard copy directly handed from sender to receiver - Hard copy directly sent via mail system/courier (e.g., Express Mail)	

4.2.4 T: Triage Events (Triage) Process

Triage is the process of sorting, categorizing, correlating, prioritizing, and assigning incoming events, incident reports, vulnerability reports, and other general information requests. It can be compared to triage in a hospital, where patients who need to be seen immediately are separated from those who can wait for assistance.

Triage is an essential element of any incident management capability, particularly for any established CSIRT. Triage is on the critical path for understanding what is being reported throughout the organization. It serves as the vehicle by which all information flows into a single point of contact, allowing for an enterprise view of ongoing activity and a comprehensive correlation of all reported data. Triage allows for an initial assessment of an incoming report and queues it for further handling. It also provides a venue for beginning the initial documentation and data entry of a report or request, if this has not already been done in the Detect process.

The triage function provides an immediate snapshot of the current status of all activity reported—what reports are open or closed, what actions are pending, and how many of each type of report has been received. This process can help to identify potential security problems and prioritize the workload. Information gathered during triage can also be used to generate vulnerability and incident trends and statistics for upper management. Triage can be of particular importance when an emergency request occurs, as triage can elevate the priority of a report, escalate the handling of the report, and notify relevant parties and stakeholders, especially in the case of a critical or major event.

The Triage process involves a review of incoming information to determine its validity and to determine what type of event is being reported and what initial action to take. The initial step, Categorize and Correlate Events (T1 in the workflow diagram), uses predefined criteria, if available, to classify the incoming events. (The predefined criteria are developed by the organization.)

The classification of a request or event can involve not only determining what type of event is being reported (e.g., a denial of service, a privileged compromise, or reconnaissance activity) but also correlating the event with other events and incidents. For example, is this a new report or is this report part of an ongoing incident? Is it a known attack type or is it some new intruder methodology? If an event is determined to be part of an ongoing incident, its priority and assignment may be automatically set to be the same as that incident. In this case, the correlation actually impacts and affects the categorization, priority, and assignment of the event. Because of this relationship, these processes can occur in parallel.

If the event is not part of an ongoing incident, then after it is categorized, it is passed to the Prioritize process (T2). Certain categories of events may actually have their own predefined priorities, so again, the T1, T2, and T3 processes may occur at the same time or as part of the same process. Even if there is not an assigned priority to the category, these two processes may occur so fast that they seem to be part of the same process. Other times it may take addi-

tional analysis to determine the priority. The same can be said for the Assign process (T3); assignments may be made based on the category or priority of the event or on current workload or existing CSIRT expertise.

If information is notable or suspicious, it is assigned to someone in the Respond process and passed on to that process. It should be noted that the categorization and priority, as well as the assignment, might be changed when the event is analyzed in the Respond process.

Although in these process workflows we have separated Triage into its own process, we have observed that Triage can occur at the same time as Detect. Whether it does depends on the personnel performing each function and the organizational structure that supports this incident management function.

Triage can be performed by a wide range of key personnel. Who performs it depends on the staff and job assignments within the incident management functions and across the organization. It also depends on the level of service provided by the Triage staff. For example, we have seen some organizations in which event reports come to an information security officer, who categorizes and prioritizes the event and contacts the appropriate personnel in the CSIRT to handle the event. In very small CSIRTs, it may be the CSIRT manager who receives the event report and who performs the triage functions. In a large multinational organization, it may be local IT help desks that receive the event information for triage. In a national CSIRT it may be dedicated CSIRT staff that performs triage.

Most important to how well Triage is executed is the expertise and skill level of the Triage staff. Triage is difficult to implement in an effective manner. Some organizations have devoted a lot of support and training to Triage, and they perform a higher level of analysis, a strategic assessment of the situation, rather than a tactical sorting of the information received. Depending on what role Triage plays in your incident management process—strategic or tactical—a different set of knowledge and skills is needed. Often Triage is assigned to a junior help desk person or a technician. Such a person may not have the required knowledge and skill to perform a true assessment of the situation. In that case, the assessment is done in the Respond process, and Triage is used simply to sort, categorize, and assign the initial report.

If Triage is built to perform a true assessment function, staff must have the right mix of technical skills and business awareness. Business awareness means understanding the mission and purpose of the parent organization, understanding what systems and assets are critical to the achievement of this mission, and being able to determine what affect threats, malicious activity, and exploitation of vulnerabilities in the computing infrastructure will have on the overall operation of the business. Having business awareness enables staff to determine the true impact to the organization in the Triage process, which can decrease the time to respond to the event or incident.

If Triage is performed outside of a CSIRT, particular attention must be paid to how the information is transferred to the CSIRT and what type of training is provided for those staff performing triage, so that they know what information should be passed to the CSIRT and in

what format it should be passed. This is a key handoff interaction that, if done improperly, can cause a delayed response that can increase the amount of damage and impact resulting from an incident or delay further investigation of a report because it was not received in a timely manner.

Resources available from the CERT/CC that provide more information about activities in the Triage process include

- *CSIRT Services*
<http://www.cert.org/csirts/services.html>
- *The Handbook for CSIRTs*
<http://www.cert.org/archive/pdf/csirt-handbook.pdf>
- *Organizational Models for CSIRTs*
<http://www.cert.org/archive/pdf/03hb001.pdf>

Various courses are also offered by the CERT/CC that contain modules on this topic. You can find information about these courses at http://www.cert.org/nav/index_gold.html.

Related workflow diagrams, descriptions, and handoffs that detail this process in the following pages include

- T: Triage Events Workflow Diagram ([Figure 17](#))
- T: Triage Events Workflow Description ([Table 15](#))
- Handoff from T: Triage Events to R: Respond ([Table 16](#))

4.2.4.1 T: Triage Events Workflow Diagram

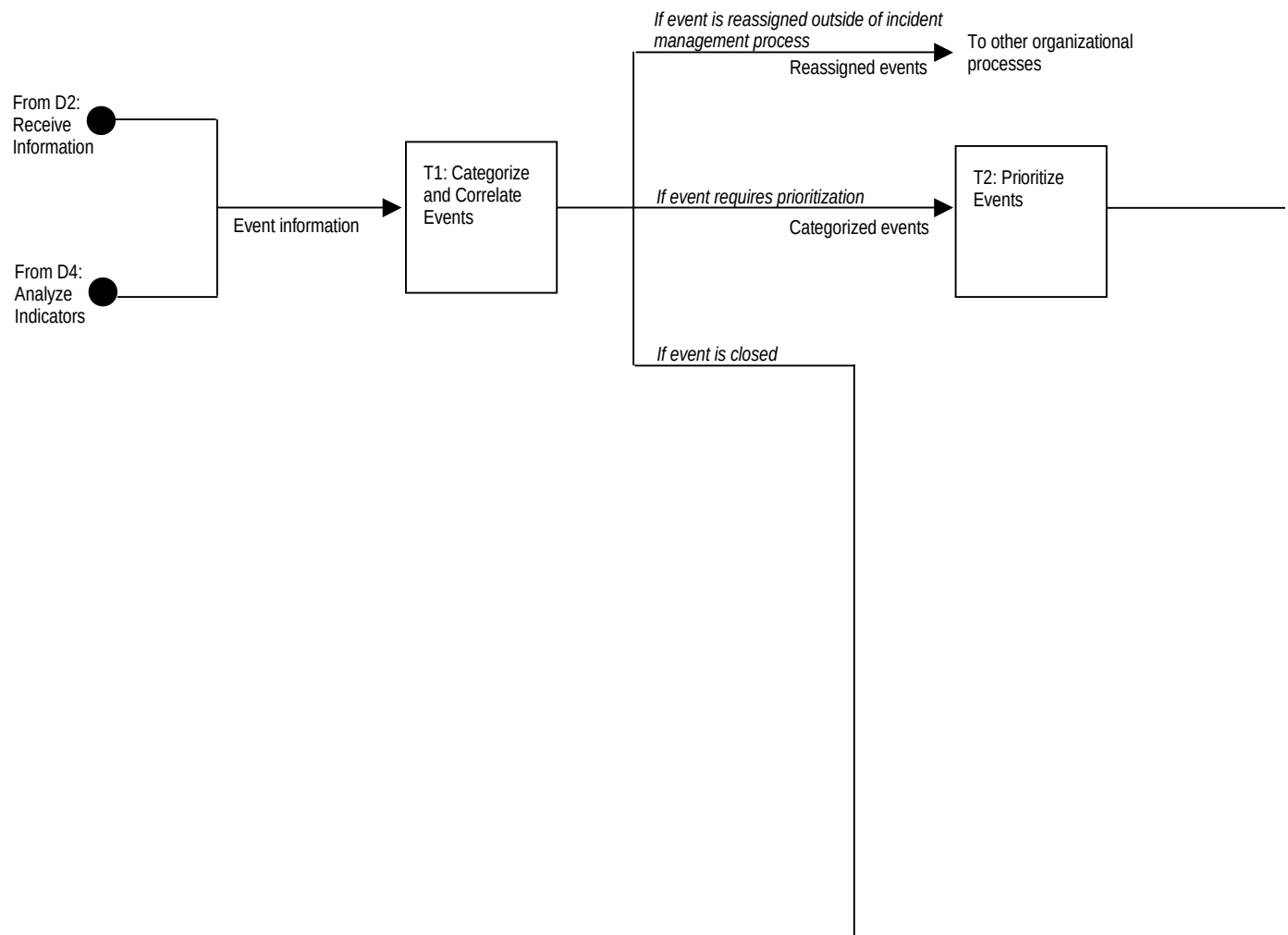
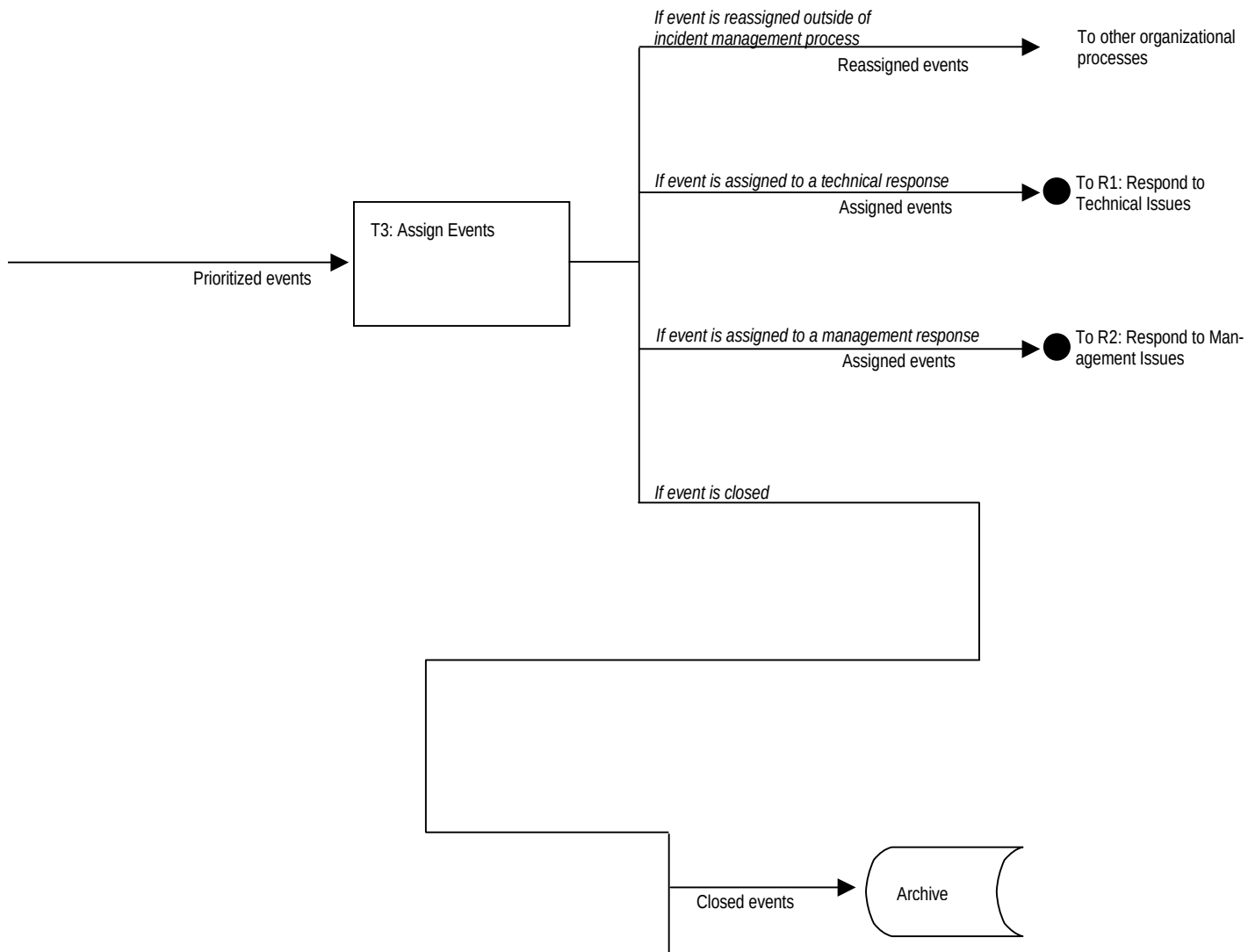


Figure 17: T: Triage Events Workflow Diagram



4.2.4.2 T: Triage Events Workflow Description

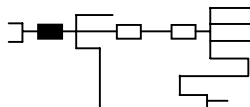
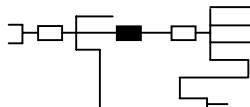
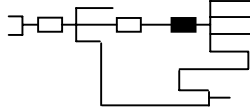
Table 15: T: Triage Events Workflow Description

Mission/Objectives	Triggers
• To sort event information and assign it to appropriate personnel – within defined time constraints – while handling information within the appropriate security context – while documenting information in an appropriate manner	• When event information arrives

Inputs		
Input	Description	Form
Event information	This includes all information that is passed to T: Triage Events from D: Detect Events. It can include reported information and general indicators, general requests and reports, any preliminary analysis performed on the information, and the decision rationale for forwarding the information to T: Triage Events.	Verbal, electronic, or physical

Completion Criteria	Policies and Rules	General Requirements
When events have been categorized, prioritized, assigned, closed, or reassigned	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- When an event is part of an incident that has previously been closed, designated personnel can reopen the closed incident if appropriate. - Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel document and track results in accordance with CSIRT and organizational policies. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Periodic quality assurance checks are performed on automated tools. - Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools.

Outputs			
Decision	Output	Description	Form
Event is assigned to a technical or management response	Assigned events	This includes all information that is passed to R: Respond for a given event. It can include event information received by T: Triage Events, the event's category and priority, and assigned responsibility for incident handling. Some events may be identified as incidents during T: Triage Events, while other events are passed to R: Respond for further evaluation.	Verbal, electronic, or physical
Event is reassigned outside of the incident management process	Reassigned events	This includes all information related to an event that has been reassigned outside of the incident handling process. It can include event information received by T: Triage Events, as well as the decision rationale for reassigning the information.	Verbal, electronic, or physical
Event is closed	Closed events	This includes all information related to an event that has been closed. It can include event information received by T: Triage Events, as well as the rationale for closing the event.	Verbal, electronic, or physical

Subprocess	Subprocess Requirements	Written Procedures				
T1: Categorize and Correlate Events 	- Designated personnel review event information against predefined categorization criteria and decide what to do with it (i.e., forward to T2: Prioritize Events, reassign to other groups, or close). - Designated personnel review event information to determine whether it is a new or ongoing event and whether it correlates with other reported information. - If an event's category cannot be determined using predefined criteria, designated personnel review information related to the event and determine its category, consulting with others as needed. - Automated tools use predefined criteria to categorize events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Event Information* </td><td> - Categorized Events - Reassigned Events* - Closed Events* </td></tr></table>	Inputs	Outputs	Event Information*	- Categorized Events - Reassigned Events* - Closed Events*	- Designated personnel follow triage procedures for categorizing and correlating events. - Designated personnel use predefined categorization criteria when categorizing events. - Designated personnel follow appropriate procedures for reassigning and closing events. - Automated tools are designed to follow triage procedures for categorizing events. - Automated tools use predefined criteria when categorizing events.
Inputs	Outputs					
Event Information*	- Categorized Events - Reassigned Events* - Closed Events*					
T2: Prioritize Events 	- Designated personnel review categorized events against predefined prioritization criteria and determine the priority of each event. - If an event's priority cannot be determined using predefined criteria, designated personnel review information related to the event and determine its priority, consulting with others as needed. - Automated tools use predefined criteria to prioritize events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Categorized Events </td><td> - Prioritized Events </td></tr></table>	Inputs	Outputs	Categorized Events	Prioritized Events	- Designated personnel follow triage procedures for prioritizing events. - Designated personnel use predefined prioritization criteria when prioritizing events. - Automated tools are designed to follow triage procedures for prioritizing events. - Automated tools use predefined criteria when prioritizing events.
Inputs	Outputs					
Categorized Events	Prioritized Events					
T3: Assign Events 	- Designated personnel review prioritized events against assignment guidelines and decide what to do with them (i.e., forward to R: Respond, reassign to other groups, or close). - If assignment guidelines do not indicate where to assign an event, designated personnel review information related to the event and assign it to the appropriate parties, consulting with others as needed. - Automated tools use predefined criteria to assign events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Prioritized Events </td><td> - Assigned Events* - Reassigned Events* - Closed Events* </td></tr></table>	Inputs	Outputs	Prioritized Events	- Assigned Events* - Reassigned Events* - Closed Events*	- Designated personnel follow triage procedures for assigning events. - Designated personnel follow assignment guidelines when assigning events (e.g., work schedule rotations, functional expertise, load balancing). - Designated personnel follow appropriate procedures for reassigning and closing events. - Automated tools are designed to follow triage procedures for assigning events. - Automated tools use predefined criteria when assigning and closing events.
Inputs	Outputs					
Prioritized Events	- Assigned Events* - Reassigned Events* - Closed Events*					

Note: An asterisk (*) after an input to or an output of a subprocess indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Key People	Technology	Other/Miscellaneous
• Designated personnel for categorizing and correlating events can include – CSIRT triage staff – CSIRT hotline staff – CSIRT manager – help desk staff – incident handling staff – IT staff – information security officer – coordination center	• Designated personnel can use the following technology when categorizing and correlating events: – incident handling database/tracking system – trouble ticket system – decision support tools (e.g., checklists, automated systems, other databases) – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) • Automated triage tools can be used to automatically categorize events.	• ---
• Designated personnel for prioritizing events can include – CSIRT triage staff – CSIRT hotline staff – CSIRT manager – help desk staff – incident handling staff – IT staff – information security officer – coordination center	• Designated personnel can use the following technology when prioritizing events: – incident handling database/tracking system – trouble ticket system – decision support tools (e.g., checklists, automated systems, other databases) – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) • Automated triage tools can be used to automatically prioritize events.	• ---
• Designated personnel for assigning events can include – CSIRT triage staff – CSIRT hotline staff – CSIRT manager – help desk staff – incident handling staff – IT staff – information security officer – coordination center	• Designated personnel can use the following technology when assigning events: – incident handling database/tracking system – trouble ticket system – decision support tools (e.g., checklists, automated systems, other databases) – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) • Automated triage tools can be used to automatically assign and close events.	• ---

4.2.4.3 Handoff from T: Triage Events to R: Respond

This handoff details the requirements and transactions to successfully send assigned events from the Triage process to the Respond process. It includes all information that is passed to the Respond process for a given event. That information can include

- any event or incident information. For example, if a report was sent to Triage of a worm propagating through a segment of an organization's network, and that report included network logs of the malicious activity and a copy of the malicious code, all of that information would be passed on to the Respond process for analysis, mitigation, and response.
- any descriptive information added in the Triage process such as the event's category, priority, and assigned responsibility for incident handling. This can also include any information discovered by correlating the incoming event report with other past or current reports. For example, if this is the tenth report of the same propagating worm, the number of reports and the reported damage would also be passed on to the Respond process.

Some events may be identified as incidents during Triage, while other events are passed to the Respond process for further evaluation before being categorized as incidents.

If Triage is performed by different staff than those performing the corresponding Respond process, particular attention must be paid to how the information is transferred between the two processes. Appropriate training must be provided for staff performing triage so they know what information should be passed to the Respond process and in what format it should be passed.

This handoff is a key interaction that, if done improperly, can cause a delayed response that can increase the amount of damage and impact resulting from an incident.

Note that the workflow description in [Table 16](#) on page 124 details four different types of handoffs, depending on whether the actor is a person or an automated tool, such as an automated triage tool or an automated response tool. The four types of handoffs are

- person to person – The receiving and sending actors are both people, even if they are using technology such as email or an assignment function in a help ticket tool to do the information transfer.
- technology to person – The sending actor is actually an automated tool, which reads and reviews incoming reports or mail and makes assignments based on predefined criteria such as functional expertise or workload balancing.
- technology to technology – The sending and receiving actors are both automated tools.
- person to technology – The sending actor is a person forwarding the information or report to an automated response tool (some type of automated self-healing system tool performing some response functions, for example).

It's possible that the handoff might use more than one of these methods of transfer depending on the type of report or request and the organizational structure.

Table 16: Handoff from T: Triage Events to R: Respond

Mission/Objectives	Triggers
- To send assigned events successfully from T: Triage Events to R: Respond - within defined time constraints - while handling information within the appropriate security context - while tracking information in an appropriate manner	- When assigned events meet the criteria for being passed to R: Respond - When assigned events are ready to be passed to R: Respond

Processes Involved	
Sending Process	Receiving Process
T3: Assign Events	R1: Respond to Technical Issues R2: Respond to Management Issues

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor
- Designated personnel in T: Triage Events send assigned events to designated personnel in R: Respond. - Designated personnel in R: Respond provide confirmation that assigned events were received. - Designated personnel in T: Triage Events and R: Respond verify the integrity of event information.	Designated personnel follow operational procedures for sending and receiving assigned events.	- Designated personnel in T: Triage Events who send assigned events can include - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - help desk staff - incident handling staff - IT staff - information security officer - coordination center

Completion Criteria	Policies and Rules	General Requirements
- When assigned events have been sent to T: Triage Events - When assigned events have been received and their content verified (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Periodic quality assurance checks are performed on automated tools. - Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools.

Objects Being Transported/Transmitted	
Object	Description
Assigned events	This includes all information that is passed to R: Respond for a given event. It can include event information received by T: Triage Events, the event's category and priority, and assigned responsibility for incident handling. Some events may be identified as incidents during T: Triage Events, while other events are passed to R: Respond for further evaluation.

Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
- Designated personnel in R: Respond who receive assigned events can include - CSIRT staff - CSIRT manager - IT staff (system and network administrators) - security staff (physical and cyber) - information security officer - upper management of the CSIRT constituency, business and functional units, IT management, etc. - CSIRT manager - HR staff - PR staff - coordination center	Verbal	- Phone - Face-to-face communication	---
	Electronic	- Email - Fax - Incident tracking system - Electronic reporting system	
	Physical	Hard copy directly handed from sender to receiver	

Technology-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor
- Automated tools from T: Triage Events send assigned events to designated personnel in R: Respond. - Designated personnel in R: Respond review assigned events for completeness and reasonableness.	- Automated tools are designed to follow operational procedures for sending and receiving assigned events. - Designated personnel follow operational procedures for sending and receiving assigned events.	Automated tools from T: Triage Events send assigned events.	- Designated personnel in R: Respond who receive assigned events can include - CSIRT staff - CSIRT manager - IT staff (system and network administrators) - security staff (physical and cyber) - information security officer - coordination center

Technology-to-Technology Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor
- Automated tools from T: Triage Events send assigned events to automated tools from R: Respond. - Automated tools send assigned events via verifiable means (e.g., TCP/IP).	Automated tools are designed to follow operational procedures for sending and receiving assigned events.	Automated tools from T: Triage Events send assigned events.	Automated tools from R: Respond receive assigned events.

People-to-Technology Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor
- Designated personnel in T: Triage Events send assigned events to automated tools from R: Respond. - Automated tools from R: Respond provide confirmation that assigned events were received.	- Designated personnel follow operational procedures for sending and receiving assigned events. - Automated tools are designed to follow operational procedures for sending and receiving assigned events.	- Designated personnel in T: Triage Events who send assigned events can include - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - help desk staff - incident handling staff - IT staff - information security officer - coordination center	Automated tools from R: Respond receive event information.

Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
Electronic	- Email - Incident tracking system - Electronic reporting system (automated incident reporting system)	---

Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
Electronic	Tool-to-tool interface	---

Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
Electronic	- Email - Electronic reporting interface	---

4.2.5 R: Respond Process

The Respond process includes the steps taken to address, resolve, or mitigate an event or incident. We have defined three types of response activities: technical, management, and legal. These three types of activities can happen simultaneously, but for the most effective response they should happen in a coordinated function with members from all response areas coordinating the planning and execution of the response activities. Where possible and appropriate, information should be shared across these subprocesses. This coordination aspect is noted on the workflow diagram by the large dotted box around the three response paths (see [Figure 18](#)). It should also be noted that communication with external entities to obtain advice or guidance or to report an incident or vulnerability to another entity, such as a national CSIRT or a Critical Infrastructure Reporting Center or Information Sharing and Analysis Center (ISAC), is designated by the arrows going to and from the Coordination dotted line and the box titled “External Communication with Others.”

Although each of the three subprocesses involves different people with different skills and expertise, the basic steps followed in each process are similar.

4.2.5.1 Technical Response

This response focuses on the actions taken by the technical staff to analyze and resolve an event or incident. Technical staff can include CSIRT staff such as incident, artifact, and vulnerability handlers, as well as other technical staff internal and external to the organization, such as system and network administrators, other members of IT operations, external security experts, or members of other CSIRTs as appropriate. Technical response actions taken can include

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

Depending on the scope of the event or incident being handled, actions in the Respond process may be performed by a variety of people. For example, a CSIRT may perform correlating or analysis activities and provide guidance on incident activity but not be involved in the monitoring or maintenance of infrastructure components. The CSIRT may also make recommendations to IT operations for changes in the infrastructure. IT staff members then make

those changes. But as all actions are in response to ongoing incident activity, all the actions are considered part of the incident management process.

4.2.5.2 Management Response

Management response highlights activities that require some type of supervisory or management intervention, notification, interaction, escalation, or approval as part of any response that is undertaken. Such management involvement may include actions taken by executive management or functional managers. Administrative or management support activities are also included in management response. These include areas of an organization such as human resources, public relations, financial accounting, audits and compliance, and other internal organizational entities.

Management response activities might include contacting legal counsel for advice regarding the liability related to an organizational network computing system being used to attack an external entity, or having human resources remove an employee found to be performing illegal activity on the organizational network. Management response can also involve ensuring that various parts of the organization work together to handle events and incidents and resolving any problems that occur between different parts of the organization.

4.2.5.3 Legal Response

Legal response includes actions associated with incident activity that relate to investigation; prosecution; liability; copyright and privacy issues; interpretation of legal rulings, laws, and regulations; non-disclosures; and other information disclosure agreements. The legal response can be initiated only by management.³¹ This process has been mapped separately because it includes steps and activities that may be outside the domain and expertise of the incident management technical staff. These tasks involve activities such as legal prosecution, computer forensics, and determination of legal liability. Each of these requires skills, training, and procedures that are different from those required for other incident handling functions. Also, some legal response tasks can take longer to resolve than other incident response tasks, since they may involve court proceedings that could take months or years to complete. For these reasons, we believe that legal response deserves its own level of process maps.

4.2.5.4 Coordination of Response Activities

Coordination must occur across all three areas of the Respond process for the process to be efficient and effective. This means that all those involved in the response must communicate the steps that are being taken and any relevant information. It also means that during a particular type of response (a technical response, for example), a need may be seen to get management or legal staff involved. This type of cooperation and coordination should occur through established channels of communication that should be outlined in the policies, pro-

³¹ At the time of this publication, we had not as yet expanded legal response into the third level. That is why it does not resemble the technical and management response workflows.

cedures, and plans associated with the Respond process. Actions must be coordinated to ensure that duplicate effort does not occur and that all tasks are completed within agreed-upon timeframes. Sometimes all three processes will be initiated to resolve an incident and sometimes only one or two of the processes will be required. However many are activated, some type of leader or project coordinator for the Respond process is needed to ensure that all the appropriate tasks are being performed across all the response actors.

Resources available from the CERT/CC that provide more information about actions that can be taken in the Respond process include

- *The Handbook for CSIRTs*
<http://www.cert.org/archive/pdf/csirt-handbook.pdf>
- *The State of the Practice of CSIRTs*
<http://www.cert.org/archive/pdf/03tr001.pdf>
- *CSIRT Services*
<http://www.cert.org/csirts/services.html>
- *Responding to Intrusions*
<http://www.cert.org/security-improvement/modules/m06.html>
- *Steps for Recovering from a UNIX or Windows System Compromise*
http://www.cert.org/tech_tips/win-UNIX-system_compromise.html
- *Dealing with External Computer Security Incidents*
<http://www.cert.org/archive/pdf/external-incidents.pdf>
- *Tracking and Tracing Cyber Attacks: Technical Challenges and Global Policy Issues*
<http://www.cert.org/archive/pdf/02sr009.pdf>
- *Managing the Threat of Denial-of-Service Attacks*
http://www.cert.org/archive/pdf/Managing_DoS.pdf

Various courses are also offered by the CERT/CC that contain modules on this topic. You can find information about these courses at http://www.cert.org/nav/index_gold.html.

Related workflow diagrams, descriptions, and handoffs that detail this process in the following pages include

- R: Respond Workflow Diagram ([Figure 18](#))
- R: Respond Workflow Description ([Table 17](#))
- Handoff from R: Respond to PC: Prepare/Sustain/Improve ([Table 18](#))
- R1: Respond to Technical Issues Workflow Diagram** ([Figure 19](#))
- R2: Respond to Management Issues Workflow Diagram** ([Figure 20](#))
- R3: Respond to Legal Issues Workflow Diagram** ([Figure 21](#))

**No corresponding workflow descriptions have yet been done for these diagrams.

4.2.5.5 R: Respond Workflow Diagram

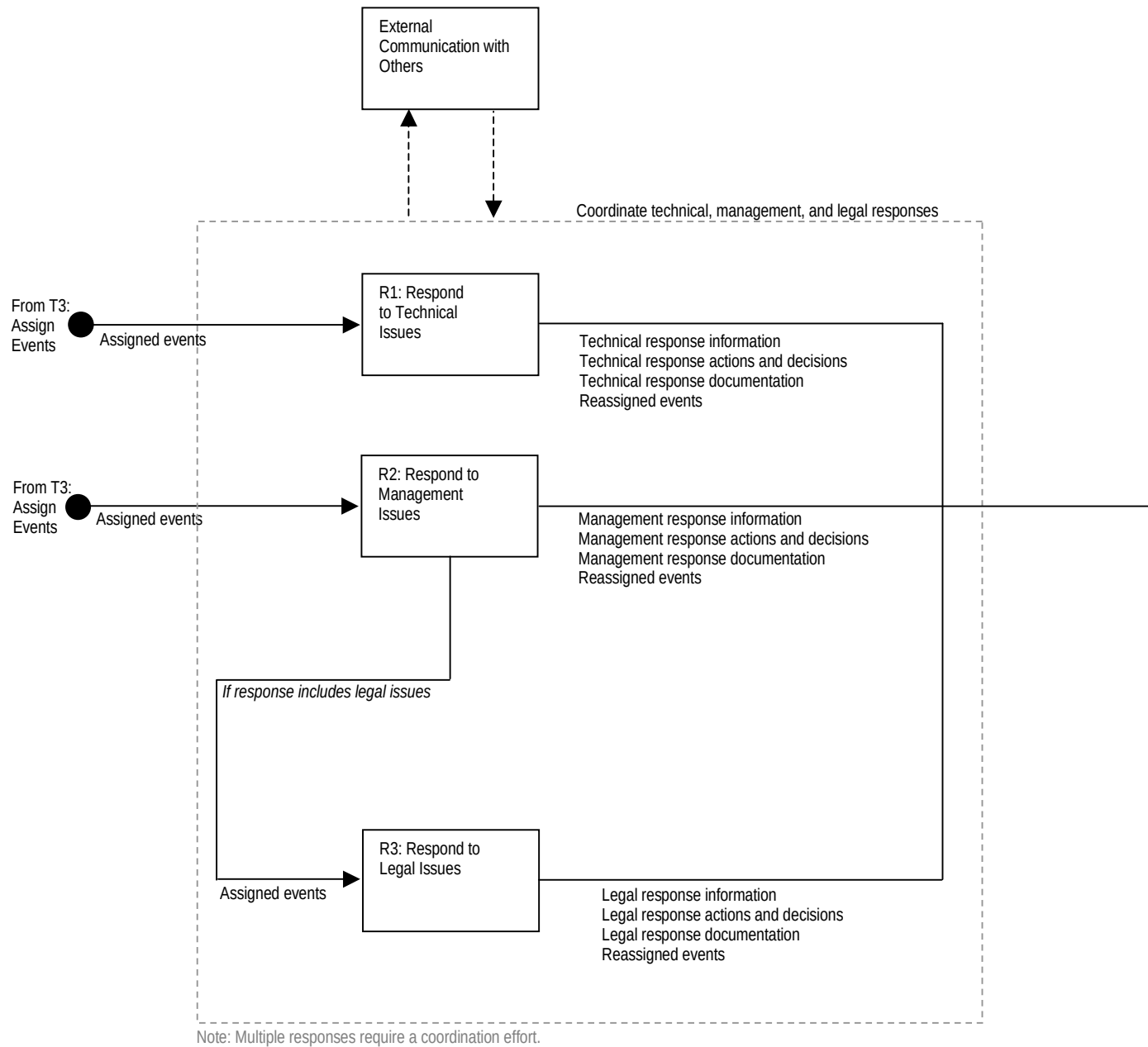
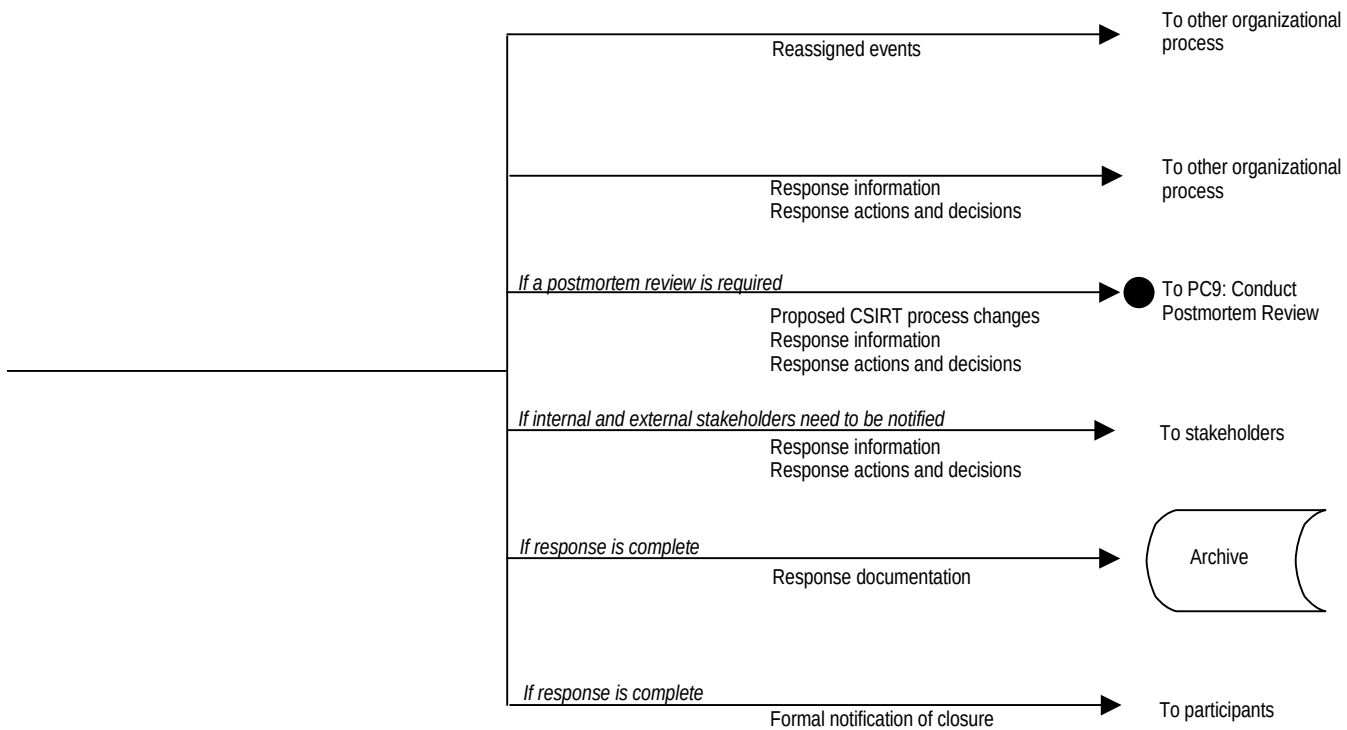


Figure 18: R: Respond Workflow Diagram



4.2.5.6 R: Respond Workflow Description

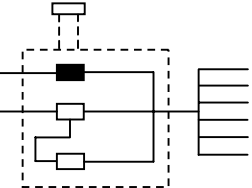
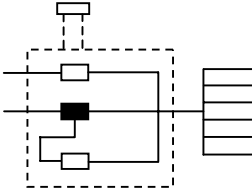
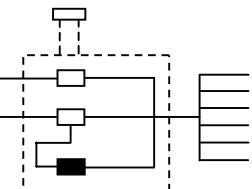
Table 17: R: Respond Workflow Description

Mission/Objectives	Triggers
• To resolve events and incidents – within defined time constraints – while handling information appropriately (e.g., within security, legal, and investigative contexts) – according to established policy, procedures, and quality requirements	• When assigned events arrive

Inputs		
Input	Description	Form
Assigned events	This includes all information that is passed to R: Respond for a given event. It can include event information received by T: Triage Events, the event's category and priority, and assigned responsibility for incident handling. Some events may be identified as incidents during T: Triage Events, while other events are passed to R: Respond for further evaluation.	Verbal, electronic, or physical

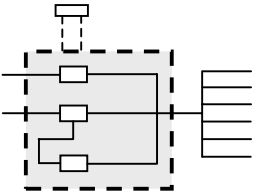
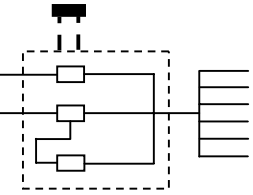
Completion Criteria	Policies and Rules	General Requirements
When technical, management, and legal responses are complete (e.g., no further response actions remain, the event or incident is closed, or the event or incident is reassigned outside of the incident handling process) Note: The technical, management, and legal responses might not close at the same time.	- CSIRT/IT policies - Organizational security policies (including HR and PR) - Security-related regulations, laws, guidelines, standards, and metrics - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Designated personnel document and track results in accordance with CSIRT and organizational policies and procedures. - When an event is part of an incident that has previously been closed, designated personnel can reopen the closed incident if appropriate.

Outputs			
Decision	Output	Description	Form
A postmortem review of the incident is required	Response information	This includes all relevant response-related data tailored for a specific audience (e.g., for a postmortem, for stakeholders, for other organizational personnel).	Verbal, electronic, or physical
Internal and external stakeholders need to be notified	Response actions and decisions	This includes the following data about the response: - technical, management, or legal actions taken - technical, management, or legal decisions made	Verbal, electronic, or physical
Response is reassigned outside of the incident management process			
A postmortem review of the incident is required	Proposed CSIRT process changes	This includes projected modifications to an existing CSIRT process. When the decision to conduct a postmortem is made, proposed CSIRT process changes are forwarded from R: Respond to PC: Prepare/Sustain/Improve.	Verbal, electronic, or physical
Event is reassigned outside of the incident management process	Reassigned events	This includes all information related to an event that is reassigned outside of the incident management process. It can include information received by R: Respond, any preliminary analysis performed on the information, and the rationale for reassigning the event. When applicable, it can also include the response strategy, as well as any actions and decisions made during the response.	Verbal, electronic, or physical
The response is complete	Response documentation	This includes all information related to the response. It is recorded once the response is complete.	Electronic or physical
	Formal notification of closure	This is an official notice to everyone who participated in the response that it is complete.	Verbal, electronic, or physical

Subprocess	Subprocess Requirements	Written Procedures				
R1: Respond to Technical Issues 	- Designated personnel analyze each event and plan, coordinate, and execute the appropriate technical response across involved sites and other relevant parties. - Designated personnel decide that the technical response is complete, all appropriate personnel are notified, and the incident is closed. - Automated tools execute preplanned technical responses when appropriate. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Assigned events* </td><td> - Technical response information* - Technical response actions and decisions* - Technical response documentation* - Reassigned events* </td></tr></table>	Inputs	Outputs	Assigned events*	- Technical response information* - Technical response actions and decisions* - Technical response documentation* - Reassigned events*	- Designated personnel follow incident handling procedures when analyzing, planning, coordinating, and responding to events. - Designated personnel use predefined guidelines when responding to specific types of events. - Designated personnel follow appropriate procedures for closing incidents. - Automated response tools are designed to execute preplanned technical responses for specific types of events or incidents.
Inputs	Outputs					
Assigned events*	- Technical response information* - Technical response actions and decisions* - Technical response documentation* - Reassigned events*					
R2: Respond to Management Issues 	- Designated personnel analyze each event and plan, coordinate, and execute the appropriate management response. - Designated personnel decide that the management response is complete, all appropriate personnel are notified, and the incident is closed. - Designated personnel trigger a legal response when appropriate. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Assigned events* </td><td> - Management response information* - Management response actions and decisions* - Management response documentation* - Reassigned events* </td></tr></table>	Inputs	Outputs	Assigned events*	- Management response information* - Management response actions and decisions* - Management response documentation* - Reassigned events*	- Designated personnel follow organizational procedures (e.g., project management, IT governance, policy management) for coordinating and responding to events. - Designated personnel follow appropriate procedures for closing incidents. - Designated personnel follow human resource procedures when dealing with staffing issues. - Designated personnel follow PR procedures when dealing with media issues. - Designated personnel follow risk and audit procedures when dealing with liability and compliance issues. - Designated personnel follow quality assurance procedures when dealing with quality issues.
Inputs	Outputs					
Assigned events*	- Management response information* - Management response actions and decisions* - Management response documentation* - Reassigned events*					
R3: Respond to Legal Issues 	- Designated personnel analyze each event and plan, coordinate, and execute the appropriate legal response regarding legal advice, investigation, and prosecution. - Designated personnel decide that the legal response is complete, all appropriate personnel are notified, and the incident is closed. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Assigned events* </td><td> - Legal response information* - Legal response actions and decisions* - Legal response documentation* - Reassigned events* </td></tr></table>	Inputs	Outputs	Assigned events*	- Legal response information* - Legal response actions and decisions* - Legal response documentation* - Reassigned events*	- Designated personnel follow appropriate guidelines and procedures, regulations, and laws when - providing legal advice - conducting investigations - collecting evidence - prosecuting perpetrators - Designated personnel follow appropriate procedures for closing incidents.
Inputs	Outputs					
Assigned events*	- Legal response information* - Legal response actions and decisions* - Legal response documentation* - Reassigned events*					

Note: An asterisk (*) after an input to or an output of a subprocess indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Key People	Technology	Other/Miscellaneous
• Designated personnel for responding to technical issues can include – CSIRT staff – CSIRT manager – IT staff (system and network administrators) – security staff (physical and cyber) – SMEs/trusted experts – information security officer – vendors – other CSIRTs – ISPs/network service providers – CSIRT constituency – victim or involved sites – coordination center	• Designated personnel can use the following technology when responding to technical issues: – security tools (e.g., log analysis tools, event monitoring tools, antivirus tools, file integrity checkers, vulnerability scanning tools, DNS query tools, whois, port number lists, forensics and other investigative tools) – infrastructure components (firewalls, intrusion detection systems, routers, filters) – knowledge bases (CERT/CC, CVE) – system and network administration tools (tools for configuration management, patch management, and user management) – incident handling database/tracking system – communication channels, encrypted when appropriate (email, mailing lists, newsgroups, web, XML RSS channels, automated call distribution system) • Automated response tools can be used to automatically execute a preplanned technical response.	• Periodic quality assurance checks are performed on automated tools. • Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools. • Designated personnel can recategorize and reprioritize incidents when appropriate.
• Designated personnel for responding to management issues can include – upper management of the CSIRT constituency, business and functional units, IT management, etc. – CSIRT manager – HR staff – PR staff – auditors, risk management staff, compliance staff – SMEs/trusted experts – victim or involved sites – coordination center	• Designated personnel can use the following technology when responding to management issues: – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) – decision support tools	• Designated personnel use executive and technical summaries as aids in decision making. • Designated personnel can recategorize and reprioritize incidents when appropriate.
• Designated personnel for responding to legal issues can include – legal counsel for constituency and CSIRT – inspectors general – attorneys general – law enforcement (state, local, federal, international) – criminal investigators – forensics specialists – victim or involved sites	• Designated personnel can use the following technology when responding to legal issues: – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) – forensics and other investigative tools – knowledge bases (case law, judicial precedents, laws, regulations, integrated justice systems) – any technologies that support the legal process	• ---

Subprocess	Subprocess Requirements	Written Procedures
Coordinate Technical, Management, and Legal Responses 	• Designated personnel plan, coordinate, and execute their response by providing advice, developing and disseminating recommendations, sharing data, and giving directions and assigning actions. • Designated personnel decide that the coordinated response is complete, all appropriate personnel are notified, and the incident is closed. Shared Information • Technical, management, and legal response information* • Technical, management, and legal response actions and decisions* Output • Response information* • Response actions and decisions* • Response documentation* • Reassigned events*	• Designated personnel follow procedures required for technical, management, and legal responses. • Designated personnel follow appropriate procedures for coordinating technical, legal, and management responses. • Designated personnel follow information disclosure policies, guidelines, and procedures.
External Communication with Others 	• Designated personnel communicate with external parties as part of the response. This communication can include queries for additional information about an incident, recommendations for addressing an incident, information required for coordinating the response with external parties, and required reporting to designated entities.	• Designated personnel follow procedures required for communicating with external parties. • Designated personnel follow appropriate procedures for working with external parties. • Designated personnel follow information disclosure policies, guidelines, and procedures.

Key People	Technology	Other/Miscellaneous
• Designated personnel for coordinating technical, management, and legal responses can include – key people involved in the technical, management, and legal responses	• Designated personnel can use the following technology when coordinating technical, management, and legal responses: – communication channels, encrypted when appropriate (email, phone, fax, XML RSS, videoconferencing, groupware, web) – data sharing tools, formats, and standards (web, IODEF, XML, IDMEF, CAIF) – documentation and publication technologies	• ---
• Designated personnel for communicating with external parties can include – key people involved in the technical, management, and legal responses – external people who might be involved in the response (e.g., media, other CSIRTs, vendors, SMEs, ISPs, NAPs, MSSPs, law enforcement, ISACs, other compliance organizations) – people from all involved sites	• Designated personnel can use the following technology when communicating with external parties: – communication channels, encrypted when appropriate (email, phone, fax, XML RSS, videoconferencing, groupware, web, special reporting systems) – data sharing tools, formats, and standards (web, IODEF, XML, IDMEF, CAIF) – documentation and publication technologies	• ---

4.2.5.7 Handoff from R: Respond to PC: Prepare/Sustain/Improve

This handoff details the requirements and transactions to successfully send incident management process changes, along with corresponding incident information and response actions and decisions, from the Respond process to the Prepare process. CSIRT process changes are proposed modifications to an existing CSIRT or incident management process.

When the decision to conduct a postmortem review is made, any process changes are forwarded from the Respond process to the Prepare process. Because this postmortem review will take a detailed look at how a particular response activity was handled, along with information that details what caused the event or incident to happen in the first place, any data related to the event or incident will also be passed to the Prepare process for analysis in the postmortem subprocess (PC9, Conduct Postmortem Review, on PC: Prepare/Sustain/Improve Workflow in [Table 6](#)).

The incident data may include information such as

- a description of the incident
- what caused the incident
- what was affected by the incident
- the constituency affected
- the effect on the global community
- hosts involved
- tools and exploits used

Response actions and decisions may include information about the event or incident resolution and mitigations steps that were taken, such as

- summary reports from the technical, management, or legal responses
- who was involved in the response process
- what worked well and what did not work well
- any failures in incident management processes and handoffs
- what could have been done to prevent the event or incident from happening³²

The above data are needed for the review so that those doing the postmortem can have a full picture of what actually happened. Such information can point out problems in existing computing infrastructures, incident management processes, staff training, end-user security awareness, and corresponding policies or procedures.

For example, take the following scenario. An end user reports (through the Detect process) that he clicked on an attachment in an email message and his computer became infected with

³² This can be an important question to ask during the postmortem review to determine what actions should be taken to improve operations so that similar activity does not occur.

a malicious virus. The message is passed to Triage and assigned to an incident handler in the organization's CSIRT. As part of the Respond process, the incident handler undertakes analysis and determines that the infected computer actually sent out copies of the virus in other emails to other users in the organization who also clicked on the attachments, further propagating the malicious code. In the analysis it is also found that the end users in question did not have up-to-date versions of virus scanning software on their systems. By looking at this data in a postmortem review, it may be determined that some end-user training on the proper handling of attachments and the proper use of antivirus scanning software is required. This type of training can be seen as part of the process improvements that would be implemented as part of the Prepare process. Also it may be determined from the postmortem review that a new policy regarding use of automatic updates of virus scanning software must be put in place. This in turn may be sent as a process improvement to the Protect process, where new changes would be made in the organizational computing infrastructure.

Table 18: Handoff from R: Respond to PC: Prepare/Sustain/Improve

Mission/Objectives	Triggers
- To successfully send proposed CSIRT process changes, response information, and response actions and decisions from R: Respond to PC: Prepare, Sustain, and Improve CSIRT Process - within defined time constraints - while handling information within the appropriate security context - while tracking the handoff in an appropriate manner	- When the decision to conduct a postmortem review of an incident is made - When proposed CSIRT process changes, response information, and response actions and decisions are ready to be passed to PC: Prepare, Sustain, and Improve CSIRT Process

Processes Involved	
Sending Process	Receiving Process
R1: Respond to Technical Issues R2: Respond to Management Issues R3: Respond to Legal Issues	PC9: Conduct Postmortem Review

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor
- Designated personnel in R: <i>Respond</i> send incident information and response actions and decisions to designated personnel in PC: <i>Prepare, Sustain, and Improve CSIRT Process</i>. - Designated personnel in R: <i>Respond</i> provide confirmation that proposed CSIRT process changes, response information, and response actions and decisions were received. - Designated personnel in R: <i>Respond</i> and PC: <i>Prepare, Sustain, and Improve CSIRT Process</i> verify the integrity of transmitted incident information and response actions and decisions.	- Designated personnel follow operational procedures for sending and receiving CSIRT process improvements. - Designated personnel follow organizational or CSIRT change management processes or guidelines.	- Designated personnel in R: <i>Respond</i> who send proposed CSIRT process changes, response information, and response actions and decisions can include - Key people involved in the technical, management, and legal responses

Completion Criteria	Policies and Rules	General Requirements
- When proposed CSIRT process changes, response information, and response actions and decisions have been sent to <i>PC: Prepare, Sustain, and Improve CSIRT Process</i> - When proposed CSIRT process changes, response information, and response actions and decisions have been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Objects Being Transported/Transmitted	
Object	Description
Proposed CSIRT process changes	This includes projected modifications to an existing CSIRT process. When the decision to conduct a postmortem is made, proposed CSIRT process changes are forwarded from <i>R: Respond to PC: Prepare, Sustain, and Improve CSIRT Process</i> .
Response information	This includes all relevant response-related data tailored for a specific audience (e.g., for a post-mortem, for stakeholders, for other organizational personnel).
Response actions and decisions	This includes the following data about the response: - technical, management, or legal actions taken - technical, management, or legal decisions made

Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Miscellaneous
- Designated personnel in <i>PC: Prepare, Sustain, and Improve CSIRT Process</i> who receive proposed CSIRT process changes, response information, and response actions and decisions can include - CSIRT staff - CSIRT manager - IT staff - IT manager - business function managers - CSIRT constituency - representatives from administrative operations (e.g., legal, HR, PR, compliance) - auditors, risk management staff, compliance staff	Verbal	- Phone - Face-to-face communication	---
	Electronic	- Email - Fax - Electronic reporting system (e.g., special change management system)	
	Physical	Hard copy passed from one person to another (e.g., change management forms and reports)	

4.2.5.8 R1: Respond to Technical Issues Workflow Diagram

This workflow displays the next level of detail for the Respond process as it relates to responding to technical issues (R1). The basic functions or processes include

- analyzing the incoming event or incident information (R1.1). Information that has not been categorized as an incident is considered an event. The last place that an event can be categorized as an incident is during this analysis phase in the Respond process. Analysis tasks will involve determining what has happened, along with researching options for resolution and mitigation. From the analysis phase, an event can be reassigned outside the incident handling process, closed if there is no further action to be taken, or designated as an incident and passed through the rest of the Respond process.
- planning the appropriate technical response (R1.2). This step involves determining what steps to take to mitigate or resolve the incident and determining who needs to be involved and who will perform which task.
- coordinating and responding to the incident (R2.3). This is the step in which the actual response work is completed. It involves implementing the planned response steps and coordinating with any internal or external groups that are part of the response or that require notification. Output from this step can include performing more analysis if the response is ineffective or if more information is required, reassigning an incident outside of the CSIRT process for resolution, deciding to perform a postmortem review on the incident response actions to determine any process improvements, or notifying internal or external stakeholders of the incident resolution.
- closing response (R1.4). If no further action can be taken or if an incident state matches a predefined criterion for closure, this step is taken.

This part of the incident management process is the one most associated with incident response actions. Technical response actions taken can include

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

Future work will develop detailed process workflows for these different types of subprocesses.

Figure 19 details the workflow diagram for this subprocess. A corresponding workflow description (table) has not been done for this level of process.

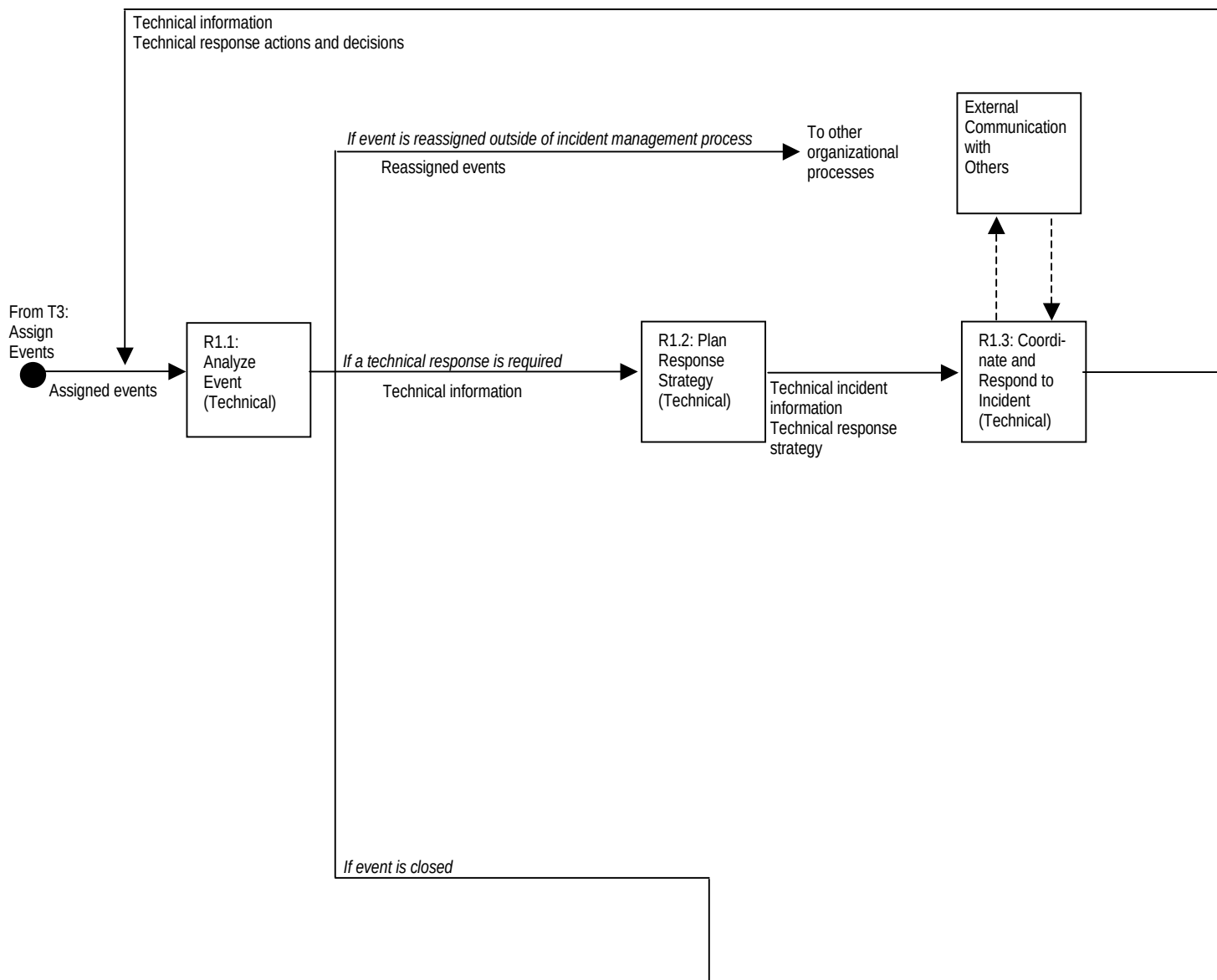
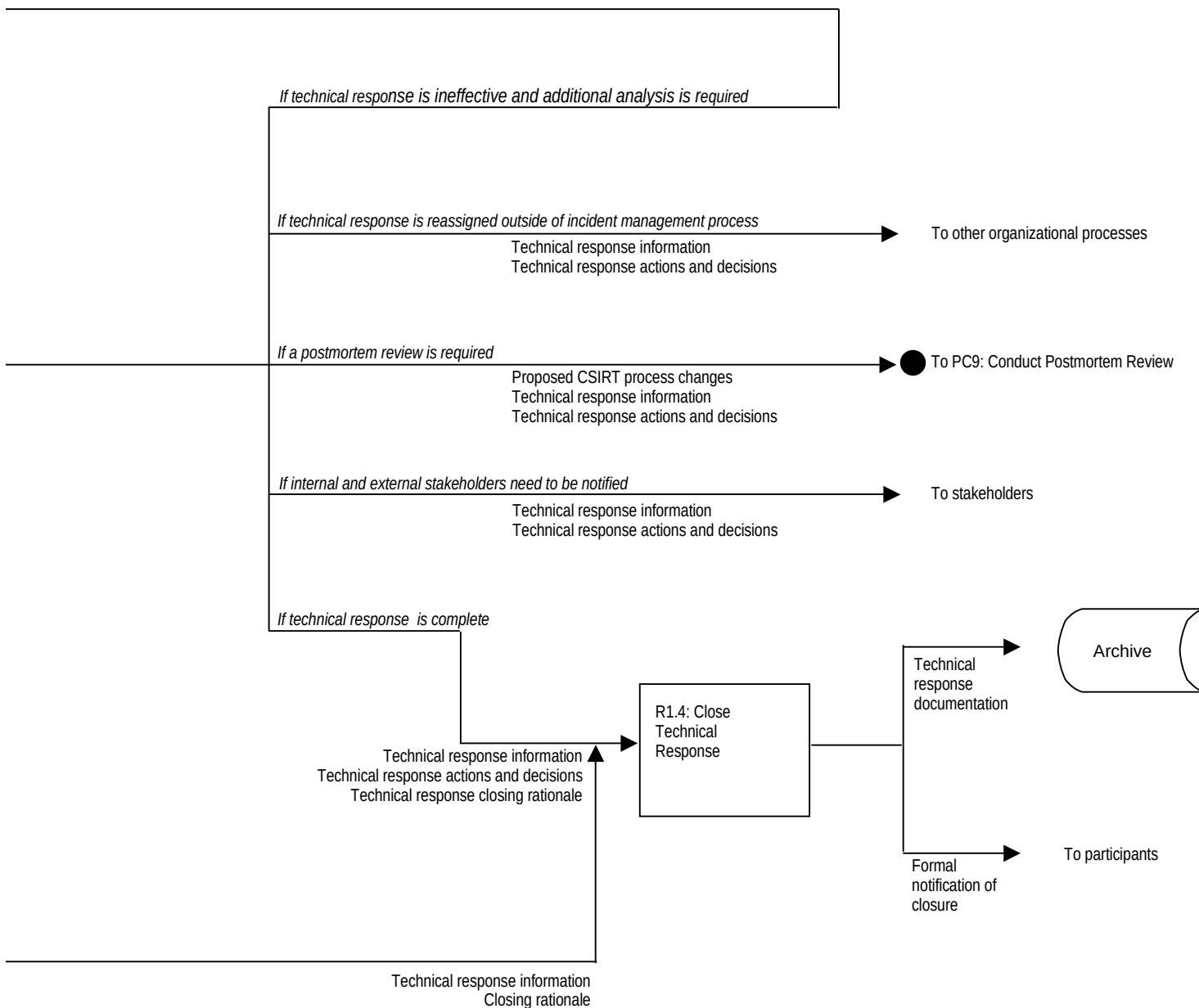


Figure 19: R1: Respond to Technical Issues Workflow Diagram



4.2.5.9 R2: Respond to Management Issues Workflow Diagram

This workflow displays the next level of detail for the Respond process as it relates to responding to management issues (R2). The basic functions or processes include

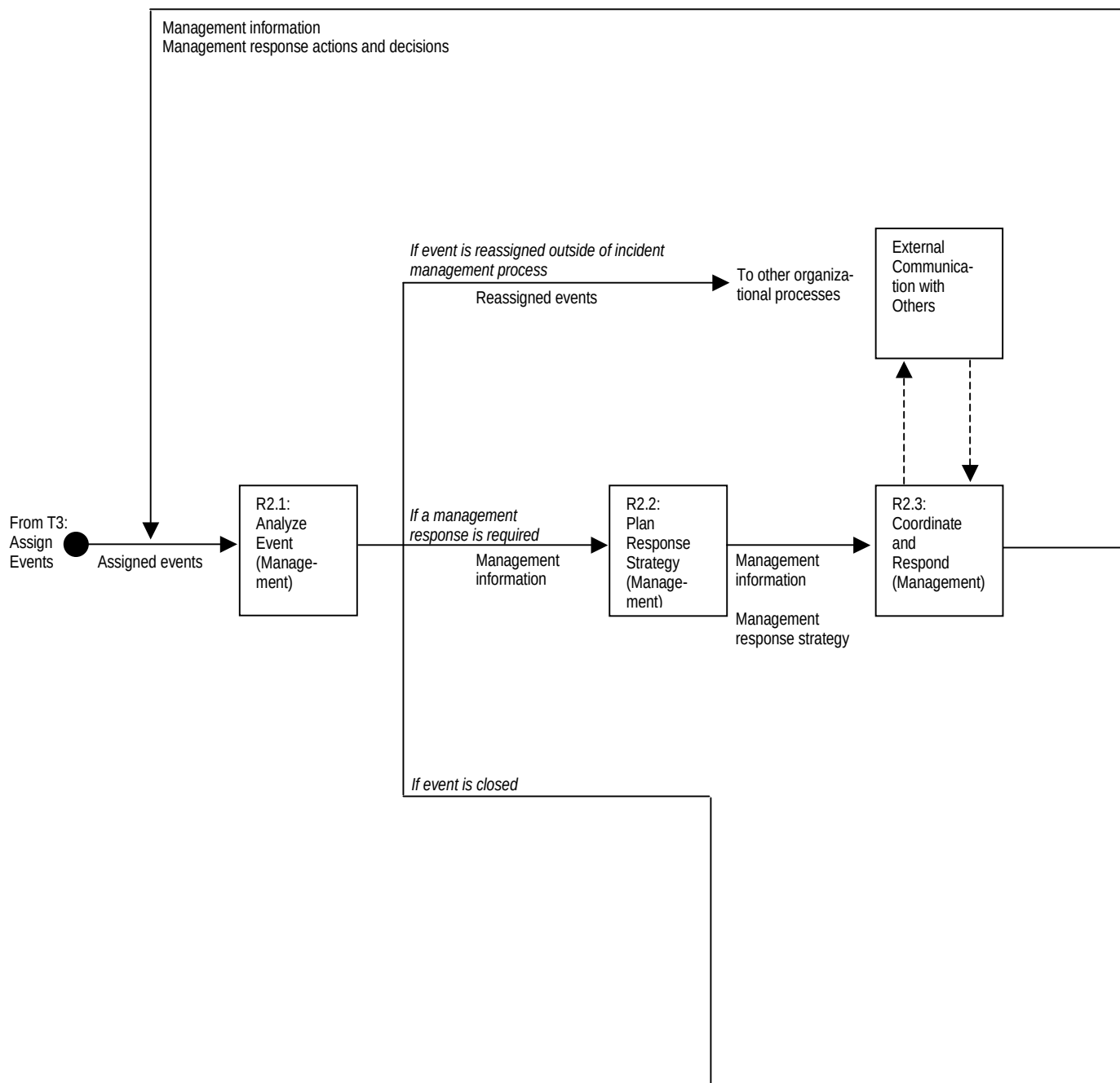
- analyzing the incoming event or incident information (R2.1). Analysis tasks will involve determining what has happened, along with researching options for resolution and mitigation. From the analysis phase, an event can be reassigned outside the incident management process, closed if there is no further action to be taken, or designated as an incident and passed through the rest of the Respond process.
- planning the appropriate management response (R2.2). This step involves determining what steps to take to mitigate or resolve the event or incident and determining who needs to be involved and who will perform which task.
- coordinating and responding to the incident (R2.3). This is the step in which the actual response work is completed. It involves implementing the planned response steps and coordinating with any internal or external groups that are part of the response or that require notification. Output from this step can include performing more analysis if the response is ineffective or if more information is required, reassigning an incident outside of the incident management process for resolution, deciding to perform a postmortem review on the incident response actions to determine any process improvements, or notifying internal or external stakeholders of the response resolution.
- closing response (R2.4). If no further action can be taken or if an incident state matches a predefined criterion for closure, this step is taken.

Management response actions might include

- human resources removing an abusive employee who has been involved in internal malicious activity
- media relations developing a press release concerning incident activity that has been made public
- specific organizational actions taken by senior management
- management contacting legal counsel for assistance and advice (This would cross over into the R3: Respond to Legal Issues subprocess.)
- working with risk management and financial services to determine the total impact and cost of any down time due to an incident

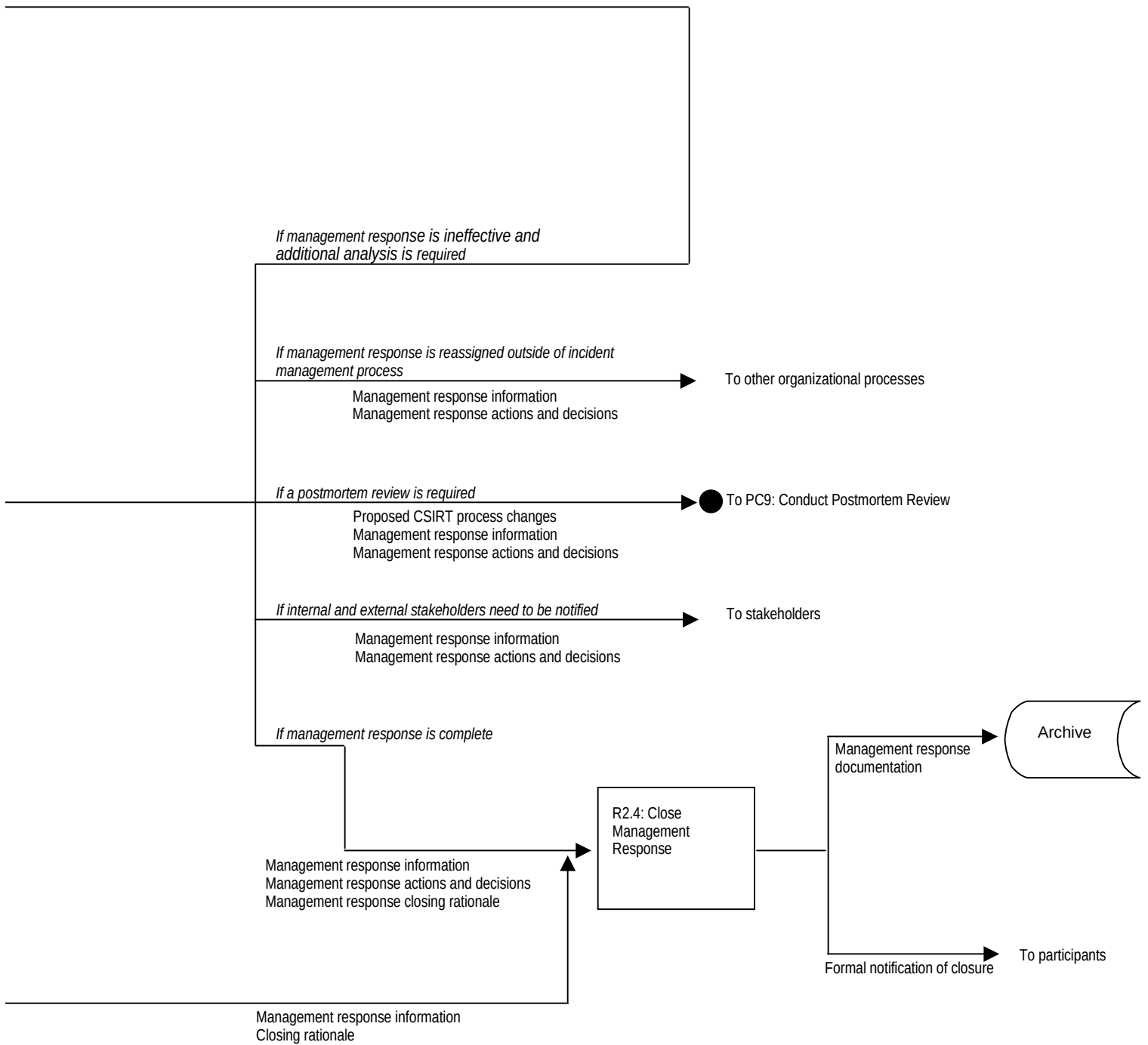
Future work will develop detailed process workflows for these different types of subprocesses.

Figure 20 details the workflow diagram for this subprocess. A corresponding workflow description (table) has not been done for this level of process.



Note: If technical or legal responses are part of an overall coordinated response, the coordination of all responses is embedded in R2.2, R2.3, and R2.4.

Figure 20: R2: Respond to Management Issues Workflow Diagram



4.2.5.10 R3: Respond to Legal Issues Workflow Diagram

The workflow diagram in [Figure 21](#) details the steps for performing a legal response. The more detailed level of this workflow process has not yet been completed. This process is presented at a high overview level.

This process can be initiated only by the Respond to Management Issues process. This is because, unless technical staff have been designated or automatic notification criteria are in place, it is usually management that decides that a legal response is needed.

The type of people that may be involved in legal response can vary, depending on the actions taken and expertise required. They can include

- organizational legal counsel or paralegals
- national, state, or local law enforcement and corresponding members of any government organization related to justice, such as the U.S. Attorney General's office, the U.S. Department of Justice, the U.S. Secret Service, the U.S. FBI, Interpol, or federal police in other countries
- computer or network forensic analysts

Legal response actions can include

- providing advice on what response options are legally allowed according to any applicable laws and regulations
- providing advice from legal counsel on the legal liability of malicious activities occurring on the organizational network
- reviewing press releases or organizational memos for any legal or liability issues
- developing nondisclosure agreements for working with external experts during a response action
- notifying and involving law enforcement
- coordinating with technical response to perform computer forensics tasks to preserve evidence in a manner that will allow it to be used in a court of law
- reviewing legal documents and briefs related to the ongoing response actions or initiating activity

Future work will develop detailed process workflows for these different types of subprocesses.

Resources available from the CERT/CC that provide more information about legal response issues include

- *How the FBI Investigates Computer Crime*
http://www.cert.org/tech_tips/FBI_investigates_crime.html

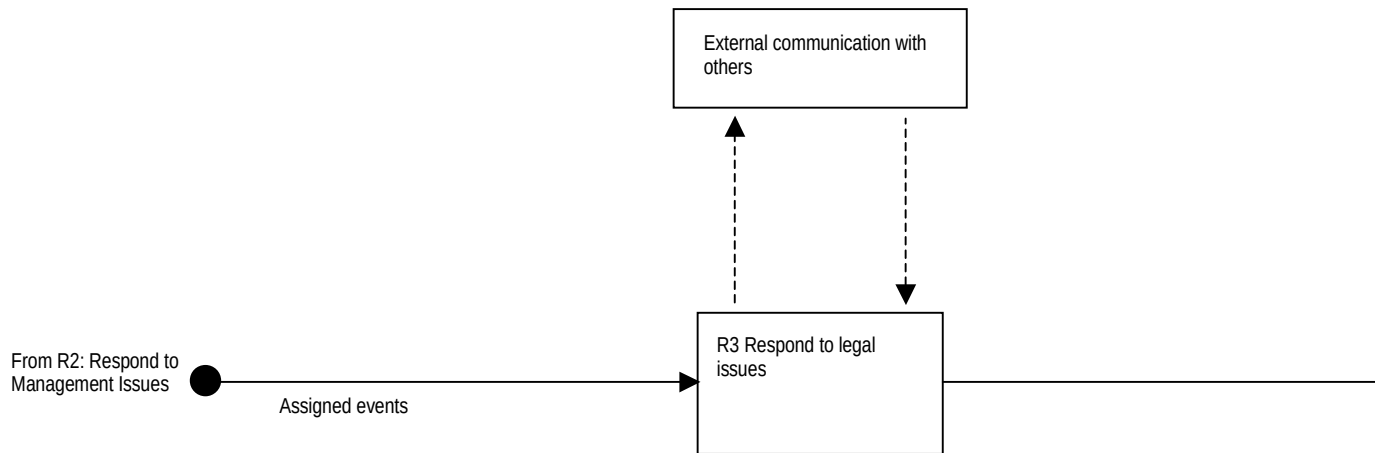
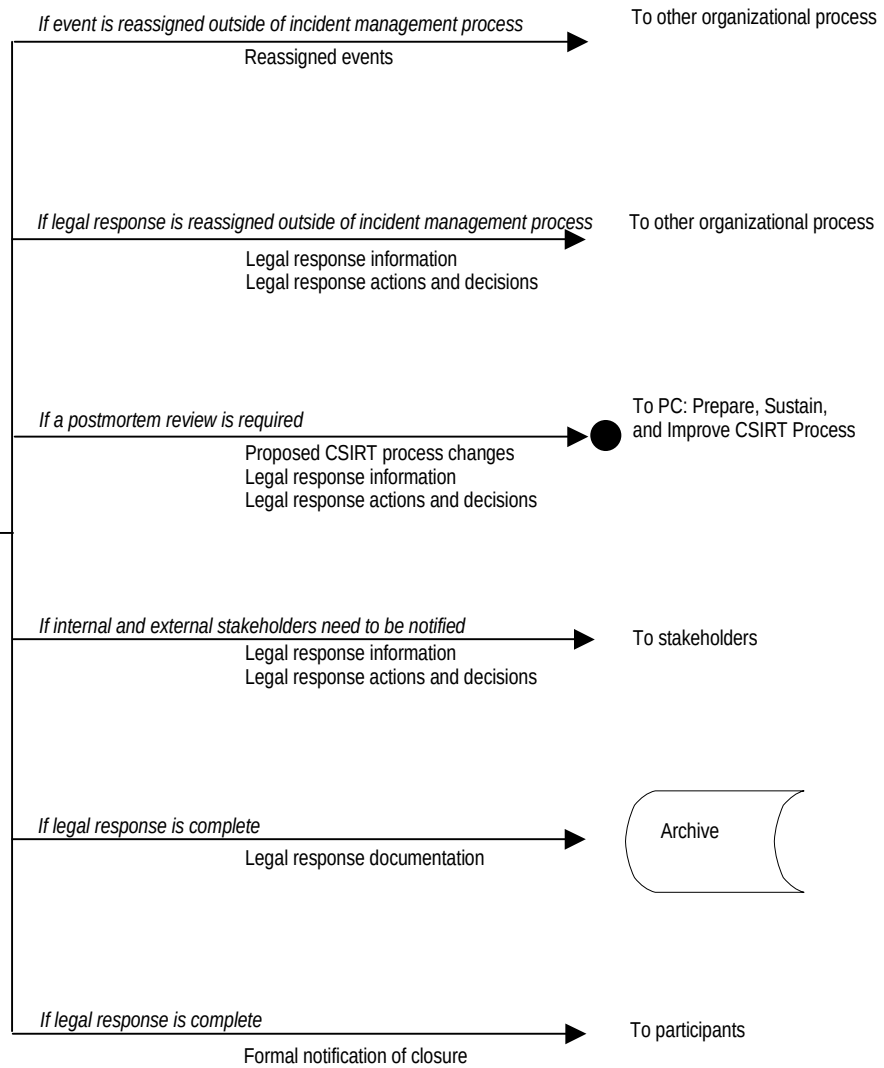


Figure 21: R3: Respond to Legal Issues Workflow Diagram



5 Future Work

As mentioned at the beginning of this report, the work presented here showcases our evolving ideas and thoughts about CSIRT processes and incident management processes in general. It outlines our premise that incident management is an enterprise-wide, distributed function. It also presents our belief that successful incident management must support and enable the core business functions of the parent organization or constituency. This work presents our initial attempt to document and describe the basic processes required for incident management to be effective.

This publication alone is not an effective mechanism for organizations to take our ideas and implement them. Additional products and tools will be necessary to allow organizations to use the concepts to help create, sustain, evaluate, and improve incident management capabilities. Future work will involve the development of various products and guides that will be useful in

- understanding the various processes and activities generally required to perform incident management work
- documenting existing incident management processes (current, as-is state) in an organization
- benchmarking existing incident management capabilities in an organization against this presented best practice model
- planning and designing a new or improved incident management capability (creating a desired, to-be state and corresponding implementation strategy)
- evaluating the incident management performance of a CSIRT or capability

The work presented here is only one step in continuing to add to the body of knowledge for incident management (and CSIRT) operations. These process maps will continue to drive other work, including changes to our existing courses, development of follow-up technical reports and publications, and development of additional supporting materials and guides for creating, sustaining, and evaluating incident management capabilities.

The next phase of this work will be to

- refine the existing maps based on input from the community
- continue the process mapping function at the third or further level
- develop additional publications that explain in more depth the incident management processes detailed here

- develop more user-friendly guidance and a methodology for applying the concepts and process maps presented in this report
- develop a gap analysis instrument to help document the as-is state of an organization in regard to incident management processes
- develop a risk analysis instrument to help identify potential risks to successful CSIRT operations. This will also entail determining
 - common failure modes for each process
 - common mitigation strategies to prevent failure
- perform a pilot evaluation of assessment and evaluation instruments
- document our work, the resulting process maps and evaluation instruments, and the supporting pilot studies in a series of technical reports, white papers, and case studies
- integrate the resulting work into our course materials and any other relevant resources
- identify potential new work resulting from the process mapping project

Other work currently underway will involve comparing our incident management process maps for CSIRTs to other standard security best practices, including

- ISO 17799/British Standards Institute 7799 Part 2
- Control Objectives for Information and related Technology (COBIT)
- Information Technology Infrastructure Library (ITIL)
- National Institute of Standards and Technology (NIST) (selected SP 800 series); FIPS 199
- other relevant standards

The scope of the work related to this project is large. As we continue this work, we are looking for collaborators to

- review and comment on the draft process maps, resulting technical reports, and supporting documents
- help develop new materials and supporting documents based on these process maps and the resulting work
- serve as a possible pilot site for testing and validating evaluation instruments
- develop tools to apply the resulting incident management process map methodologies

If you are interested in collaborating with us on this work, contact us at csirt-info@cert.org.

You can also contact us at that address if you have comments, criticisms, or recommendations to make about our initial set of incident management processes or the corresponding work-flow diagrams and descriptions associated with this project, or if you know of a process that is missing and should be considered for inclusion in this model.

We realize that only by actually piloting this work through real implementations by us or others will we truly discover any inherent problems. If you do attempt to implement the concepts documented here before we release additional guidance or support materials, please feel free to share your results with us. We would be interested in answers to any of the following questions:

- Did the process maps provide you an adequate framework for creating, sustaining, evaluating or improving your incident management capabilities?
- If not, what type of guidance would have been helpful?
- If the process maps were beneficial, in what way were they helpful?
- Were you able to use the workflows and corresponding descriptions to document your current processes?
- Were you able to use the workflows and corresponding descriptions to benchmark your current processes?
- Were you able to use the workflows and corresponding descriptions to plan improvements to your current processes and structure?
- Did you find that your processes included tasks and functions not documented in our incident management processes?
- If so, what were they?

As we continue our work and develop new materials for publication, we will continue to ask these types of questions. Any feedback you can provide will be appreciated.

Bibliography

URLs are valid as of the publication date of this document.

- [Alberts 02]** Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE Approach*. Reading, MA: Addison-Wesley, 2002.
- [Allen 99]** Allen, Julia H. *The CERT Guide to System and Network Security Practices*. Reading, MA: Addison-Wesley, 2001.
- [Brownlee 98]** Brownlee, N. & Guttman, E. *Expectations for Computer Security Incident Response* (RFC 2350).
<http://www.ietf.org/rfc/rfc2350.txt?number=2350> (1998).
- [Caralli 04]** Caralli, Richard; Allen, Julia; & Wilson, William. *The Critical Success Factors Technique: Establishing a Foundation for Enterprise Security Management*. Preconference Workshop, Second Annual Information Technology Security Conference (Secure IT). San Francisco, CA, 2004. http://www.secureitconf.com/2004/Pre-Conference_Workshop.asp.
- [Cunningham 97]** Cunningham, L.; Firth, R.; Ford, G; Fraser, B.; Kochmar, J.; Konda, S; Richael, J.; & Simmel, D. *Detecting Signs of Intrusion* (CMU/SEI-SIM-001, ADA329629). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997.
<http://www.cert.org/security-improvement/#modules>.
- [FISMA 02]** U.S. Congress. *Federal Information Security Management Act of 2002, Title III of the Egovernment Act of 2002* (HB2458). Available online through <http://thomas.loc.gov/>.
- [Fraser 97]** Fraser, B., ed. *Site Security Handbook* (RFC 2196).
<http://www.ietf.org/rfc/rfc2196.txt> (1997).
- [ISS 01]** Internet Security Systems (ISS). *Computer Security Incident Response Planning: Preparing for the Inevitable*.
<http://documents.iss.net/whitepapers/csirplanning.pdf> (2001).

- [Jackson 97]** Jackson, Michael & Twaddle, Graham. *Business Process Implementation: Building Workflow Systems*. New York, NY: Association for Computing Machinery Press; Harlow, England: Addison-Wesley; 1997.
- [Johnson 92]** Johnson, D. *NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist* (RFC 1297). <http://www.ietf.org/rfc/rfc1297> (1992).
- [Killcrece 02]** Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. *CSIRT Services*. <http://www.cert.org/csirts/services.html> (2002).
- [Killcrece 03a]** Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-001, ADA421684). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. <http://www.sei.cmu.edu/publications/documents/03.reports/03hb001.html>.
- [Killcrece 03b]** Killcrece, G.; Kossakowski, K.; Ruefle, R.; & Zajicek, M. *State of the Practice of Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-TR-001, ADA421664). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. <http://www.sei.cmu.edu/publications/documents/03.reports/03tr001.html>.
- [Kobielus 97]** Kobielus, James G. *Workflow Strategies*. Foster City, CA: IDG Books Worldwide, Inc. 1997.
- [Kossakowski 99]** Kossakowski, K.; Allen, J.; Alberts, C.; Cohen, C.; Ford, G.; Fraser, B.; Hayes, E.; Kochmar, J.; Konda, S.; & Wilson, W. *Responding to Intrusions* (CMU/SEI-SIM-006, ADA360500). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. <http://www.cert.org/security-improvement/#modules>.
- [Kruse 02]** Kruse, Warren G. II & Heiser, Jay G. *Computer Forensics: Incident Response Essentials*. Reading, MA: Addison-Wesley, 2002.
- [Mandia 01]** Mandia, Kevin & Proise, Chris. *Incident Response: Investigating Computer Crime*. Berkeley, CA: Osborne/McGraw-Hill, 2001.

- [Navy 96]** Department of the Navy. *Computer Incident Response Guidebook, Module 19* (NAVSO P-5239-19). <http://www.nswc.navy.mil/ISSEC/Guidance/P5239-19.html> (1996).
- [OGC 03]** Office of Government Commerce (OGC). *ICT Infrastructure Management Glossary*. <http://www.get-best-practice.co.uk/glossary.aspx?product=ictinfrastructurelibrary> (2003).
- [SANS 03]** The SANS Institute. *Computer Security Incident Handling Step-by-Step*. The SANS Institute, October 2003. Information on how to acquire this guide is available at <http://store.sans.org/>.
- [Schultz 90]** Schultz, Eugene; Brown, David S.; & Longstaff, Thomas A. *Responding to Computer Security Incidents*. <ftp://ftp.cert.dfn.de/pub/docs/csir/ihg.txt.gz> (1990).
- [Schultz 02]** Schultz, Eugene & Shumway, Russell. *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*. Indianapolis, IN: New Riders Publishing, 2002.
- [Sharp 01]** Sharp, Alex & McDermott, Patrick. *Workflow Modeling*. Boston, MA: Artech House, 2001.
- [Shirey 00]** Shirey, R. *Internet Security Glossary* (RFC 2828). <http://www.ietf.org/rfc/rfc2828.txt> (2000).
- [Sokol 00]** Sokol, Marc S. & Curry, David A. *Security Architecture and Incident Management for E-business*. Internet Security Systems (whitepaper), 2000.
- [Starr 03]** Starr, Randy; Newfrock, Jim; & Delurey, Michael. "Enterprise Resilience: Managing Risk in the Networked Economy." *strategy+business*, Spring 2003. <http://www.strategy-business.com> (registration required).
- [Symantec 01]** Symantec Corp. *Advance Planning for Incident Response and Forensics*. <http://enterprisesecurity.symantec.com/SecurityServices/content.cfm?ArticleID=1557> (2001).
- [van Wyk 01]** van Wyk, Kenneth R. & Forno, Richard. *Incident Response*. Sebastopol, CA: O'Reilly & Associates, Inc., 2001.

[Vermont 01]

State of Vermont. *Incident Response Procedure*.

http://www.dii.state.vt.us/Home/pdf/sov_intrusion_procedures.pdf
(2001).

[West-Brown 03]

West-Brown, M.; Stikvoort, D.; Kossakowski, K.; Killcrece, G.; Ruefle, R.; & Zajicek, M. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002, ADA413778). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. <http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html>.

Appendix A: Context for Each of the Process Workflows

The following tables contain informal notes taken during our process mapping development work. The notes correspond to the fields in the process workflow descriptions and provide more detailed information about the related process and any exceptions or special circumstances.

Context for PC: Prepare/Sustain/Improve	
Applicable Table Element	Additional Information
Objectives	- Includes both the initial efforts to set up an incident response capability and all further changes and improvements. Both lessons learned and improvements from Prepare (PC) and any changes directed by the organization itself for other reasons would drive this activity. Coordination with the infrastructure protection improvements (PI) is likely required as this activity occurs. Outputs of Prepare are used to establish a more formal CSIRT capability as well as continually improve it. Changes to Detect (D), Triage (T), and Respond (R) are possible. - Prepare for CSIRT—what needs to be in place for incident response to occur—administration aspects, e.g., includes being able to collect and analyze general information about what’s going on.
Triggers	
Completion Criteria	
Policies and Rules	
General Requirements	- Reporting requirements can come from many sources, such as regional, state, or federal laws, European Union or other foreign regulations, DHS, ISAC, etc. - Personnel who have not received any training may have a set of standard, best practices, guidelines, or model to follow.
Inputs	Input/Description/Form
CSIRT process needs	Can come from constituency feedback or any other recommendation from a CSIRT process, or from some external decision or mandate that results in a change in CSIRT process needs.
Current CSIRT capability	
CSIRT process changes	
Incident information	

Context for PC: Prepare/Sustain/Improve	
Response actions and decisions	
Outputs - Decision	Output/Description/Form
CSIRT capability is initially being established	
Current CSIRT capability is not modified or improved	
Current CSIRT capability is modified or improved	Not all changes may be improvements. Some changes may be decreases in resources or requirements driven by other conditions or realignments of priorities. Circumstances may require a roll-back or a scaling back of efforts.
Improvements to infrastructure are required	External personnel or stakeholders need to be notified of lessons learned; archival of lessons learned is required
Subprocess	Subprocess Requirements/Written Procedures/Key People/Technology/Other
PC1. Identify CSIRT Requirements	• A planning step. Defines what the CSIRT capability is supposed to be. • Can include drivers from local, state, federal, and international laws and regulations, relevant standards, institutional standards and regulations, partners' standards and regulations.
PC2. Establish CSIRT Vision	• A planning step. Define roles and responsibilities, goals and objectives, internal and external constituencies and stakeholders, authority, services to be provided, what services will be provided to whom, and what authority the CSIRT has to carry out their activities. • Cannot occur until after identification of CSIRT requirements (PC1).
PC3. Obtain Sponsorship and Funding for CSIRT	• A planning step. Get the necessary corporate or external sponsorship and funding to set up and maintain a CSIRT capability. • Funding and sponsorship are both needed, but the order of these is not fixed. Funding could occur before sponsorship. Also this planning activity can occur before identification of requirements (PC1), and before or after establishment of the mission (PC2).
PC4. Develop CSIRT Implementation Plan	• A planning step. • Plan for setting up the CSIRT capability to meet the requirements and vision, within the constraints of the current sponsorship and funding.
Coordinate Planning and Design	Within the planning activities, coordination is required, as these are not disjoint activities nor do they necessarily occur in a fixed order. Overlap and reiteration are usual.

Context for PC: Prepare/Sustain/Improve	
PC5. Develop CSIRT Policies, Procedures, and Plans	• An implementation step. Define the “what” (policies), the “how,” and the specific steps to take (procedures). These are more detailed plans as opposed to the strategic plans. Includes – policies for reporting to CSIRTS – policies for working with CSIRTS – CSIRT staff policies – communication policy and plans – policies for working with corporate legal counsel and law enforcement • Inputs may include corporate or institutional policies, procedures, and plans to be coordinated with. Best practices, examples of policies, procedures, and plans.
PC6. Establish CSIRT Incident Handling Criteria	• An implementation step. A set of decision support materials, including sets of criteria and other lists to support CSIRT activities. Includes such things as – prioritization criteria – categories of incidents – escalation criteria – assignment criteria – notification and contact lists – critical information lists (what to collect and retain) – checklists for legal considerations and issues (e.g., what is required of the CSIRT team during investigations, what’s optional, corporate recommendations for interfacing with law enforcement) – new signatures for IDS – baselines for normal infrastructure activity
PC7. Implement Defined CSIRT Resources	• An implementation step. Includes such things as – staffing (internal and external) – training, mentoring, clearances for staff (internal and external and constituency/stakeholders) – non-disclosure agreements, etc. with external personnel – equipment and tools (e.g., secure phone lines, PCs, network) – CSIRT’s infrastructure—technical and physical – templates and artifacts, such as reporting forms and guidance for use – access to appropriate sources of information
Coordinate Implementation	Within the implementation activities, coordination is required, as these are not disjoint activities nor do they necessarily occur in a fixed order, although they do occur roughly in parallel. They require a lot of feedback and coordination to get everything in synch. Overlap and reiteration are usual.
PC8. Evaluate CSIRT Capability	• Assess the incident management capability against their requirements or do a Q&A check. Different from the lessons learned after an incident postmortem, which looks at specific activities related to handling that specific incident. This is broader, an overview of the incident management capability to determine longer range improvements to processes. • <i>Not</i> a general security assessment of the organization. • Can trigger improvement efforts in the incident management processes by a return to one or more of the Prepare steps. • Would likely include identification and collection of incident management capability effectiveness or quality measures to support periodic evaluations.

Context for PC: Prepare/Sustain/Improve	
PC9. Conduct Postmortem Review	- Review all of the information relative to the incident to determine the quality and completeness of the response and any needed improvements. Determine whether any activity at all is needed to make further improvements to incident management processes or whether any other lesson was learned from handling this incident. - Evaluate the relevant incident management activities and processes for adequacy and needed improvements. - Evaluate the infrastructure in terms of changes needed to prevent future similar incidents. - Identify gaps, weaknesses, or needed changes in the constituency. - Not every incident needs a formal review. Frequently the lessons to be learned are obvious enough that the incident handler can make the decision to improve and document the lesson learned. However, without any formal activity, if there are lessons learned or improvements that need to be made, these are not passed to the relevant party for implementation. May need a set of criteria to determine when something else needs to be done after closing an incident. Most incidents are repeats of earlier incidents and don't result in postmortems or lessons learned. If nothing else is needed, no further activity on the incident occurs. - Note that sometimes a technical response can continue for a long time with a continued series of attacks, but the postmortem may be conducted before the incident is closed.
PC10. Determine CSIRT Process Modifications	- Document what was learned from the incident and move to the next required activity with that knowledge. This document would be archived or passed along to other activities. These are immediate or short-term improvements. - This is not data related to the incident (chronology, what happened, etc.) but what could have been done better or what went wrong in handling the incident. The lessons learned could trigger one or more of the following: - archival of lessons learned documents and other outputs - improvements and changes to CSIRT processes, artifacts, tools, etc. (recommendations for changes in services, interaction guidelines, tech tips, training requirements, new POC lists, etc.) - changes and improvements to the infrastructure (recommendations for protecting systems, changes in services, interaction guidelines, tech tips, training requirements, etc.) - Communicate with constituency and stakeholders to pass along new artifacts, suggestions, improvements, etc. for them to implement (all of the above, as well as reports or just the lessons learned)
PC11. Implement CSIRT Process Modifications	- Implement any changes or improvements to CSIRT processes from postmortems and capability evaluations. - Note that modifications may not always be improvements, as some changes may be driven by changes in funding, resources, or other negative drivers.

Context for PC: Prepare/Sustain/Improve	
Side notes	- Note that when trying to start a more formal incident management capability, the following types of items are usually needed: identifying who needs to be involved in handling incidents; assigning responsibility; establishing policies; procedures, and guidelines for constituents for reporting/interacting with CSIRTs; notification lists, current inventory of tools, etc.; logistics; criteria and categories. - There are likely additional people who may be involved in a supporting role to many of these processes and activities. This would include people such as technical writers or editors and other support staff who provide underlying support functions but do not directly perform any of these activities. - CSIRT activities, as well as some of the general information coming in, can provide the basis for making changes and improvements to both the CSIRT and the infrastructure. Lessons learned, postmortems, indicators, or other types of information are products of this activity. Coordination between improvements made to the CSIRT and the infrastructure will likely be required and would be done here. Note that the decision to do a postmortem and get lessons learned may occur before an incident is closed but should be made no later than closure. - Note that some communications with stakeholders and constituents may require a review from the corporation's legal counsel. - Improve/Sustain—improve the incident management processes, abilities, services, response time, etc., as well as the system protection. - Ad hoc incident handling usually exists before any effort to formalize or organize a CSIRT capability occurs. Informality usually means there are no predetermined assignments or categories, the same mistakes and analyses are done repeatedly, and no lessons are learned. In that sense, then, Detect, Triage, and Respond are just ad hoc or poorly done, and someone eventually learns enough lessons to decide to actually prepare for a CSIRT capability and gets the process started in Prepare (PC). - When there's a change in personnel between one box and another, then the actual effectiveness of communication is one thing that needs to be considered.
Context for PI: Protect Infrastructure	
Applicable Table Element	Additional Information
Objectives	Does not include the initial set of activities to set up a secure infrastructure for the corporation. This addresses only the ongoing activities to maintain and improve the security of the systems as a result of evaluations or incident handling. Other changes from other sources besides the CSIRT activity are likely (e.g., routine and planned maintenance and upgrades). Coordination with (PC) is needed to ensure that the CSIRT team members are sufficiently aware of infrastructure changes and to synchronize joint improvements. This is basically the implementation of best practices for the protection of the systems based on the relevant standard of due care, be it ISO 17799 or a different standard.
Triggers	
Completion Criteria	
Policies and Rules	

Context for PC: Prepare/Sustain/Improve	
General Requirements	
Inputs	Input/Description/Form
Infrastructure protection improvements	Reports, advisories, and other notifications that are not specifically incident related can indicate the need for improvements to the infrastructure.
Current infrastructure	The current infrastructure that will be improved
Outputs	Decision/Output/Description/Form
Current infrastructure is improved	Can include additional components, changes to existing components, upgrades, etc.
Current infrastructure is not improved	Decision may be made to not improve or change the current infrastructure due to costs, potential negative impacts to constituency, or other reasons.
A potential incident is identified during evaluation	If a possible incident is uncovered during this process, it needs to be forwarded to Detect (D).
Subprocess	Subprocess Requirements Written Procedures/Key People/Technology/Other
PI1. Evaluate Infrastructure	- Assess and analyze infrastructure for survivability. Infrastructure can be periodically evaluated for problems or evaluated after significant improvements or changes to verify that no new problems have been introduced. - If the current infrastructure meets or exceeds the current requirements, then no further improvements may be needed. - Evaluations can include vulnerability assessments, risk assessments, red teaming, or independent, third-party assessments (ISE or OCTAVE). - Could relate to physical as well as cyber security, for those aspects of physical security that relate to the infrastructure.
PI2. Determine Infrastructure Protection Requirements	- As a result of evaluation, define requirements for additional or modified infrastructure protection. - Determine infrastructure protection and survivability requirements for improving and changing over time the protection and survivability of physical and cyber security.
PI3. Harden and Secure Infrastructure	- Implement the protection requirements and continue to carry out changes and improvements as needed. Repair and recover from problems, events, incidents, etc. - Theoretically, improved protection of the systems reduces the number of incidents the CSIRT must handle.
Side notes	- Protect—who owns the relevant practice, who needs to fix it. Communication channels need to be set up during Prepare. - When there's a change in personnel between one box and another, then the actual effectiveness of communication is one thing that needs to be considered.

Context for D: Detect	
Applicable Table Element	Additional Information
Objectives	Information about potential incidents is gathered either proactively (monitoring indicators of possible incidents) or reactively (received from internal or external sources in the form of reports or notifications). If a possible event is indicated, the event information is sent to Triage (T). Received information is analyzed to determine whether it is a possible event or not. If the information does not indicate that an event that needs action, the event is closed. Detect and Triage can occur in minutes or days—it depends on the efficiency of the team. Detect only includes the first order of information gathering. If additional information is required during the analysis steps, it is addressed there, not in Detect. Note that the initial steps of Detect could be done by non-CSIRT folks such as help-desk personnel.
Triggers	Whenever the CSIRT, their constituency, or external stakeholders notice something that may be an event or is significant enough to report.
Completion Criteria	
Policies and Rules	
General Requirements	
Inputs	Input/Description/Form
General indicators	Input to Detect can also come from Protect Infrastructure (PI)—for example, new things to look for, changes in configurations, etc. that might alter what is being proactively monitored. May also include new potential incidents found while analyzing a current incident.
Event reports	
Outputs - Decision	Output/Description/Form
Event requires further incident handling action	Event information—the event may or may not be declared an incident at this point, but it is passed to Triage for further analysis.
Event is reassigned outside of the incident handling process	Some types of events (such as requests for information or other non-incident related events) are sent to other parties outside of the CSIRT for handling. No further CSIRT activity is required.
Event is closed	Event is clearly not an incident or decision is made to take no further action. Event is documented appropriately and closed.

Subprocess	Subprocess Requirements/Written Procedures/Key People/Technology/Other
D1. Notice Events (reactive)	• Reports of potential incidents from internal constituency (people seeing anomalies) • Reports from internal users to IT that something is wrong. They may describe symptoms, anomalies, or anything weird (such as files not found, a message that they are already logged in, a virus download, an odd error message). A report of a potential incident can include the event description, POCs, and other details. IT then must pass this information on to Detect so that it goes through the processes of Triage and Respond. • Reports of incidents from external sources • Reports of advisories, alerts, etc. from external sources. Use lists of places, sources, etc. that are trusted. Dynamic lists that should be kept up-to-date. Can include sites, news groups, vendor sites. Need to know which sites become old and be aware of new ones. • Notifications of new potential problems. Advisories from CERTs, vendors, etc.; incidents reported from externals; daily summaries of activities from other CERTs. • Templates for reporting noteworthy information
D2. Receive Information	• Can get information via emails, news bulleting reports, etc. • If no further action is needed, close event. • The CSIRT constituency could be the source of the incident, an intermediate point, or the one under attack. May get reports from external entity that this constituency is attacking the external entity. • An event could be called an incident at this point, or not, if staff is unsure.
D3. Monitor Indicators (proactive)	• Monitor networks and hosts, proactive vulnerability evaluation, public monitoring/technology watch, etc. • Monitor logs, hosts, networks, alerts from IDS, net flows, firewall alerts, firewall logs, host logs, event logs for windows/Unix, application logs, user accounts/logs. Some things like AirCert have different types of IDS. Other types of logs can also be monitored. Look for suspicious activity, bad trends, errors, and alerts. Monitoring usually requires human interpretation of results. • Proactive scanning like red teams, any type of vulnerability evaluation (maybe something like OCTAVE), for organizational vulnerabilities, can also provide useful information. • Technology watch, new products, web sites, tech trends, news bulletins, any current activities, anything of interest that might spell a future problem, virus news. Being aware of and alert for possible trends and changes. May use access ID obfuscation to hide real identity when logging onto some boards, discussion sites, etc. • General awareness also enables CSIRT staff to answer management questions on current issues and explain how they are being dealt with.

D4. Analyze Indicators	• The information from monitoring is analyzed to determine if action is needed. • Usually this is a simple analysis to decide if the information indicates an event is occurring/has occurred. Other, in-depth analyses occur later in the process. This is the first cut at deciding if anything needs to be done—if this is a potential event that needs action or even further analysis (to Triage) or if the event can be closed or reassigned to another part of the organization. Analysis should indicate why this event is significant, what might be affected, etc. • If indicators require no further action, then close the event. Closure of an event requires proper documentation and archiving of information. No documentation or archival is not recommended, although in practice some information may be so trivial or unimportant that little is needed and some information may be discarded. • An event could be called an incident at this point, or not, if staff is unsure.
Side notes	A coordination center may play a role in Detect. It can be either an internal or external group. Having situational awareness and cyber intelligence helps in understanding the severity of an issue. For example, if someone asks for an incident report form, knowing that there have already been a dozen requests provides the indication that there's an issue to follow up on now. Or knowing that the request comes from a constituent bank and there's been a report of a bank being hacked indicates that something needs to be investigated. Situational awareness is knowing when there is a coincidence of information/events or trends coming together. Pattern analysis and trends, correlation of data, combining proactive and reactive data, internal and external. A first pass at data correlation occurs during Triage, a second more detailed pass occurs during Response type of analysis. May be largely mental activity, may be supported by tools. Miscellaneous notes: • Some information gathered from monitoring indicators becomes generally useful information and could be used during Prepare. • When there's a change in personnel between one box and another, the actual effectiveness of communication is one thing that needs to be considered. • Some CSIRTS may cross into physical security (e.g., when a report comes in of a stolen laptop that could allow access to the infrastructure).

Context for T: Triage	
Applicable Table Element	Additional Information
Objectives	Review of information to determine its validity and decide what to do with it. Filtering and prioritizing. This is a preliminary analysis to determine what initial action to take. There are many kinds of analysis – is it an incident or not, does it need a response, are they already in the tracking system, already exploited. Can be as simple as a set of criteria for help desk personnel to follow when making assignments. Can be one person doing all activities. If later activities determine that the category or priority or even assignment was incorrect, it will be corrected during that step. A return to Triage does not occur. Depending upon the nature of a team, some amount of threat assessment may be performed during Triage (as opposed to during Response) to determine a more correct category, priority, and assignment.
Triggers	When event information arrives that needs to be triaged or if an event is reopened and re-categorization, prioritization, or assignment is needed.
Completion Criteria	
Policies and Rules	
General Requirements	When secure handling is required; this does imply that approved configurations of the relevant infrastructure components are being used.
Inputs	Input/Description/Form
Event information	- Other electronic forms of reporting or sending events can include web applications and third-party/vendor products. - New event information can be added to existing events or used to re-open older events.
Outputs – Decision	Output/Description/Form
Event is assigned to a technical or management response	- Events that move to Respond (either technical or management response) are categorized, prioritized, and assigned in Triage. - Events are not assigned directly to legal personnel for a legal response. A management decision must be made to involve legal. - Events may be assigned based on an ongoing or previously closed incident.
Event is reassigned outside of the incident management process	Events may be reassigned outside the incident management process when action is required by others but no further incident management action is needed.
Event is closed	Events are closed if no further action is required. Closed events are properly documented and archived.

Subprocess	Subprocess Requirements/ Written Procedures / Key People / Technology / Other
T1. Categorize and Correlate Events	• Assign event to some category, usually from a list of predetermined categories. • Categorization and correlation may be iterative (i.e., categorize the event, look for similar events, and re-categorize based on correlated information). • Correlation may be a matter of determining if the event is part of an ongoing incident or using situational awareness to correlate several disparate events into one complex incident. More mature teams will be better able to correlate events and information. • There is always some form of Categorization, even if it's automatic. Some functions may also have auto-response/protect functions embedded in the systems/tools, self-repairing/self-healing. • Categorize always occurs first, then prioritize, then assign to someone to handle. Categorization includes even the simplest kinds of categories, including an existing checklist of types used by Help Desk personnel. Such lists could include "who event is from" categories such as information from important customers or others. • An event could be determined to need no further action, and it could be closed. • Categories can include: information request, incident report, vulnerability report, types of attack, or outcomes of attack.
T2. Prioritize Events	• Certain types of events require different handling and have specified priorities depending upon who, what, when, extent, where, etc. Lists used during these activities should define the specifics. • Determine a priority for this event. Priority does determine how fast or what level of response or activity is taken by the assignee and could indicate who is assigned the event. • Hotlists can be used to specify very high priorities; this is usually dictated by who is reporting the incident, but also may be specific types of events or affected IP addresses. Even the hotlist people could get bumped down if the event is not really a critical item. • It is possible to get a NULL priority for an event – equivalent of Not Applicable; these may be closed or reassigned outside the incident management capability. • Prioritize includes hotlists, predetermined priorities for some types of events, thinking about priorities, and second-guessing the hotlists and predetermined lists. Might need to look at additional data for a final determination of priority.

T3. Assign Events	• Can assign new events to staff who handled older, closed events when the event is reopened or they can be assigned to whoever is handling a related, still-open event. • Assign one (or more) persons to continue looking at the event. • May also have notification as well as assigning to someone to handle it. Notification of legal, media, human relations, status reporting all along. • Some assignments may be driven by the category and priority (predetermined). The event may be assigned for a technical response (T1) or a managerial response (T2). It may also not be assigned at all and be closed instead. Assign can go in several directions, such as incident handler (tech); artifact handler (tech); vulnerability handler (tech); malicious code/virus handler (tech); platform, applications, OS, infrastructure specialists (tech); other CSIRTs (external groups) (tech); management (high priority/visibility, escalation, etc.) (mgmt); human resources (mgmt); public relations/media interface (mgmt); investigators (legal – although management will initiate); law enforcement (mgmt/legal); legal council (mgmt/legal)
Side notes	Although the CSIRT itself could be an outsourced, third-party MSSP, in this work process flow, it is always referred to as the CSIRT and is not included under any reference to a third party. Triage may or may not notify others of the event (e.g., PR, management). Notifying others depends on the event, its category, priority, etc. and what the requirements are for that specific type of event. Events may be classified as incidents at any time during these activities or later during Respond. Triage answers the following questions: • Is it an ongoing incident (e.g., it hasn't been closed yet or is awaiting closure)? • Has it happened before? • Is it a known type of attack or unknown? Fix if known, no standard if new, anything similar? • Who? (may direct speed and level of response, escalation procedures) • What type of incident? • What's the impact, scope of impact (number of computers, users)? Was confidential data exposed? What happened? Note that some exceptions to the order of activities could occur. Significant events may be assigned immediately to someone to handle before any categorization or prioritizing (formally getting into the system); e.g., a senior manager sees the incoming report and immediately has the best technologist start working it.
Side notes, cont.	Miscellaneous notes: • Prepare (P) comes before Triage (T) so you have a chance to come up with fixed or canned responses, known responses, cheat lists, hot lists, checklists, etc. • When there's a change in personnel between one box and another, then the actual effectiveness of communication is one thing that needs to be considered.

Context for R: Respond	
Applicable Table Element	Additional Information
Objectives	Understand what the problem is, contain, recover/repair, become operational, and archive incident report. New event information can also point to an ongoing incident and can be merged into that incident.
Triggers	
Completion Criteria	Note that legal activity can continue long after technical and management responses have been completed. An incident may be closed and archived before a legal response is complete. However, much of the legal-related information (e.g., warrants, court proceedings) would not be included in any incident information and would likely be kept in separate legal systems, databases, etc. Incidents may also be reopened if later information or events warrant reopening. Reopening an event can be driven from either Detect (e.g., new information that changes a decision to close the event), Triage (e.g., another related event that makes the older event more important), or from anywhere in Respond (as someone realizes a link to a previously closed event). There can be the following types of responses: technical response, management response only, mix of technical and management or management and legal, or a mix of all three.
Policies and Rules	
General Requirements	
Inputs	Input/Description/Form
Assigned events	- Events become incidents at some point from Triage through Response when those analyzing and responding to the event decide that it is an actual incident. The latest point at which an event can be determined to be an incident is when it goes to closure. - Input—event information from Triage with value added. May include support information, monitoring/proactive info, incident/reactive info, advisories/alerts (reactive), triage info, other external info. Minimal set of info; some additional info such as authentication logs.

Context for R: Respond	
Outputs – Decision	Output/Description/Form
Postmortem is required; personnel from other organizational processes need to be notified; internal and external stakeholders need to be notified; event or incident is closed.	At a minimum, document and archive; the rest is optional. Documentation for a closed incident includes all relevant information gathered during Detect, Triage, and Respond such as who, what, when, where, extent, what was done or not done, what was learned, actions taken, costs, statistics, types of tools used, specific lessons learned (such as trends, improvements, knowledge that expands the body of information about incident response, what to do better next time, etc.).
Event or incident is closed	- Lessons learned may be for the constituency or the global community. - Other forms of outputs that are part of closing the incident are workshops, invitation-only gatherings, collaborations, training, etc.—whatever it takes to get the message out and ensure adequate handling and closure. - Legal information may be different and may include forensics, court/legal/prosecutorial evidence, human resources actions, disciplinary actions, regulatory actions, etc. Closing rationale examples: all actions were successful; nothing else could be done; turned over to Legal; etc. Each organization will need to set guidelines and criteria for closing incidents.
Subprocess	Subprocess Requirements/Written Procedures/Key People/Technology/Other
R1. Technical Response	- Technical response is one of the more complicated activities, and on-the-job-training is usually an important component for teams. Can be done with or without formal procedures. - Incident handlers, vulnerability handlers, artifact analysts, malicious code analysts, all do similar things. They receive information, analyze, and respond as appropriate. Response could be on-site by the team, support to another team or group, or coordination or sharing of information with others. Details are different, such as who performs the repair. IT is usually involved in the technical responses. - Possible details of a response (whoever is assigned responsibility gets the event information): - Find out what occurred or verify that the incident occurred—when, where, who, how, scope of event, other relevant information, outside or external chatter, similar reports. This may involve additional gathering of information or follow-up discussions with the information source. (analysis) - Perform additional or more in-depth correlation with other ongoing or previous events and other relevant information. - Gather additional data if needed—call site, look at CERT/CC information. (analysis) - Make recommendations to contain incident. (response) - Take steps to contain incident. (response) - Notify whoever needs to be told—constituency, alerts, announcements, ancillary people, victims of attacks, sources of report, etc. (response) - Collect evidence such as forensic, legal, etc. (response) - Recovery and repair, which includes some Protect, such as turn off unwanted services. (response) - Coordinate within Technical Response. - Technical analysis includes an impact analysis. Incident could turn into a vulnerability that needs to be patched – need to know then how many PCs, what kind of code it is, how it works, how to fix it.

Context for R: Respond	
	• Reprioritization, additional correlation, recategorization, and even reassignment are possible at this step if analyst determines a mistake was made. If coordination is required with management and legal, it is addressed in Coordination. • Response plan details will vary. May involve additional personnel to carry out plan and communication. May include identifying and determining a coordinated technical response with actions from other CSIRTs or other external technical parties or with other internal technical groups (such as an independent IT). • Carry out the response plan—pure technical coordination of activities may involve status and reporting with external technical groups. Could include notifying whoever needs to be told – constituency, alerts, announcements, ancillary people, victims of attacks, sources of report, etc. Coordination with other technical groups may be needed to conduct external actions or actions that must be carried out by internal/non-CSIRT personnel. • Decide if additional technical response is needed or if incident can be closed. Closing can occur because all actions have been taken to resolve it or nothing else can be done within the bounds of the resource and time constraints. • Vulnerability handling = analysis only. Vulnerability patching is part of incident response. In other words, you patch based on an incident or report of an incident, not a vulnerability alert, as the vulnerability alert may be irrelevant. Vulnerability handling includes a technical code analysis, although only mature teams can do this. Impact analysis determines what the threat is and what is exposed. Patch then if needed.
R2. Management Response	• Management response could be called for during technical response, if it was not already called for from Triage. • Management response includes all types of management activity, including human resources and public relations. Only legal response is broken out separately from other types of response because of its unique aspects. • Management—all non-technical response activity except legal. Senior managers, PR, HR, etc. receive event information, conduct non-technical analysis, and respond (non-technical). Management analyses methods and techniques are different from technical. Their response actions are different based on who they are, e.g., HR actions, PR releases etc. Only management can kick off the involvement of legal-type personnel. Coordination across managers may be required. • Reprioritization, additional correlation, recategorization, and even reassignment are possible at this step if analyst determines a mistake was made. If coordination is required with technical and legal, it is addressed as an overall coordination or control function. • Inclusion of a legal response may be decided at this stage, requiring coordination across management and legal (and optionally technical). • Decide if need more management response or if done. Closing an incident can occur because all actions have been taken to resolve it or because nothing else can be done within the bounds of the resource and time constraints.
R3. Legal Response	• Legal responses may produce information and results that are more legal than incident related, such as investigative and prosecutorial data. Such results are

Context for R: Respond	
	unique to the legal domain and are not considered outputs of the incident management process. This type of information is also not likely kept as part of an incident report. Summary information, legal decisions, or advice (e.g., that legal action was successfully pursued or a criminal investigation is underway) may be included in the incident report. Legal issues can be criminal, civil, or even privacy laws. • Legal response can be initiated only through management response. A rare exception might be a direct connection from one legal representative to another; however, that is equivalent to an event report coming in from a legal channel and will more than likely require technical and management response. Management must make the decision to coordinate with internal legal personnel or at least be involved in the decision. If external legal issues such as law enforcement become involved, management is at least notified and is more than likely involved in the decision (if there is a corporate decision to make). If technical data collection and analysis are required, the technical response side may provide that work. Legal group may also have its own technical personnel. • Legal refers to internal legal aspects—those requiring the corporation’s own legal counsel. Involving external law enforcement results in the external people conducting some of their own activities as well. Consider the following: international, national/federal, state, local, domain, internal, and partner/stakeholder laws, regulations, standards, and penalties. Legal is frequently asked to provide legal advice, deal with criminal and civil prosecutions and investigations, and work with external organizations or law enforcement in legal matters. Legal advice could include what relevant laws and regulations to follow or guidelines for handling data supporting, ensuring the appropriateness of legal contracts (e.g., NDAs), what evidence to collect and how for both internal and external investigations and prosecutions, etc. Related to external contacts with law enforcement—make recommendations, contain, notify, collect evidence, repair, and recover. • Coordinate as needed with external law enforcement. If external law enforcement brings their own technical people in, then some coordination may be required with the corporation’s technical people, although in some cases law enforcement may simply take what they need. Corporate legal advice on dealing with the confiscation of equipment, etc. may be needed. • Closing an incident can occur because all actions have been taken to resolve it or because nothing else can be done within the bounds of the resource and time constraints. • Note that some communications with stakeholders and constituents may require a review from the corporation’s legal counsel.
Coordinate Technical, Management, and Legal Responses	• This overall coordination effort is used to manage all of the parallel activities, although coordination may simply be including one of the people from the specific type of response teams. Anyone in a branch (technical, management, legal) may need to coordinate efforts with people in other branches or with people external to these three branches. • Guidelines for coordination requirements may vary for different types of events. • Coordination of notification to relevant parties may also be required. • Either the initial technical or management responder can decide coordination is required. Management can also decide to include legal through the coordi-

Context for R: Respond	
	nation activity. Decision to coordinate comes from technical response or management response. Escalation decisions would also result in coordination and attention from higher levels of management. Need escalation criteria for what and when and to whom to escalate. Data and processes used during escalation might be somewhat unique. Rationale is different. • Coordinate would include – Determine participants (obviously, if participants are not available adjustments would be made). – Analyze incident (may be any kind of analysis). This may be in addition to analyses done already during technical or management response. – Develop coordination plan: Assign response activities, responsibilities, and schedules. – Initiate other response group activities, get status back. – Track progress, gathering status as needed from participants. – Close incident when all participants are in agreement that incident can be closed. Closing an incident can occur because all actions have been taken to resolve it or because nothing else can be done within the bounds of the resource and time constraints.
Side notes	Note that closure of an incident could occur at variable times; e.g., technical response could be completed before management response and before legal response (which could go on for years if prosecution becomes a part of a legal response). SMEs could also be third parties; security staff could be physical or cyber security staff. Additional assignment of activities can occur at any time during response. Closing an incident under Response: • verification that all of the necessary steps, documentation, etc. are complete. Sometimes includes making sure everyone completed the necessary response activities. • notification of closure and final status to stakeholders and participants affected, management, incident reporters • formal documentation, including status reports for management • archival of all incident information, including email, attachments, reports, etc. When closing an event, the nature of the event can dictate the depth and formality of documentation, but once the event is determined to be an incident, formality and completeness of documentation and archival is required. Complete all documentation relative to the incident, including any unfinished fields in reports and other items left undone while trying to respond. • Make all changes and updates, and complete all report items. • Write any required status reports or summary reports for managers and constituents. • Optionally notify constituents that incident is now actually closed. • Archive all relevant information about the incident. When there's a change in personnel between one box and another, the actual effectiveness of communication is one thing that needs to be considered.

Appendix B: Acronyms

CAIF	common announcement interchange format (formerly common advisory interchange format), “an XML-based format to store and exchange security announcements in a normalized way” (http://cert.uni-stuttgart.de/projects/caif/)
CERT/CC	CERT Coordination Center (http://www.cert.org/)
CIO	chief information officer
CISO	chief information security officer
CISSP	Certified Information Systems Security Professional (https://www.isc2.org/cgi/content.cgi?category=19)
CMM	Capability Maturity Model (http://www.sei.cmu.edu/cmm/)
CMMI	Capability Maturity Model Integration (http://www.sei.cmu.edu/cmmi/)
CND	Computer Network Defense
CNO	Computer Network Operations
COBIT	Control Objectives for Information and related Technology (http://www.isaca.org/cobit)
CSF	critical success factor
CSIRT	computer security incident response team
CSO	chief security officer
DARPA	Defense Advanced Research Projects Agency (http://www.darpa.gov/)
DoD	U.S. Department of Defense (http://www.dod.gov/)
ESM	enterprise security management
FFIEC	Federal Financial Institutions Examination Council
FIPS	Federal Information Processing Standards (http://www.itl.nist.gov/fipspubs/)
FIRST	Forum of Incident Response and Security Teams (http://www.first.org/)

GAISP	Generally Accepted Information Security Principles (http://www.issa.org/gaisp/gaisp.html)
HTML	Hypertext Markup Language (http://www.ietf.org/rfc/rfc1866 and http://www.w3.org/MarkUp/)
IDMEF	Intrusion Detection Message Exchange Format (http://www.ietf.org/html.charters/idwg-charter.html)
IDS	intrusion detection system
IODEF	Incident Object Description Exchange Format (http://www.ietf.org/html.charters/inch-charter.html)
ISAC	information sharing and analysis center
ISP	Internet service provider
ISSA	Information Systems Security Association (http://www.issa.org/)
IT	information technology
ITGI	IT Governance Institute (http://www.itgi.org/)
ITIL	IT Infrastructure Library (http://www.ogc.gov.uk/index.asp?id=2261)
MSSP	managed security service provider
NAP	network access point
NIC	network information center
NIST	National Institutes of Standards and Technology (http://www.nist.gov/)
NOC	network operations center
NSP	network service provider
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation (http://www.cert.org/octave/)
RSS	RDF Site Summary; or Rich Site Summary; or Really Simple Syndication
SEI	Software Engineering Institute (http://www.sei.cmu.edu/)
SKiP	Security Knowledge in Practice (http://www.cert.org/security-improvement/skip.html)

SME	subject matter expert
SOC	security operations center
SOP	standard operating procedures
XML	Extensible Markup Language (http://www.w3.org/XML/)

Appendix C: Glossary

activity	an occurrence in a system that may be relevant to the security of the system. The term includes security events (and security incidents) and those that are not. Until an occurrence can be identified or confirmed as a security event, it may be referred to more generally as just an activity.
advisory	[West-Brown 03]: a document that provides “mid-term and long-term information about problems and solutions suitable to raise awareness and help avoid incidents. They typically contain information about new vulnerabilities, but may also contain information about intruder activity.”
alert	[West-Brown 03]: “short-term notices about critical developments containing time-sensitive information about recent attacks, successful break-ins, or new vulnerabilities. There may already be complete information regarding the subject of an alert, but something may have changed to require the publication of new information.”
archive	[Shirey 00]: “(1.) Noun: A collection of data that is stored for a relatively long period of time for historical and other purposes, such as to support audit service, availability service, or system integrity service. (See: backup.) (2.) Verb: To store data in such a way. (See: back up.)”
archive system	a group of tools, mechanisms, or other elements that enable data to be archived
as-is state	the current or existing condition (e.g., of an organization’s incident management capability)
auto response tool	a device that automatically replies or reacts to a report
automated detection agent	a tool or device that recognizes and identifies something without human intervention
automated tool	a device or implement that works on its own

best practice	the highest rated or superior action or process to follow. In an evolving technological field (in which better practices may be identified in the future), this may sometimes be referred to as a “best current practice.”
business drivers	the resources and forces that shape or influence an organization’s decisions for success and profit
business function	the work or activity performed by a specified group in an organization to enable it to conduct its business, such as human resources, payroll and accounting, sales, information technology
capability	the ability or capacity to perform some task
categorization	the process of assigning a predefined category to some incoming information, activity, event, or incident
chain of custody	for use in legal prosecution, a documented record identifying the person who maintained physical ownership or control of evidence, from its time of collection until its presentation or admission into a court of law
change management	the process for controlling or administering alterations or differences to something
C-level manager	a person in a chief management position; one who administers or controls a specified operations area at the highest level of the organization, such as CIO, CEO, CSO
close	to designate as completed; no further action required
computer security incident (CSIRT)	[Brownlee 98]: “any adverse event which compromises some aspect of computer or network security”

computer security incident response team	In this document: a capability or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents. According to Brownlee et al.: “a team that coordinates and supports the response to security incidents that involve sites within a defined constituency. In order to be considered a CSIRT, a team must: provide a (secure) channel for receiving reports about suspected incidents; provide assistance to members of its constituency in handling these incidents; disseminate incident-related information to its constituency and to other involved parties” [Brownlee 98].
configuration management	the process for controlling or administering the setup or arrangement of something, typically a computer system or network
constituency	[Brownlee 98]: “the group of users, sites, networks or organizations served by the team. The team must be recognized by its constituency in order to be effective.” [West-Brown 03]: a specific group of people and/or organizations that have access to specific services offered by a CSIRT
coordination center	a focal point for harmonizing or organizing information or actions; in this text, an organization that coordinates incident and vulnerability reports and other relevant information across its constituency
correlation	a linked, causal relationship between two or more items
criteria	requirements or rules for making a decision or judgment
CSIRT hotline	a telephone number that can be called for contacting or reporting events to a computer security incident response team
CSIRT process change	a difference or alteration in the series of actions or steps for a computer security incident response team
CSIRT process need	a required (necessary) or wanted (desirable) series of actions or steps intended to bring about a desired result for a computer security incident response team
CSIRT requirement	a mandatory resource or need of a computer security incident response team
CSIRT vision	the desired future image of a computer security incident response team
data manipulation tool	a device or implement to rearrange information in a desired way

decision support system	a group of tools, mechanisms, or other elements that assists the making of choices
establish	to bring about or set into place something
event	see “security event”
event report	a detailed account of an occurrence in a system, typically a computer security event
executive manager	a person in a high management position, often one who administers other managers
external	outside or beyond the boundaries of a specified thing (For example, “external to the organization” would mean that a person is not a member of that organization but outside of it.)
general indicator	an identifying characteristic of something, at the broadest level
groupware	software programs that are used by two or more people, typically for communication (e.g., chat or discussions) or collaboration tasks
handoff	something (typically a task) that is passed from one person (or group) to another
hardened infrastructure	a set of underlying equipment (in this text, of a computer network) that has a sufficiently high level of security to prevent unauthorized penetration
help desk	a part of the organization that provides assistance or responds to problem reports or requests (typically computer-based problems)
improvements	desirable changes or advances in the quality of something
incident	In this text, the term implies a “security incident” or “computer security incident.”
incident handling	the processes used for handing an incident; in this text, the term includes the processes for detecting, reporting, triaging, analyzing, and responding to computer security incidents.

incident management	the processes for controlling or administering tasks associated with computer security incidents; in this text, the term implies management of a computer security incident, and includes all of the Detect, Triage, and Respond processes as well as the Prepare (improve, sustain) processes and the Protect processes outlined in this report. Incident management is the performance of reactive and proactive services to help prevent and handle computer security incidents. It can include security awareness and training functions, incident handling, vulnerability handling, assessment activities, IDS, and other services as listed in Figure 1 in this report.
incident response	an answer given or action taken by people designated to react to an incident. It is the process that encompasses the planning, coordination, and execution of any appropriate mitigation and recovery strategies and actions.
infrastructure	set of underlying equipment (of a computer network)
infrastructure protection requirements	the needs that enable the set of underlying equipment (of a computer network) to resist attacks or security breaches
input	something that feeds into a process
internal	inside or within the boundaries of a specified thing (For example, “internal to the organization” would mean that a person is a member of that organization.)
knowledgebase	a database (or archive) for storing acquired information
legal response	an answer given or action taken by people designated to react to any incident aspects related to or governed by the law
lessons learned	knowledge that is gained or identified after a completed activity
management response	an answer given or action taken by a manager or higher ranking authority within an organization; note that this response differs from “technical response”
mission	an assignment or duty, the purpose of an organization. For a given organization, this term is often identified or defined in a mission statement.
organization	a body of people that is organized and recognizable by some identifiable characteristic(s). Examples: a small business, a company, a government agency, a university department.

organizational CSIRT development project team	a group of people tasked with planning, creating, and implementing a computer security incident response team (or capability) for their organization
output	the outcoming result of a process
postmortem	a review that occurs after a completed event, often used to determine what went well and what needs to be improved in the organization's staffing, infrastructure, or procedures
predefined criteria	characteristics that are specified in advance
prioritization	the ranking or sorting in order of importance or urgency
process	a series of actions or steps intended to bring about a desired result
quality assurance check	a confirmation that the characteristics of an object, process, or procedure meet the specified (or expected) degree of excellence
rationale	a reason or justification for something
reassign	to assign or hand off a task to another individual (or group)
reporting requirement	a mandatory instruction or guideline for submitting an account of some specified activity (security event or incident)
request	a voluntary asking for some thing or action
resource	an available asset that can be used for help (to accomplish or produce an outcome)
response action	a task to be performed in reply or reaction to a report
response decision	the identification of a choice made in reaction to a report
response information	knowledge that is provided in reply or reaction to a report
risk assessment	[Shirey 00]: "a process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure"
security context	background information relevant to the security of a system or a situation

security event	[Shirey 00]: “an occurrence in a system that is relevant to the security of the system. (See: security incident.) [Comment] The term includes both events that are security incidents and those that are not.”
security incident	[Shirey 00]: “a security event that involves a security violation. [Comment] In other words, a security-relevant system event in which the system's security policy is disobeyed or otherwise breached.” See “computer security incident.”
security tool	a device or implement that can be used to enable or improve the security of a system or network
sensor	a device or tool that detects (and responds to) the existence of a given condition or stimulus
stakeholder	an individual or group that is interested in (or may affected by) the enterprise
subprocess	a lower level process
subprocess requirement	something (e.g., a resource, a condition, information) that is necessary for a lower level process
summary report	the documented findings that provide a brief overview of an event
technical response	an answer given or action taken by someone who is familiar with the technology-related aspects of a reported incident or vulnerability. This response typically could include a summary of their analysis of the incident, as well as recommendations or suggested steps for recovering from the activity and for hardening or securing the affected system(s). It can also include the execution of these actions. Note that this response differs from “management response.”
to-be state	the desired or future condition (e.g., of an organization’s incident management capability)
triage	[West-Brown 03]: “the process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling”
trouble ticket system	a group of tools, mechanisms, or other elements that enables the recording and tracking of a problem report (and its assignment and resolution). For example, see <i>NOC Internal Integrated Trouble Ticket System Functional Specification Wishlist</i> [Johnson 92].
unusual or suspicious activity	an occurrence that is out of the ordinary or that raises concern or doubt about its intent or impact; a potential security event

vulnerability

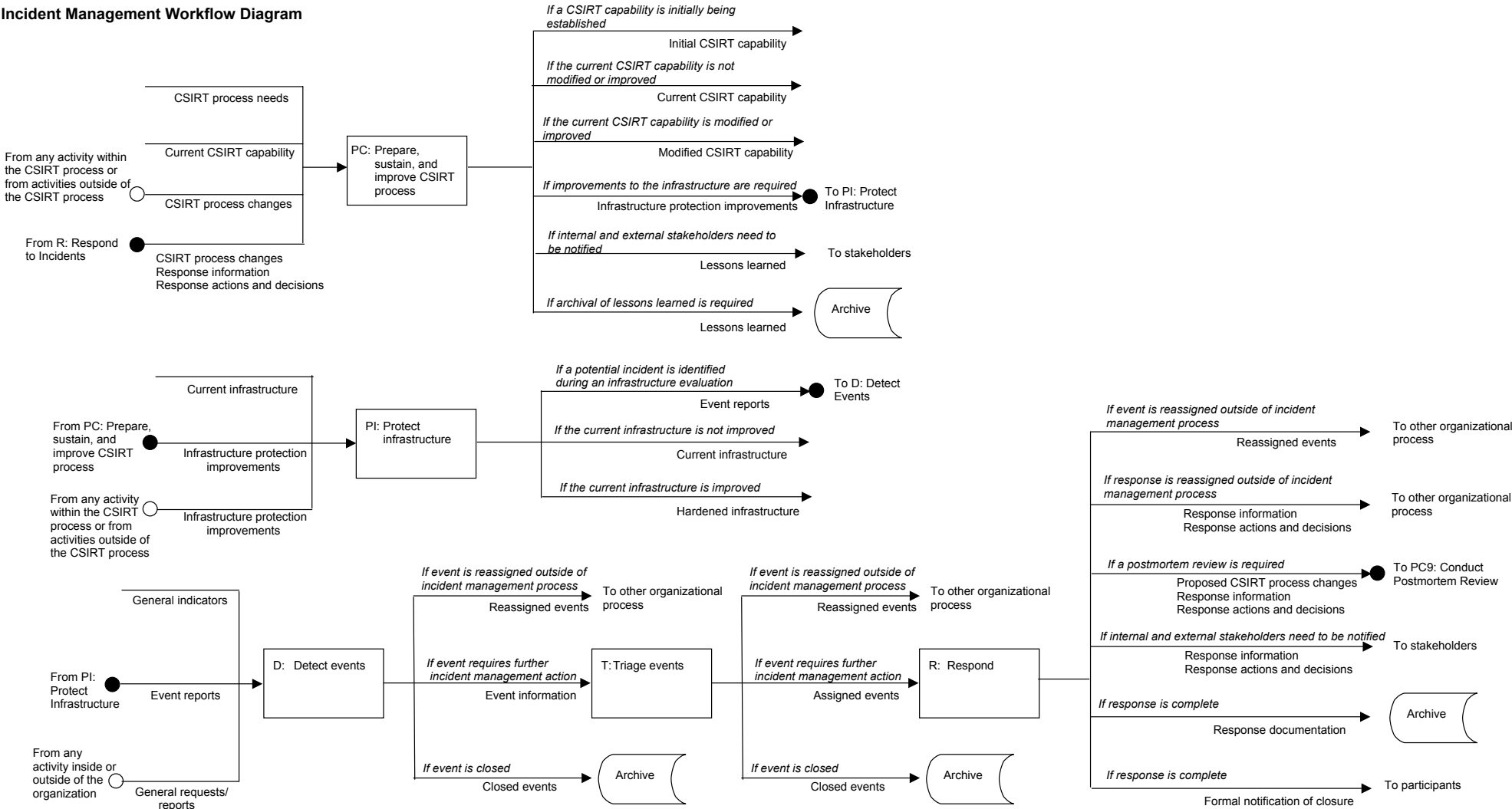
[Brownlee 98]: “a characteristic of a piece of technology which can be exploited to perpetrate a security incident.” [West-Brown 03]: “the existence of a software weakness, such as a design or implementation error, that can lead to an unexpected, undesirable event compromising the security of a system, network, application, or protocol”

**vulnerability
assessment**

an act or procedure intended to evaluate or identify the existence of known vulnerabilities (in a computer system or network)

Appendix D: One-Page Versions of the Process Workflow Diagrams

Incident Management Workflow Diagram

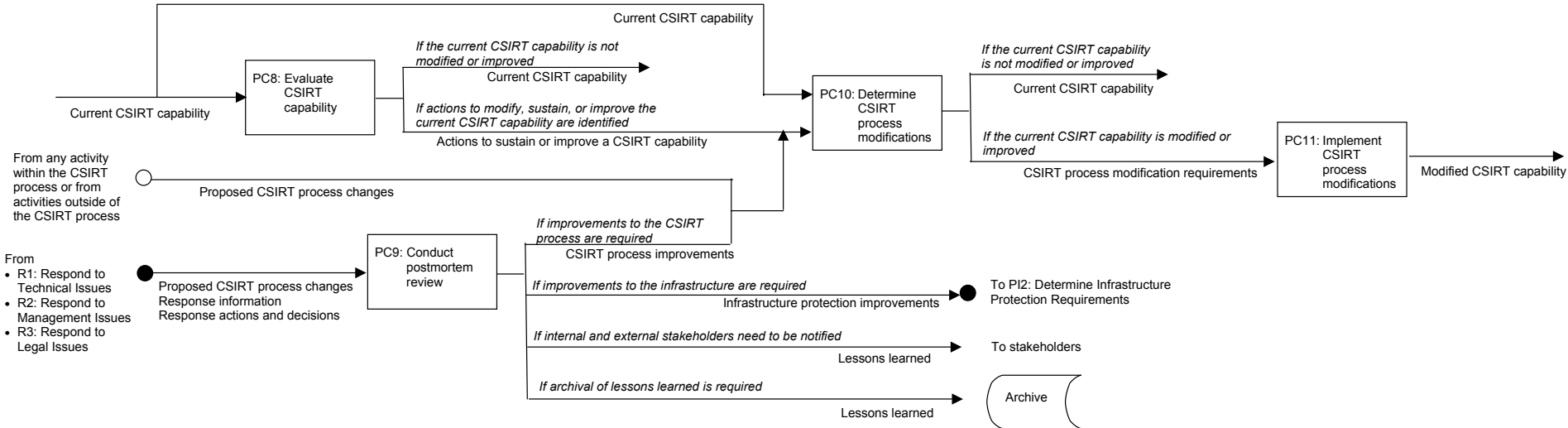
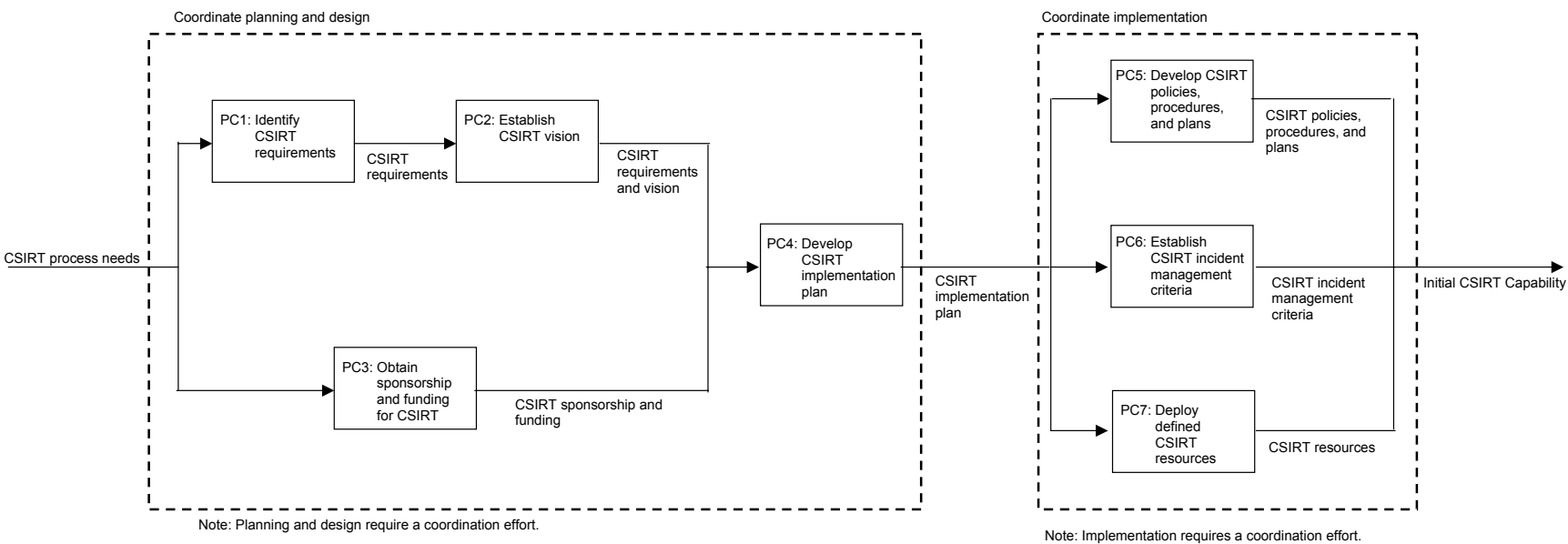


PC: Prepare/Sustain/Improve Workflow Diagram

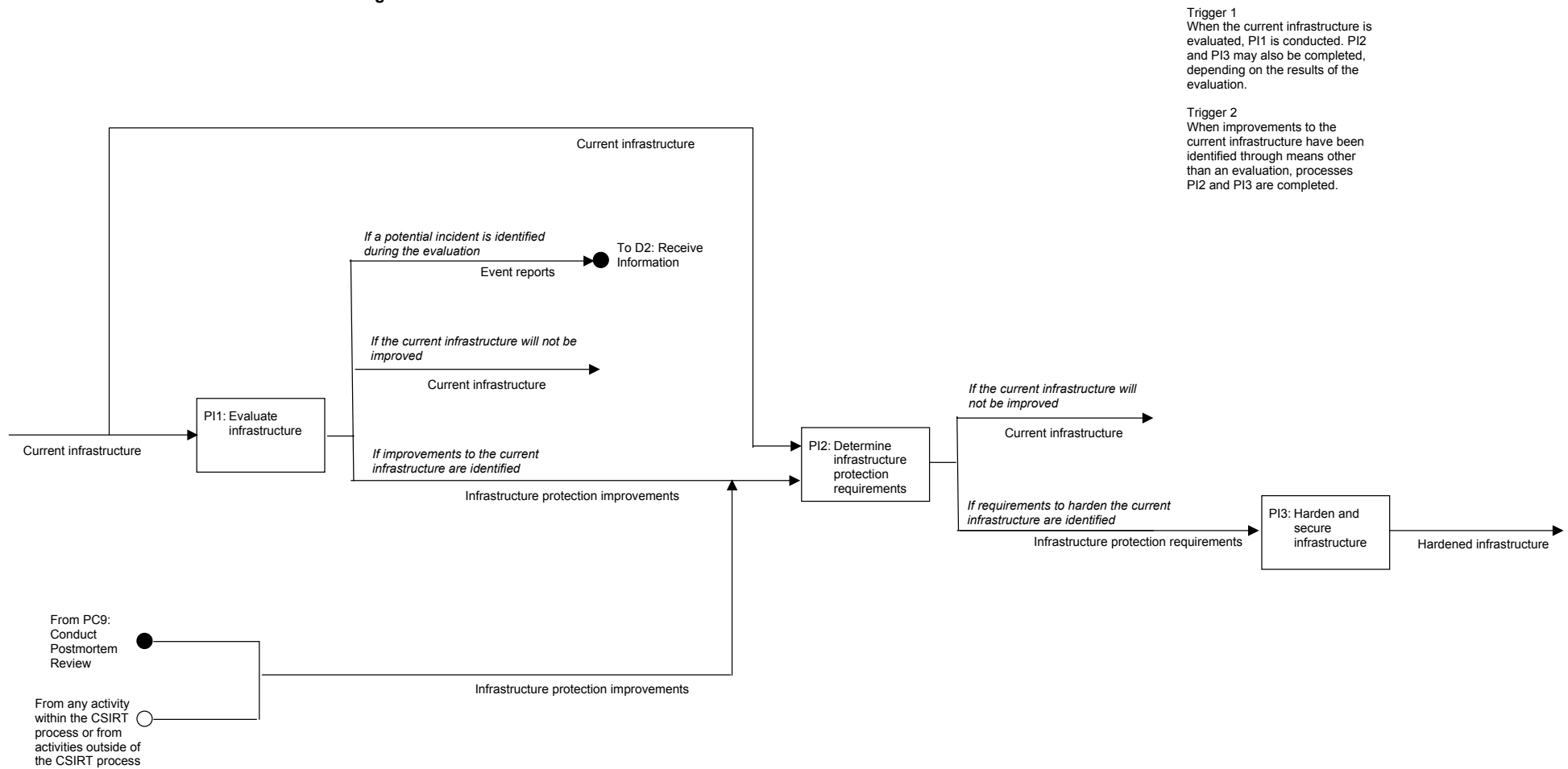
Trigger 1
When a CSIRT capability is initially being established, Processes PC1 through PC7 are completed.

Trigger 2
When changes or improvements to an existing CSIRT capability have been identified through means other than an evaluation, Processes PC 10 and PC11 are completed. PC 9 is optional. It is completed only when a postmortem review is needed to identify CSIRT process improvements.

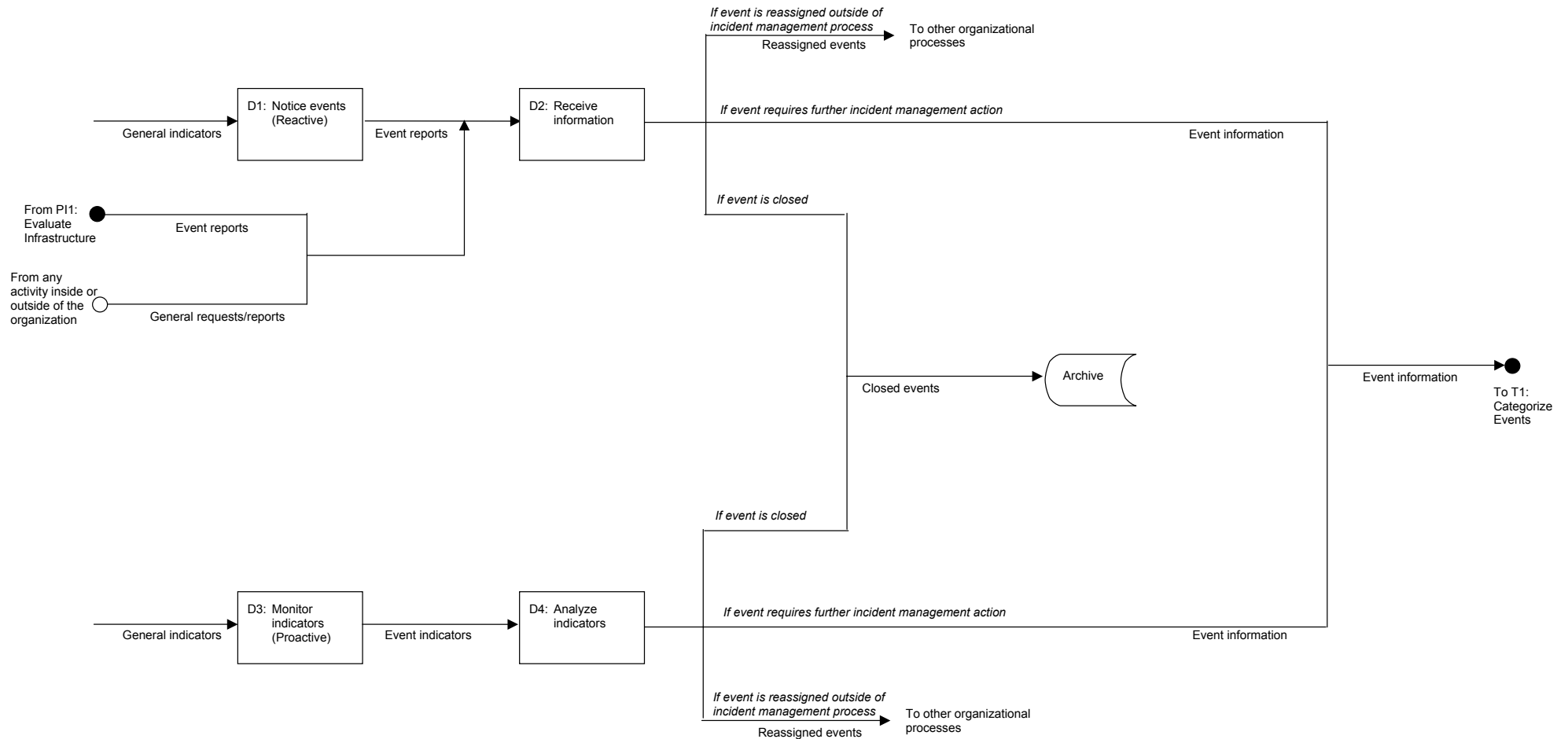
Trigger 3
When an existing CSIRT capability is evaluated, then PC8 is conducted. PC10 and PC11 may also be completed, depending on the results of the evaluation.



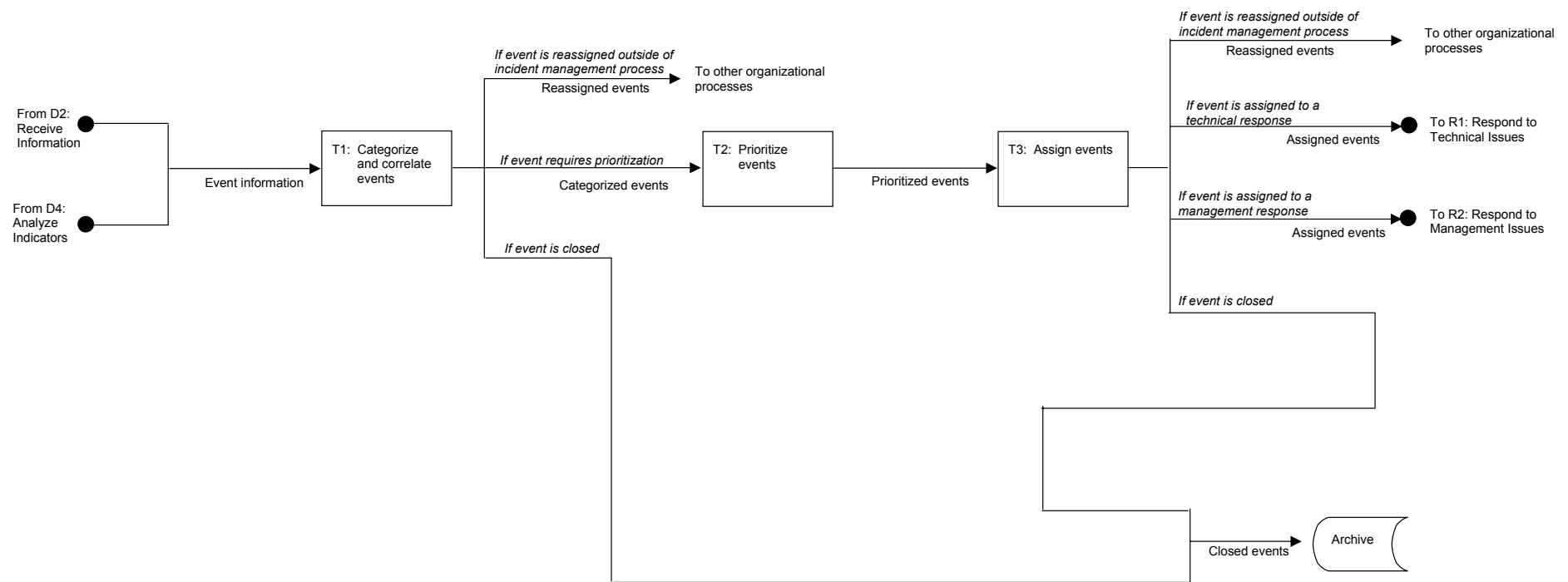
PI Protect Infrastructure Workflow Diagram



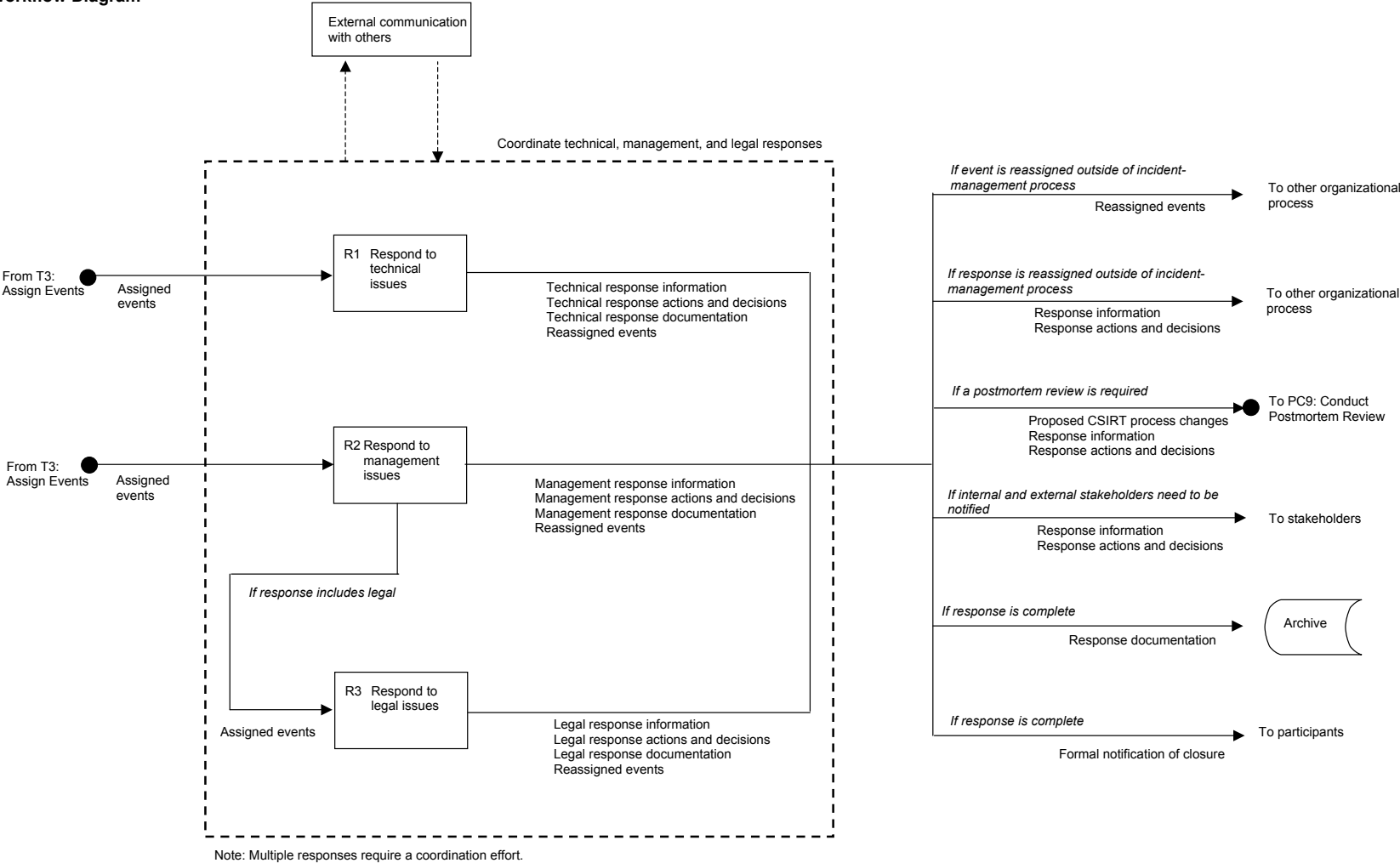
D: Detect Events Workflow Diagram



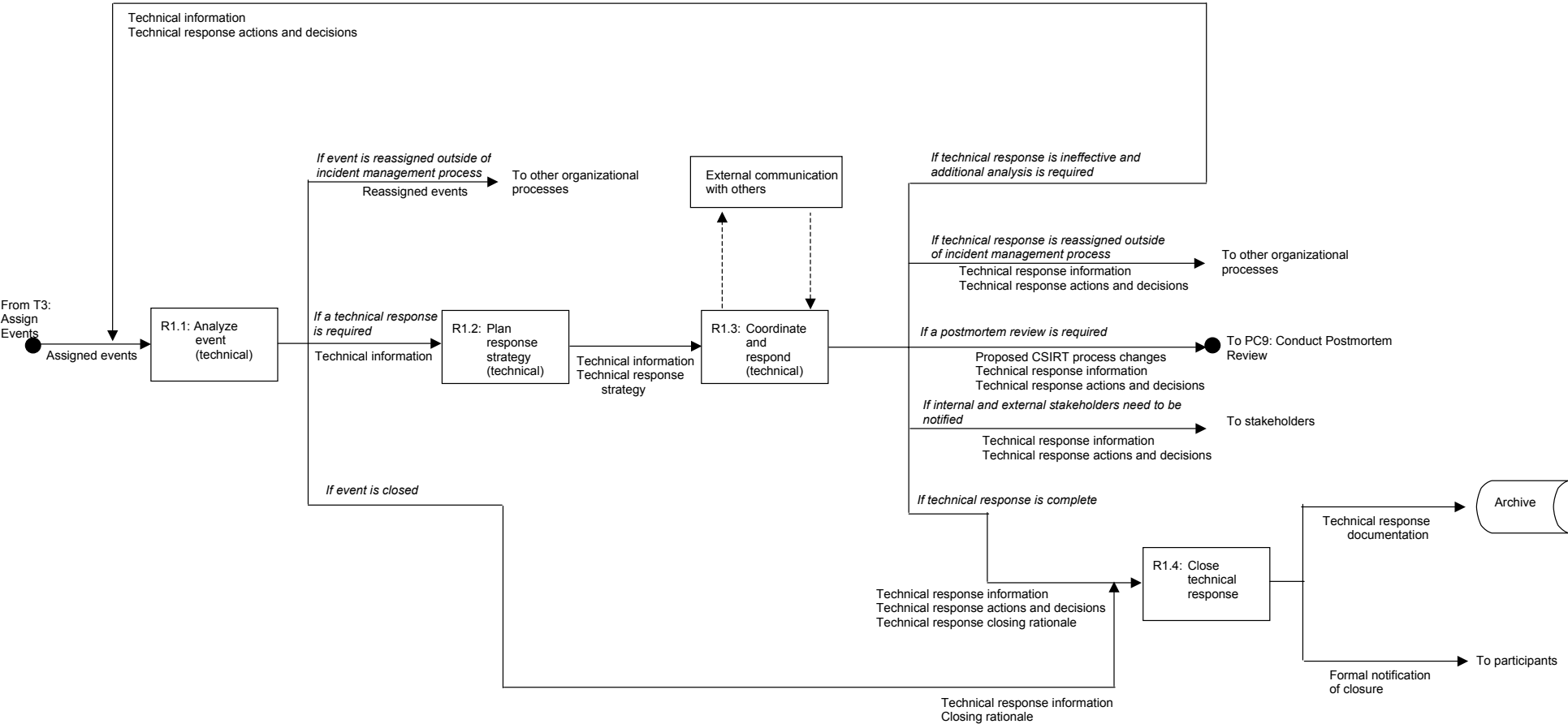
T: Triage Events Workflow Diagram



R: Respond Workflow Diagram

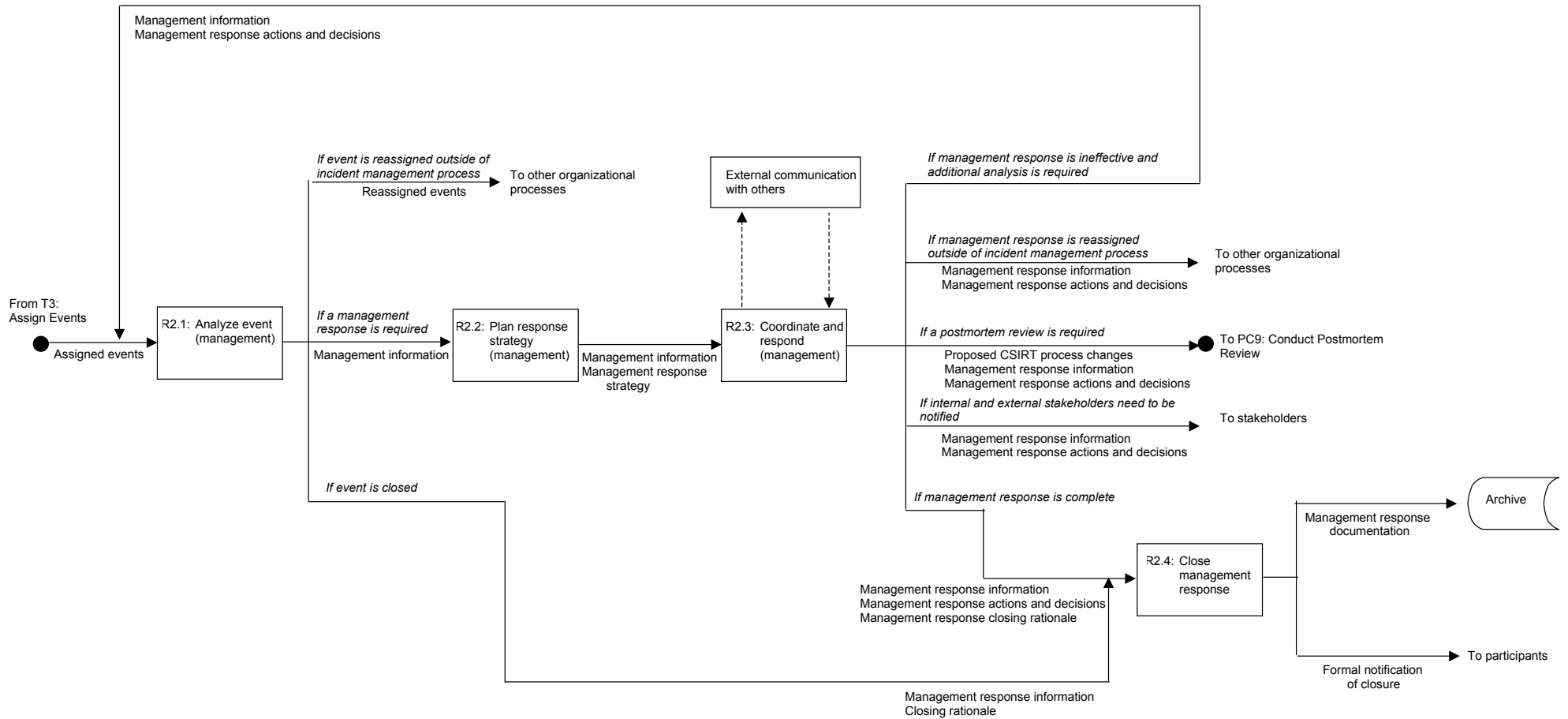


R1: Respond to Technical Issues Workflow Diagram



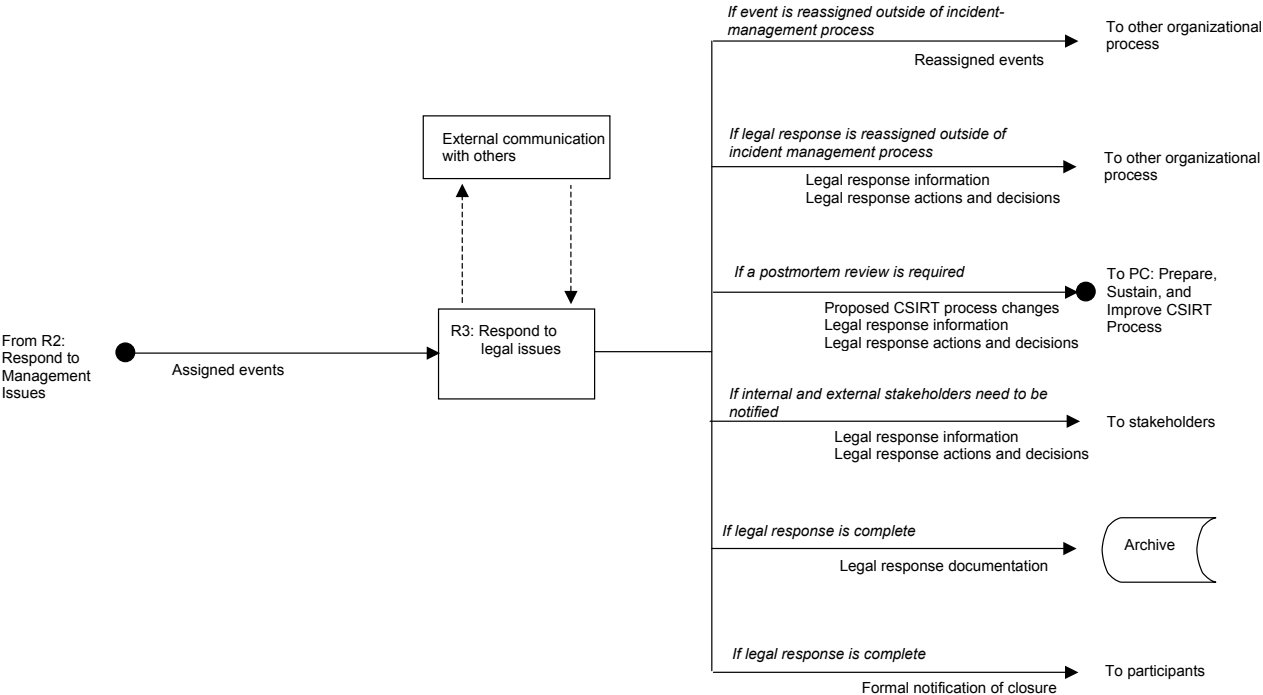
Note: If management or legal responses are part of an overall coordinated response, the coordination of all responses is embedded in R1.2, R1.3, and R1.4.

R2: Respond to Management Issues Workflow Diagram



Note: If technical or legal responses are part of an overall coordinated response, the coordination of all responses is embedded in R2.2, R2.3, and R2.4.

R3: Respond to Legal Issues Workflow Diagram



Appendix E: One-Page Versions of the Process Workflow Descriptions and Handoffs

PC: Prepare/Sustain/Improve

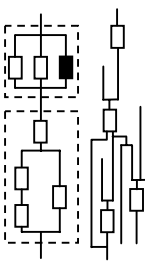
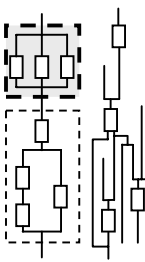
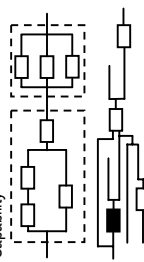
Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To create a formalized CSIRT capability that supports the mission and goals of the constituency - To improve an existing CSIRT capability that supports the mission and goals of the constituency	- When an organizational entity decides or is mandated to create a formalized incident management capability - When an organizational entity decides or is mandated to evaluate an existing CSIRT capability - When changes or improvements to an existing CSIRT capability have been identified through means other than an evaluation (i.e., through activities within or outside of the CSIRT process)	- When CSIRT formalized process, capability, or team is established (both short-term CSIRT operations as well as long-term CSIRT sustainment) - When CSIRT process is improved or enhanced	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Designated personnel model the CSIRT process after relevant standards, guidelines, and practices. - Designated personnel document and track results in accordance with CSIRT and organizational policies.

Inputs						
Input	Description	Form	Decision	Output	Description	Form
CSIRT process needs	This includes the drivers and conditions that indicate the need for a CSIRT capability when one does not currently exist. CSIRT process needs can come from a variety of sources, including local, state, federal, and international laws and regulations; relevant standards; site-security, IT, and organizational policies; general information collected as part of a CSIRT development project; and having suffered through an incident.	Verbal, electronic, or physical	A CSIRT capability is initially being established	Initial CSIRT capability	This includes the initial set of resources (people, processes, and technologies) required for the incident management process and deployed for that purpose. A CSIRT capability includes the following elements: - mission - constituency - set of services - defined organizational model or framework - assigned resources with designated roles and authority - appropriate equipment for performing incident management functions - secure physical and electronic infrastructures	People, processes, and technologies
Current CSIRT capability	This includes the existing resources (people, processes, and technologies) available to provide CSIRT services to a defined constituency.	People, processes, and technologies	The current CSIRT capability is not modified or improved	Current CSIRT capability	This includes the existing resources (people, processes, and technologies) available. There is no change to the current capability.	People, processes, and technologies
Proposed CSIRT process changes	This includes projected modifications to an existing CSIRT process. These changes can come from many different sources, including - proposed improvements resulting from observations about where the CSIRT process has failed (from R: Respond as well as from any activity within the CSIRT process) - modifications directed by an organization's management (e.g., changes to the funding profile, decision to outsource part of the process, change in mission, new requirements, change in services) - modifications mandated by laws and regulations	Verbal, electronic, or physical	The current CSIRT capability is modified or improved	Modified CSIRT capability	This builds on the current CSIRT capability by incorporating changes identified through various means. The end result is a modified set of resources (people, processes, technologies) available to improve or modify the incident management process.	People, processes, and technologies
Response information	This includes all relevant response-related data required to conduct a postmortem review.	Verbal, electronic, or physical	Improvements to the infrastructure are required	Infrastructure protection improvements	Infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure. During PC: Prepare/Sustain/Improve, these proposed improvements are identified during postmortem reviews and then forwarded to PI: Protect Infrastructure.	Verbal, electronic, or physical
Response actions and decisions	This includes the following data about the response: - technical, management, or legal actions taken - technical, management, or legal decisions made	Verbal, electronic, or physical	Internal and external stakeholders need to be notified Archival of lessons learned is required	Lessons learned	Lessons learned are a summary of how well the incident management process worked based on how well a specific response worked. These lessons are the result of either a formal or informal review of the actions, decisions, and occurrences related to the response.	Verbal, electronic, or physical

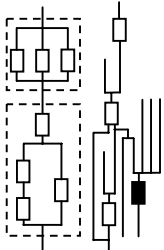
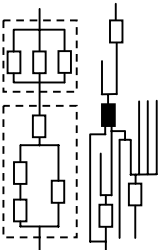
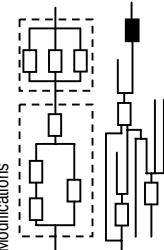
Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology	Other/Misc.
PC1: Identify CSIRT Requirements 	Designated personnel collect and review CSIRT process needs and determine requirements for the CSIRT capability. Inputs • CSIRT process needs* Outputs • CSIRT requirements	Designated personnel follow organizational project management and implementation guidelines or procedures Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when identifying CSIRT requirements Designated personnel follow organizational or CSIRT change management processes or guidelines.	Designated personnel for identifying CSIRT requirements can include – organizational CSIRT development project team – executive managers (i.e., any C-level manager) – business function managers – IT operations – representatives from administrative operations (e.g., legal, HR, PR, compliance) – representatives from constituency – representatives from law enforcement – representatives from critical infrastructures – third-party MSSP personnel – CSIRT development SMEs	Designated personnel can use the following technology when identifying CSIRT requirements: – documentation and publication technologies – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web)	• ---
PC2: Establish CSIRT Vision 	Designated personnel define the CSIRT vision, which includes the CSIRT mission, constituency, services, organizational framework, and resources. Designated personnel obtain approval of CSIRT vision. Inputs • CSIRT requirements Outputs • CSIRT requirements and vision	Designated personnel follow organizational project management and implementation guidelines or procedures Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when establishing the CSIRT vision. Designated personnel follow organizational or CSIRT change management processes or guidelines.	Designated personnel for establishing and refining the CSIRT vision can include – organizational CSIRT development project team – executive managers (i.e., any C-level manager) – business function managers – IT operations – representatives from administrative operations (e.g., legal, HR, PR, compliance) – representatives from constituency – representatives from law enforcement – representatives from critical infrastructures – third-party MSSP personnel	Designated personnel can use the following technology when establishing the CSIRT vision: – documentation and publication technologies – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) – decision support systems	• ---
PC3: Obtain Sponsorship and Funding for CSIRT 	Designated personnel obtain sponsorship and funding for establishing the CSIRT process. Inputs • CSIRT process needs* Outputs • CSIRT sponsorship and funding	Designated personnel follow organizational guidelines for obtaining funding and sponsorship. Designated personnel follow budgetary guidelines for acquiring and implementing project funding.	Designated personnel for obtaining sponsorship and funding for CSIRT can include – organizational CSIRT development project team – executive managers (i.e., any C-level manager) – business function managers – CSIRT sponsor – marketing and business development staff	Designated personnel can use the following technology when obtaining sponsorship and funding for CSIRT: – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) – financial and accounting systems	• ---
PC4: Develop CSIRT Implementation Plan 	Designated personnel develop the CSIRT implementation plan. Inputs • CSIRT requirements and vision • CSIRT sponsorship and funding Outputs • CSIRT implementation plan	Designated personnel follow organizational project management and implementation guidelines or procedures Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when developing the CSIRT implementation plan. Designated personnel follow organizational or CSIRT change management processes or guidelines.	Designated personnel for developing the CSIRT implementation plan can include – organizational CSIRT development project team – executive managers (i.e., any C-level manager) – business function managers – IT operations – representatives from administrative operations (e.g., legal, HR, PR, compliance) – representatives from constituency – representatives from law enforcement – representatives from critical infrastructures – third-party MSSP personnel – CSIRT development SMEs – CSIRT manager – CSIRT sponsor	Designated personnel can use the following technology when establishing the CSIRT vision: – project planning and management software – documentation and publication technologies – communication channels, encrypted when appropriate (email, videoconferencing, groupware, web)	• ---

Note: An asterisk (*) after an input to or an output of a subprocess listed in this table indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology	Other/Misc.
Coordinate Planning and Design 	Designated personnel coordinate planning activities when establishing the CSIRT process. Shared Information - CSIRT requirements and vision - CSIRT sponsorship and funding Output - CSIRT implementation plan	- Designated personnel follow procedures required for identifying CSIRT requirements, establishing the CSIRT vision, obtaining sponsorship and funding for the CSIRT, and developing the CSIRT implementation plan. - Designated personnel follow appropriate procedures for coordinating the planning and design of the CSIRT capability. - Designated personnel follow organizational or CSIRT change management processes or guidelines. - Designated personnel follow third-party	- Designated personnel for coordinating planning and design can include - key people involved in identifying CSIRT requirements, establishing the CSIRT vision, obtaining sponsorship and funding for the CSIRT, and developing the CSIRT implementation plan	- Designated personnel can use the following technology when coordinating planning activities: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - documentation and publication technologies	---
PC5: Develop CSIRT Policies, Procedures, and Plans 	Designated personnel define core CSIRT policies, procedures, and plans consistent with the implementation plan and document the results. Designated personnel obtain consensus and approval of CSIRT policies, procedures, and plans. Inputs - CSIRT implementation plan Outputs - CSIRT policies, procedures, and plans	- Designated personnel follow organizational procedures for documenting, verifying, and institutionalizing CSIRT policies, procedures, and plans. - Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when developing CSIRT policies, procedures, and plans.	- Designated personnel for developing CSIRT policies, procedures, and plans can include - policy and standards development staff - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - third-party MSSP personnel - CSIRT development SMEs - CSIRT staff - technical writers	- Designated personnel can use the following technology when developing CSIRT policies, procedures, and plans: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - documentation and publication technologies - project planning and management software	---
PC6: Establish CSIRT Incident Management Criteria 	Designated personnel develop appropriate guidelines for supporting the CSIRT processes as specified in the implementation plan, such as: - categories - priorities - triage strategies - response strategies - notification lists - escalation process Inputs - CSIRT implementation plan Outputs - CSIRT incident management	Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when developing the CSIRT incident management criteria.	- Designated personnel for establishing CSIRT incident management criteria can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development SMEs - CSIRT staff	- Designated personnel can use the following technology when establishing CSIRT incident management criteria: - documentation and publication technologies - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - project planning and management software	---

Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology	Other/Misc.				
PC7: Deploy Defined CSIRT Resources 	- Designated personnel identify and organize resources (e.g., staff, equipment, and infrastructure) as specified in the implementation plan when establishing the CSIRT process. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - CSIRT implementation plan </td><td> - CSIRT resources </td></tr></table>	Inputs	Outputs	CSIRT implementation plan	CSIRT resources	- Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when implementing CSIRT resources. - Designated personnel follow human resource policies and procedures for hiring and training staff. - Designated personnel follow organizational purchasing guidelines or procedures. - Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow security	- Designated personnel for identifying and organizing resources can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development SMEs	- Designated personnel can use the following technology when identifying and organizing resources: - documentation and publication technologies - HR systems - purchasing systems - systems and networking technology required to establish and operate a CSIRT capability - physical security systems - communication channels,	---
Inputs	Outputs								
CSIRT implementation plan	CSIRT resources								
Coordinate Implementation 	- Designated personnel coordinate implementation activities when establishing the CSIRT process. <table><tr><th>Shared Information</th><th>Output</th></tr><tr><td> - CSIRT policies, procedures, and plans - CSIRT incident management criteria - CSIRT resources </td><td> - Initial CSIRT capability* </td></tr></table>	Shared Information	Output	- CSIRT policies, procedures, and plans - CSIRT incident management criteria - CSIRT resources	Initial CSIRT capability*	- Designated personnel follow procedures required for developing CSIRT policies, procedures, and plans, establishing CSIRT incident management criteria, and implementing CSIRT resources. - Designated personnel follow organizational project management and implementation guidelines or procedures - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when coordinating the implementation of the CSIRT capability. - Designated personnel follow organizational or CSIRT change management processes or guidelines.	- Designated personnel for coordinating implementation activities when establishing the CSIRT capability can include - key people involved in developing CSIRT policies, procedures, and plans, establishing CSIRT incident management criteria, and implementing CSIRT resources	- Designated personnel can use the following technology when coordinating implementation activities: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - documentation and publication technologies	---
Shared Information	Output								
- CSIRT policies, procedures, and plans - CSIRT incident management criteria - CSIRT resources	Initial CSIRT capability*								
PC8: Evaluate CSIRT Capability 	- Designated personnel evaluate or assess the capability of the CSIRT and decide what to do (i.e., improve the current capability or make no improvements to the current capability). <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Current CSIRT capability* </td><td> - Current CSIRT capability* - Actions to sustain or improve a CSIRT capability </td></tr></table>	Inputs	Outputs	Current CSIRT capability*	- Current CSIRT capability* - Actions to sustain or improve a CSIRT capability	- Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when evaluating a CSIRT capability. - Designated personnel follow organizational procedures and methodologies for conducting assessments.	- Designated personnel for assessing the capability of the CSIRT can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - representatives from constituency - third-party MSSP personnel - CSIRT development SMEs - auditors, risk management staff, compliance staff - third-party or independent evaluators	- Designated personnel can use the following technology when assessing the capability of the CSIRT: - electronic evaluation or assessment tools - report writing systems - database system - communication channels, encrypted when appropriate (email, videoconferencing, groupware) - incident tracking system - trouble ticket system	---
Inputs	Outputs								
Current CSIRT capability*	- Current CSIRT capability* - Actions to sustain or improve a CSIRT capability								

Note: An asterisk (*) after an input to or an output of a subprocess listed in this table indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology	Other/Misc.				
PC9: Conduct Postmortem Review 	- Designated personnel conduct a formal or informal postmortem review to determine what was learned from a response and decide if any improvements need to be implemented. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Proposed CSIRT process changes* - Response information* - Response actions and decisions* </td><td> - CSIRT process improvements - Infrastructure protection improvements* - Lessons learned* </td></tr></table>	Inputs	Outputs	- Proposed CSIRT process changes* - Response information* - Response actions and decisions*	- CSIRT process improvements - Infrastructure protection improvements* - Lessons learned*	- Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when conducting a postmortem review. - Designated personnel follow organizational or CSIRT change management processes or guidelines.	- Designated personnel for conducting a postmortem review can include - CSIRT staff - CSIRT manager - IT staff - IT manager - third parties (e.g., service providers) - business function managers - CSIRT constituency - representatives from administrative operations (e.g., legal, HR, PR, compliance) - auditors, risk management staff, compliance staff	- Designated personnel can use the following technology when conducting postmortem reviews: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - database system - incident tracking system - trouble ticket system	---
Inputs	Outputs								
- Proposed CSIRT process changes* - Response information* - Response actions and decisions*	- CSIRT process improvements - Infrastructure protection improvements* - Lessons learned*								
PC10: Determine CSIRT Process Modifications 	- Designated personnel review proposed CSIRT process changes and improvements and decide what to do with them (i.e., develop requirements to implement proposed modifications or take no further action). <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Current CSIRT capability* - CSIRT process changes* - Actions to sustain or improve a CSIRT capability - CSIRT process improvements </td><td> - Current CSIRT capability* - CSIRT process modification requirements </td></tr></table>	Inputs	Outputs	- Current CSIRT capability* - CSIRT process changes* - Actions to sustain or improve a CSIRT capability - CSIRT process improvements	- Current CSIRT capability* - CSIRT process modification requirements	- Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when determining how to modify the CSIRT capability. - Designated personnel follow organizational or CSIRT change management processes or guidelines.	- Designated personnel for determining CSIRT process modification requirements can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - Third-party MSSP personnel - CSIRT development SMEs - CSIRT manager - CSIRT staff	- Designated personnel can use the following technology when determining CSIRT process modification requirements: - communication channels, encrypted when appropriate (email, videoconferencing, groupware)	---
Inputs	Outputs								
- Current CSIRT capability* - CSIRT process changes* - Actions to sustain or improve a CSIRT capability - CSIRT process improvements	- Current CSIRT capability* - CSIRT process modification requirements								
PC11: Implement CSIRT Process Modifications 	- Designated personnel acquire and organize resources (e.g., staff, equipment, and infrastructure) for implementing the requirements for modifying the CSIRT process. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - CSIRT process modification requirements </td><td> - Modified CSIRT capability* </td></tr></table>	Inputs	Outputs	CSIRT process modification requirements	Modified CSIRT capability*	- Designated personnel follow third-party best practice guidelines, procedures, laws, or regulations when implementing changes to the CSIRT capability. - Designated personnel follow organizational or CSIRT change management processes or guidelines. - Designated personnel follow security policies and best current practices when implementing changes to resources, equipment, and infrastructure.	- Designated personnel for implementing CSIRT process modifications can include - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development SMEs	- Designated personnel can use the following technology when implementing CSIRT process modifications: - documentation and publication technologies - HR systems - purchasing systems - systems and networking technology - physical security systems - communication channels, encrypted when appropriate (email, videoconferencing, groupware)	---
Inputs	Outputs								
CSIRT process modification requirements	Modified CSIRT capability*								

Note: An asterisk (*) after an input to or an output of a subprocess listed in this table indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Handoff from Any Activity Inside or Outside CSIRT Process to PC: Prepare/Sustain/Improve

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To successfully send CSIRT process changes from any activity to PC: - Prepare/Sustain/Improve - within defined time constraints - while handling information within the appropriate security context - while tracking the handoff in an appropriate manner	When CSIRT process changes are ready to be passed to PC: Prepare/Sustain, and Improve Process	- When CSIRT process changes have been sent to PC: Prepare/Sustain/Improve - When CSIRT process changes have been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Processes Involved			
Sending Process	Receiving Process	Object	Description
Any activity	PC10: Determine CSIRT Process Modifications	Proposed CSIRT process changes	This includes projected modifications to an existing CSIRT process. These changes can come from many different sources, including - proposed improvements resulting from observations about where the CSIRT process has failed (from R: Respond as well as from any activity within the CSIRT process) - modifications directed by an organization's management (e.g., changes to the funding profile, decision to outsource part of the process, change in mission, new requirements, change in services) - modifications mandated by laws and regulations

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Misc.
- Designated personnel in any activity send CSIRT process changes to designated personnel in PC: Prepare/Sustain/Improve. - Designated personnel in PC: Prepare/Sustain/Improve provide confirmation that CSIRT process changes were received. - Designated personnel in any activity and PC: Prepare/Sustain/Improve verify the integrity of transmitted CSIRT process changes.	Designated personnel follow operational procedures for sending and receiving CSIRT process changes.	Any personnel involved in the sending activity.	- Designated personnel in PC: Prepare/Sustain/Improve who receive CSIRT process changes can include - organizational CSIRT development project team - executive managers (i.e., any C-level manager) - business function managers - IT operations - representatives from administrative operations (e.g., legal, HR, PR, compliance) - representatives from constituency - representatives from law enforcement - representatives from critical infrastructures - third-party MSSP personnel - CSIRT development SMEs - CSIRT manager - CSIRT staff	Verbal Electronic Physical	- Phone - Face-to-face communication - Enail - Fax - Electronic reporting system - Hard copy passed from one person to another	---

Handoff from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To successfully send infrastructure protection improvements from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure – within defined time constraints – while handling information within the appropriate security context – while tracking the handoff in an appropriate manner	- When the decision to improve the infrastructure is made - When infrastructure protection improvements are ready to be passed to PI: Protect Infrastructure	- When infrastructure protection improvements have been sent to PI: Protect Infrastructure - When infrastructure protection improvements have been received <i>(continued)</i>	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they <i>are required to perform</i>

Processes Involved	
Sending Process	Receiving Process
PC9: Conduct Postmortem	PI2: Determine Infrastructure Protection Requirements

Objects Being Transported/Transmitted	
Object	Description
Infrastructure protection improvements	Infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure. During PC: Prepare/Sustain/Improve, these proposed improvements are identified during postmortem reviews and then forwarded to PI: Protect Infrastructure.

Person-to-Person Handoff

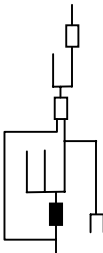
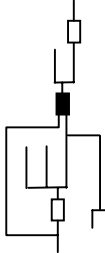
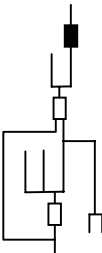
Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Misc.
- Designated personnel in PC: Prepare/Sustain/Improve send infrastructure protection improvements to designated personnel in PI: Protect Infrastructure. - Designated personnel in PC: Prepare/Sustain/Improve provide confirmation that infrastructure protection improvements were received. - Designated personnel in PC: Prepare/Sustain/Improve and PI: Protect Infrastructure verify the integrity of transmitted infrastructure protection improvements.	- Designated personnel follow operational procedures for reporting infrastructure protection improvements from PC: Prepare/Sustain/Improve to PI: Protect Infrastructure. - Designated personnel follow organizational or CSIRT change management processes or guidelines. - Designated personnel follow organizational project management and implementation guidelines or procedures.	- Designated personnel in PC: Prepare/Sustain/Improve who send infrastructure protection improvement requirements can include – CSIRT staff – CSIRT manager – IT staff – IT manager – third parties (e.g., service providers) – business function managers – CSIRT constituency – representatives from administrative operations (e.g., legal, HR, PR, compliance) – auditors, risk management staff, compliance staff	- Designated personnel in PI: Protect Infrastructure who receive infrastructure protection improvement requirements can include – IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) – third parties (e.g., MSSPs, ISPs, SMEs) – auditors, risk management staff, compliance staff – CSIRT staff	Verbal Electronic Physical	- Phone - Face-to-face communication - Email - Fax - Electronic reporting system - Hard copy passed from one person to another (e.g., change management forms and reports)	---

PI: Protect Infrastructure Workflow Description

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To adequately protect and secure critical data and the computing infrastructure of the CSIRT and its constituency - in response to current risk, threats, attacks - in response to proposed improvements - based on a predetermined schedule - while handling information within the appropriate security context	- When lessons learned from a postmortem review of a computer security incident require improvements to the computing infrastructure - When an organizational entity decides or is mandated to evaluate, manage, and improve the security of its computing infrastructure - When improvements to the security of the computing infrastructure have been identified through means other than an evaluation (i.e., through activities within or outside of the CSIRT process)	When the security of the computing infrastructure is improved or enhanced	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Designated personnel document results in accordance with organizational policies. - Designated personnel stay abreast of current methods, tools, and technologies for protecting the infrastructure.

Inputs		
Input	Description	Form
Current infrastructure	This is the existing configuration of the computing infrastructure and its susceptibility to cyber and physical attacks. <i>Note:</i> The current infrastructure comprises the people, processes, and technologies needed to support an organization's computing capability.	People, processes, and technologies
Infrastructure protection improvements	Infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure. These improvements come from many different sources, including - enhancements stemming from formal and informal postmortem reviews conducted as part of PC: Prepare/Sustain/Improve - changes resulting from observations about problems with the security of the computing infrastructure (from any activity within the CSIRT process or from activities outside of the CSIRT process) - improvements directed by mandates, best practices, standards, or an organization's management	Verbal, electronic, or physical

Outputs		
Output	Description	Form
Hardened infrastructure	This builds on the current infrastructure configuration by incorporating improvements identified through various means. The end result is a computing infrastructure that is less vulnerable to cyber and physical attacks. The hardened infrastructure meets or exceeds all infrastructure protection requirements.	People, processes, and technologies
Current infrastructure	This is the existing configuration of the computing infrastructure. Its susceptibility to cyber and physical attacks is unchanged. <i>Note:</i> The current infrastructure comprises the people, processes, and technologies needed to support an organization's computing capability.	People, processes, and technologies
Event reports	This includes reports of unusual or suspicious activity identified during infrastructure evaluations that are forwarded to D: Detect Events.	Verbal, electronic, or physical

Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology	Other/Misc.				
PI1: Evaluate Infrastructure 	- Designated personnel evaluate the computing infrastructure for vulnerability or risk and decide what to do (i.e., improve the current infrastructure, make no improvements to the current infrastructure, or send an event report to D: Detect Events when a potential incident is identified). <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Current infrastructure* </td><td> - Infrastructure protection improvements - Current infrastructure* - Event reports* </td></tr></table>	Inputs	Outputs	Current infrastructure*	- Infrastructure protection improvements - Current infrastructure* - Event reports*	- Designated personnel follow organizational procedures and methodologies for conducting vulnerability and risk assessments. - Designated personnel follow third-party best practice guidelines, procedures, standards, or regulations for protecting or securing a computing infrastructure. - Designated personnel follow organizational or CSIRT change management processes or guidelines.	- Designated personnel for assessing the computing infrastructures can include - IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) - auditors, risk management staff, compliance staff - third-party or independent evaluators - CSIRT staff	- Designated personnel can use the following technology when assessing the computing infrastructures: - vulnerability assessment or scanning tools (e.g., network scanners) - risk assessment tools (e.g., decision support tools) - tracking and compliance database/archive system - communication channels (email, videoconferencing, groupware, web)	---
Inputs	Outputs								
Current infrastructure*	- Infrastructure protection improvements - Current infrastructure* - Event reports*								
PI2: Determine Infrastructure Protection Requirements 	- Designated personnel review proposed improvements to the computing infrastructure and decide what to do with them (i.e., develop requirements to implement proposed improvements or take no further action). <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Current infrastructure* - Infrastructure protection improvements* </td><td> - Current infrastructure* - Infrastructure protection requirements </td></tr></table>	Inputs	Outputs	- Current infrastructure* - Infrastructure protection improvements*	- Current infrastructure* - Infrastructure protection requirements	- Designated personnel follow operational procedures for documenting infrastructure protection requirements. - Designated personnel follow third-party best practice guidelines, procedures, standards, or regulations for protecting or securing a computing infrastructure. - Designated personnel follow organizational or CSIRT change management processes or guidelines. - Designated personnel follow organizational criteria for prioritizing infrastructure requirements.	- Designated personnel for determining infrastructure protection requirements can include - IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) - third parties (e.g., MSSPs, ISPs, SMEs) - auditors, risk management staff, compliance staff - CSIRT staff	- Designated personnel can use the following technology when determining infrastructure protection requirements: - communication channels (email, videoconferencing, groupware, web)	---
Inputs	Outputs								
- Current infrastructure* - Infrastructure protection improvements*	- Current infrastructure* - Infrastructure protection requirements								
PI3: Harden and Secure Infrastructure 	- Designated personnel implement appropriate infrastructure protection requirements for improving the security of the computing infrastructure. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Infrastructure protection requirements </td><td> - Hardened infrastructure* </td></tr></table>	Inputs	Outputs	Infrastructure protection requirements	Hardened infrastructure*	- Designated personnel follow operational procedures for configuring and maintaining the computing infrastructure. - Designated personnel follow third-party best practice guidelines, procedures, standards, or regulations for protecting or securing a computing infrastructure. - Designated personnel follow organizational project management and implementation guidelines or procedures. - Designated personnel follow organizational or CSIRT change management processes or guidelines.	- Designated personnel for hardening and securing the computing infrastructure can include - IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) - third parties (e.g., MSSPs, ISPs, SMEs) - CSIRT staff	- Designated personnel can use the following technology when hardening and securing the computing infrastructure: - system and network administration tools - database/archive system - communication channels (email, videoconferencing, groupware, web)	---
Inputs	Outputs								
Infrastructure protection requirements	Hardened infrastructure*								

Note: An asterisk (*) after an input to or an output of a subprocess listed in this table indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Handoff from Any Activity Inside or Outside CSIRT Process to PI: Protect Infrastructure

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To successfully send infrastructure protection improvements from any activity to PI: Protect Infrastructure. – within defined time constraints – while handling information within the appropriate security context – while tracking the handoff in an appropriate manner	When infrastructure protection improvements are ready to be passed to PI: Protect Infrastructure	- When infrastructure protection improvements have been sent to PI: Protect Infrastructure - When infrastructure protection improvements have been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Processes Involved	
Sending Process	Receiving Process
Any Activity inside or outside the CSIRT process	PI2: Determine Infrastructure Protection Requirements

Objects Being Transported/Transmitted	
Object	Description
Infrastructure protection improvements	Infrastructure protection improvements are proposed means for enhancing the security of the computing infrastructure. These improvements come from many different sources, including - changes resulting from observations about problems with the security of the computing infrastructure (from any activity within the CSIRT process or from activities outside of the CSIRT process) - improvements directed by mandates, best practices, standards, or an organization's management

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Misc.
- Designated personnel in any activity send infrastructure protection improvements to designated personnel in PI: Protect Infrastructure. - Designated personnel in PI: Protect Infrastructure provide confirmation that infrastructure protection improvements were received. - Designated personnel in any activity and PI: Protect Infrastructure verify the integrity of transmitted infrastructure protection improvements.	Designated personnel follow operational procedures for reporting infrastructure protection improvements from any activity to PI: Protect Infrastructure.	Any personnel involved in the sending activity	- Designated personnel in PI: Protect Infrastructure who receive infrastructure protection improvement requirements can include - IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) - third parties (e.g., MSSPs, ISPs, SMEs) - auditors, risk management staff, compliance staff - CSIRT staff	Verbal Electronic Physical	- Phone - Face-to-face communication - Email - Fax - Electronic reporting system - Hard copy passed from one person to another	---

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To successfully send event reports from PI: Protect Infrastructure to D: Detect Events - within defined time constraints - while handling event reports within the appropriate security context - while tracking the handoff in an appropriate manner	- When an event has been detected during an evaluation and needs to be reported - When the event report is ready to be passed to D: Detect Events	- When event report has been sent to D: Detect Events - When event report has been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Objects Being Transported/Transmitted	
Object	Description
Event reports	This includes reports of unusual or suspicious activity to the CSIRT identified during Infrastructure evaluations performed as part of PI; Protect Infrastructure. Event reports received from PI; Protect Infrastructure can include the following security-related items: specific signs of intrusion, configuration errors, and artifacts.

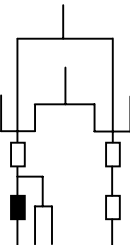
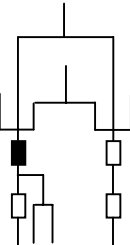
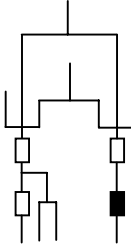
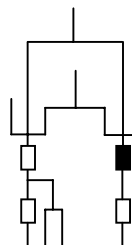
Handoff Requirements	Written Procedure	Sending Actor	Receiving Actor	Transmission/Transmission Medium	Other/Misc.	
Designated personnel in P1: Protect Infrastructure send event reports to designated personnel in D: Detect Events.	Designated personnel follow operational procedures for sending and receiving event reports.	- Designated personnel in P1: Protect Infrastructure who send event reports can include - IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) - auditors, risk management staff, compliance staff - third-party or independent evaluators	- Designated personnel in D: Detect Events who receive event reports can include - help desk staff - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - incident handlers - information security officer - system and network administrators - third-party answering service - coordination center	Verbal	- Phone - Face-to-face communication	---
Designated personnel in D: Detect Events provide confirmation that event reports were received.	Designated personnel follow any applicable special reporting procedures.			Electronic	- Email - Fax - Electronic reporting system - Database system	
Designated personnel in P1: Protect Infrastructure and D: Detect Events verify the integrity of transmitted event reports.				Physical	Hard copy passed from one person to another	

Detect Events Workflow Description

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To identify unusual activity that might compromise the mission of the CSIRT constituency and/or the CSIRT - within defined time constraints - while handling information within the appropriate security context	- When suspicious or unusual activity is noticed - When advisories, alerts, and other information reports or requests arrive	- When a decision about an event is made (i.e., forward to T: Triage Events, reassign to other processes, or close) - When outputs are ready to be passed to the next process	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Designated personnel document and track results in accordance with CSIRT and organizational policies. - Periodic quality assurance checks are performed on automated tools. - Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools.

Inputs				Outputs		
Input	Description	Form		Output	Description	Form
General indicators	This information includes the following security-related items: (1) suspicious or unusual activity noticed by internal and external sources and (2) data proactively gathered by the CSIRT, including log information, computer security news, and current events.	Verbal, electronic, or physical				
Event reports	This includes reports of unusual or suspicious activity to the CSIRT identified during infrastructure evaluations performed as part of PI: Protect Infrastructure. Event reports received from PI: Protect Infrastructure can include the following security-related items: specific signs of intrusion, configuration errors, and artifacts.	Verbal, electronic, or physical				
General requests/reports	This includes non-incident information (e.g., general information about CSIRT, general security questions, speaker requests).	Verbal, electronic, or physical				
				Event information	This includes all information that is passed to T: Triage Events for a given event. It can include the reported information and general indicators received by D: Detect Events, any preliminary analysis performed on the information, and the decision rationale for forwarding the information to T: Triage Events.	Verbal, electronic, or physical
				Reassigned events	This includes all information related to an event that has been reassigned outside of the incident handling process. It can include the reported information and general indicators received by D: Detect Events, as well as any preliminary analysis performed on the information. It can also include the rationale for reassigning the event.	Verbal, electronic, or physical
				Closed events	This includes all information related to an event that has been closed. It can include the reported information and general indicators received by D: Detect Events, as well as any preliminary analysis performed on the information. It can also include the rationale for closing the event.	Verbal, electronic, or physical

Note: An asterisk (*) after an input to or an output of a subprocess indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology	Other/Misc				
D1: Notice Events (Reactive) 	- Designated personnel notice suspicious or unusual activity and report it to the CSIRT. - Trusted external groups send advisories and alerts to the CSIRT. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - General indicators* </td><td> - Event reports </td></tr></table>	Inputs	Outputs	General indicators*	Event reports	- Designated personnel follow incident reporting guidelines for reporting information to the CSIRT. - Trusted external groups follow operational procedures and watch procedures for reporting information to the CSIRT.	- Designated personnel for noticing and reporting events can include - CSIRT - CSIRT constituency - victim or involved sites - general external groups (third-party reporters, MSSPs, media, law enforcement) - trusted external groups (other CSIRTs, vendors, etc.) - IT staff (e.g., NIC staff, NOC staff, SOC staff, system and network administrators) - coordination center	- People can use the following technology when noticing and reporting events: - security tools (e.g., IDS, encryption) - desktop workstations - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web)	---
Inputs	Outputs								
General indicators*	Event reports								
D2: Receive Information 	- Designated personnel review reports, verify them, and decide what to do with them (i.e., forward to T: Triage Events, reassign to other processes, or close). - Automated tools receive reports and forward them to T: Triage Events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Event reports from D1: Notice Events - Event reports from PI: Protect Infrastructure* - General requests/reports* </td><td> - Event information* - Reassigned events* - Closed events* </td></tr></table>	Inputs	Outputs	- Event reports from D1: Notice Events - Event reports from PI: Protect Infrastructure* - General requests/reports*	- Event information* - Reassigned events* - Closed events*	- Designated personnel follow report collection procedures for reviewing and verifying reports and deciding what to do about them. - Designated personnel follow appropriate procedures for reassigning and closing events. - Automated tools are designed to follow report collection procedures for receiving and forwarding reports.	- Designated personnel for receiving reported information can include - help desk staff - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - incident handlers - information security officer - system and network administrators - third-party answering service - coordination center	- Designated personnel can use the following technology when receiving, reviewing, and deciding what to do about reported information: - security tools (whois, port number lists, encryption, etc.) - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - database system - decision support tools - Automated receiving and forwarding tools can be used to automatically receive events and forward them to T: Triage Events.	---
Inputs	Outputs								
- Event reports from D1: Notice Events - Event reports from PI: Protect Infrastructure* - General requests/reports*	- Event information* - Reassigned events* - Closed events*								
D3: Monitor Indicators (Proactive) 	- Designated personnel proactively monitor a variety of sources for indications of potential events (e.g., log information, computer security news, current events). - Automated tools monitor systems and networks for general indicators. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - General indicators* </td><td> - Event indicators </td></tr></table>	Inputs	Outputs	General indicators*	Event indicators	- Designated personnel follow operational procedures for monitoring and reviewing general indicators. - Automated tools are designed to follow operational procedures for monitoring systems and networks for general indicators.	- Designated personnel for proactive monitoring can include - IT staff (e.g., NIC staff, NOC staff, system and network administrators) - selected members of the CSIRT staff - third parties (e.g., regulatory bodies, MSSPs, collaborators, ISPs, trusted SMEs) - coordination center	- Designated personnel can use the following technology when monitoring for general indicators: - security tools (e.g., IDS, vendor applications) - data manipulation tools - Internet search engines - communication channels, encrypted when appropriate (e.g., email, mailing lists, newsgroups, web) - database/archive system - Automated detection agents or sensors can be used to automatically monitor systems and networks for general indicators.	---
Inputs	Outputs								
General indicators*	Event indicators								
D4: Analyze indicators 	- Designated personnel review and analyze event indicators and decide what to do with the information (i.e., forward to T: Triage Events, reassign to other processes, or close). - Automated tools analyze event indicators and determine when to forward them to T: Triage Events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Event indicators </td><td> - Event information* - Reassigned events* - Closed events* </td></tr></table>	Inputs	Outputs	Event indicators	- Event information* - Reassigned events* - Closed events*	- Designated personnel follow operational procedures for reviewing and analyzing event indicators and deciding what to do with them. - Designated personnel follow appropriate procedures for reassigning and closing events. - Automated tools are designed to follow operational procedures for analyzing event indicators and determining when to forward them to T: Triage Events.	- Designated personnel for analyzing indicators can include - IT staff (e.g., NIC staff, NOC staff, system and network administrators) - selected members of the CSIRT staff - third parties (e.g., regulatory bodies, MSSPs, collaborators, ISPs, trusted SMEs) - coordination center	- Designated personnel can use the following technology when reviewing, analyzing, and deciding what to do about event indicators: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - database system - decision support tools - knowledge bases (e.g., CERT/CC, CVE) - Automated detection agents or sensors can be used to automatically analyze event indicators and determine when to forward them to T: Triage Events.	---
Inputs	Outputs								
Event indicators	- Event information* - Reassigned events* - Closed events*								

Handoff from Any Activity Inside or Outside of the Organization to D: Detect Events

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To successfully send general requests or reports from any activity to D: Detect Events – within defined time constraints – while handling information within the appropriate security context – while tracking the handoff in an appropriate manner	When general requests or reports are ready to be passed to D: Detect Events	- When general requests or reports have been sent to D: Detect Events - When general requests or reports have been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Processes Involved			Objects Being Transported/Transmitted	
Sending Process	Receiving Process		Object	Description
			General requests/reports	This includes non-incident information (e.g., general information about CSIRT, general security questions, speaker requests).

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Misc.
- Designated personnel in any activity send general requests or reports to designated personnel in D: Detect Events. - Designated personnel in D: Detect Events provide confirmation that general requests or reports were received. - Designated personnel in any activity and D: Detect Events verify the integrity of transmitted general requests or reports.	Designated personnel follow operational procedures for sending and receiving general requests or reports.	Any personnel involved in the sending activity	- Designated personnel in D: Detect Events who receive event reports can include the following people: – help desk staff – CSIRT triage staff – CSIRT hotline staff – CSIRT manager – incident handlers – information security officer – system and network administrators – third-party answering service – coordination center	Verbal Electronic Physical	- Phone - Face-to-face communication - Email - Fax - Electronic reporting system - Hard copy passed from one person to another	---

Handoff from D: Detect Events to T: Triage Events

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To successfully send event information from D: Detect Events to T: Triage Events - within defined time constraints - while handling information within the appropriate security context - while tracking information in an appropriate manner	- When event information meets the criteria for being passed to T: Triage Events - When event information is ready to be passed to T: Triage Events	- When event information has been sent to T: Triage Events - When event information has been received and its contents verified (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Periodic quality assurance checks are performed on automated tools. - Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools.

Processes Involved	
Sending Process	Receiving Process
D2: Receive Information D4: Analyze Indicators	T1: Categorize and Correlate Events

Object	Objects Being Transported/Transmitted
Event information	Description This includes all information that is passed from D: Detect Events to T: Triage Events for a given event. It can include the reported information and general indicators received by D: Detect Events, any preliminary analysis performed on the information, and the decision rationale for forwarding the information to T: Triage Events.

Person-to-Person Handoff

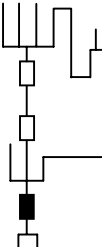
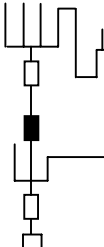
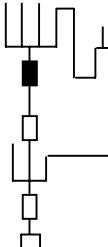
Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/ Transportation Modes	Transmission/Transportation Mechanisms	Other/Misc.
Designated personnel in D: Detect Events send event information to designated personnel in T: Triage Events.	Designated personnel follow operational procedures for sending and receiving event information.	- Personnel in D: Detect Events who send event information can include the following: - help desk staff - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - incident handlers - information security officer - system and network administrators - IT staff (e.g., NIC staff, NOC staff, system and network administrators) - third parties (e.g., answering service, regulatory bodies, MSSPs, collaborators, ISPs, trusted SMEs) - coordination center	- Personnel in T: Triage Events who receive event information can include the following: - CSIRT Triage staff - CSIRT hotline staff - CSIRT manager - help desk staff - incident handling staff - IT staff - information security officer - coordination center	Verbal	- Phone - Face-to-face communication	---
Designated personnel in T: Triage Events provide confirmation that event information was received.				Electronic	- Email - Fax - Electronic reporting system	
Designated personnel in D: Detect Events and T: Triage Events verify the integrity of event information.				Physical	- Hard copy directly handed from sender to receiver - Hard copy directly sent via mail system/courier (e.g., Express Mail)	

T: Triage Events Workflow Description

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To sort event information and assign it to appropriate personnel – within defined time constraints – while handling information within the appropriate security context – while documenting information in an appropriate manner	When event information arrives	When events have been categorized, prioritized, assigned, closed, or reassigned	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- When an event is part of an incident that has previously been closed, designated personnel can reopen the closed incident if appropriate. - Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel document and track results in accordance with CSIRT and organizational policies. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Periodic quality assurance checks are performed on automated tools. - Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools.

Inputs		
Input	Description	Form
Event information	This includes all information that is passed to T: Triage Events from D: Detect Events. It can include reported information and general indicators, general requests and reports, any preliminary analysis performed on the information, and the decision rationale for forwarding the information to T: Triage Events.	Verbal, electronic, or physical

Outputs		
Decision	Output	Description Form
Event is assigned to a technical or management response	Assigned events	This includes all information that is passed to R: Respond for a given event. It can include event information received by T: Triage Events, the event's category and priority, and assigned responsibility for incident handling. Some events may be identified as incidents during T: Triage Events, while other events are passed to R: Respond for further evaluation. Verbal, electronic, or physical
Event is reassigned outside of the incident management process	Reassigned events	This includes all information related to an event that has been reassigned outside of the incident handling process. It can include event information received by T: Triage Events, as well as the decision rationale for reassigning the information. Verbal, electronic, or physical
Event is closed	Closed events	This includes all information related to an event that has been closed. It can include event information received by T: Triage Events, as well as the rationale for closing the event. Verbal, electronic, or physical

Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology	Other/Misc.				
T1: Categorize Events 	- Designated personnel review event information against predefined categorization criteria and decide what to do with it (i.e., forward to T2: Prioritize Events, reassign to other groups, or close). - Designated personnel review event information to determine whether it is a new or ongoing event and whether it correlates with other reported information. - If an event's category cannot be determined using predefined criteria, designated personnel review information related to the event and determine its category, consulting with others as needed. - Automated tools use predefined criteria to categorize events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Event Information* </td><td> - Categorized Events - Reassigned Events* - Closed Events* </td></tr></table>	Inputs	Outputs	Event Information*	- Categorized Events - Reassigned Events* - Closed Events*	- Designated personnel follow triage procedures for categorizing and correlating events. - Designated personnel use predefined categorization criteria when categorizing events. - Designated personnel follow appropriate procedures for reassigning and closing events. - Automated tools are designed to follow triage procedures for categorizing events. - Automated tools use predefined criteria when categorizing events.	- Designated personnel for categorizing and correlating events can include - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - help desk staff - incident handling staff - IT staff - information security officer - coordination center	- Designated personnel can use the following technology when categorizing and correlating events: - incident handling database/tracking system - trouble ticket system - decision support tools (e.g., checklists, automated systems, other databases) - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - Automated triage tools can be used to automatically categorize events.	---
Inputs	Outputs								
Event Information*	- Categorized Events - Reassigned Events* - Closed Events*								
T2: Prioritize Events 	- Designated personnel review categorized events against predefined prioritization criteria and determine the priority of each event. - If an event's priority cannot be determined using predefined criteria, designated personnel review information related to the event and determine its priority, consulting with others as needed. - Automated tools use predefined criteria to prioritize events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Categorized Events </td><td> - Prioritized Events </td></tr></table>	Inputs	Outputs	Categorized Events	Prioritized Events	- Designated personnel for prioritizing events can include - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - help desk staff - incident handling staff - IT staff - information security officer - coordination center	- Designated personnel can use the following technology when prioritizing events: - incident handling database/tracking system - trouble ticket system - decision support tools (e.g., checklists, automated systems, other databases) - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - Automated triage tools can be used to automatically prioritize events.	---	
Inputs	Outputs								
Categorized Events	Prioritized Events								
T3: Assign Events 	- Designated personnel review prioritized events against assignment guidelines and decide what to do with them (i.e., forward to R: Respond, reassign to other groups, or close). - If assignment guidelines do not indicate where to assign an event, designated personnel review information related to the event and assign it to the appropriate parties, consulting with others as needed. - Automated tools use predefined criteria to assign events. <table><tr><th>Inputs</th><th>Outputs</th></tr><tr><td> - Prioritized Events </td><td> - Assigned Events* - Reassigned Events* - Closed Events* </td></tr></table>	Inputs	Outputs	Prioritized Events	- Assigned Events* - Reassigned Events* - Closed Events*	- Designated personnel for assigning events can include - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - help desk staff - incident handling staff - IT staff - information security officer - coordination center	- Designated personnel can use the following technology when assigning events: - incident handling database/tracking system - trouble ticket system - decision support tools (e.g., checklists, automated systems, other databases) - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - Automated triage tools can be used to automatically assign and close events.	---	
Inputs	Outputs								
Prioritized Events	- Assigned Events* - Reassigned Events* - Closed Events*								

Note: An asterisk (*) after an input to or an output of a subprocess indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Handoff from T: Triage Events to R: Respond

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To send assigned events successfully from T: Triage Events to R: Respond - within defined time constraints - while handling information within the appropriate security context - while tracking information in an appropriate manner	- When assigned events meet the criteria for being passed to R: Respond - When assigned events are ready to be passed to R: Respond	- When assigned events have been sent to T: Triage Events - When assigned events have been received and their content verified (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Periodic quality assurance checks are performed on automated tools. - Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools.

Processes Involved	
Sending Process	Receiving Process
T3: Assign Events	R1: Respond to Technical Issues R2: Respond to Management Issues

Objects Being Transported/Transmitted	
Object	Description
Assigned events	This includes all information that is passed to R: Respond for a given event. It can include event information received by T: Triage Events, the event's category and priority, and assigned responsibility for incident handling. Some events may be identified as incidents during T: Triage Events, while other events are passed to R: Respond for further evaluation.

Person-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Misc.
- Designated personnel in T: Triage Events send assigned events to designated personnel in R: Respond. - Designated personnel in R: Respond provide confirmation that assigned events were received. - Designated personnel in T: Triage Events and R: Respond verify the integrity of event information.	Designated personnel follow operational procedures for sending and receiving assigned events.	- Designated personnel in T: Triage Events who send assigned events can include - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - help desk staff - incident handling staff - IT staff - information security officer - coordination center	- Designated personnel in R: Respond who receive assigned events can include - CSIRT staff - CSIRT manager - IT staff (system and network administrators) - security staff (physical and cyber) - information security officer - upper management of the CSIRT constituency, business and functional units, IT management, etc. - CSIRT manager - HR staff - PR staff - coordination center	Verbal	- Phone - Face-to-face communication	• ---
			Electronic	- Email - Fax - Incident tracking system - Electronic reporting system		
			Physical	Hard copy directly handed from sender to receiver		

Technology-to-Person Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/ Transportation Modes	Transmission/ Transportation Mechanisms	Other/Misc.
- Automated tools from T: Triage Events send assigned events to designated personnel in R: Respond. - Designated personnel in R: Respond review assigned events for completeness and reasonableness.	- Automated tools are designed to follow operational procedures for sending and receiving assigned events. - Designated personnel follow operational procedures for sending and receiving assigned events.	Automated tools from T: Triage Events send assigned events.	- Designated personnel in R: Respond who receive assigned events can include - CSIRT staff - IT staff (system and network administrators) - security staff (physical and cyber) - information security officer - coordination center	Electronic	- Email - Incident tracking system - Electronic reporting system (automated incident reporting system)	---

Technology-to-Technology Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/ Transportation Modes	Transmission/ Transportation Mechanisms	Other/Misc.
- Automated tools from T: Triage Events send assigned events to automated tools from R: Respond. - Automated tools send assigned events via verifiable means (e.g., TCP/IP).	Automated tools are designed to follow operational procedures for sending and receiving assigned events.	Automated tools from T: Triage Events send assigned events.	Automated tools from R: Respond receive assigned events.	Electronic	Tool-to-tool interface	---

People-to-Technology Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/ Transportation Modes	Transmission/ Transportation Mechanisms	Other/Misc.
- Designated personnel in T: Triage Events send assigned events to automated tools from R: Respond. - Automated tools from R: Respond provide confirmation that assigned events were received.	- Designated personnel follow operational procedures for sending and receiving assigned events. - Automated tools are designed to follow operational procedures for sending and receiving assigned events.	- Designated personnel in T: Triage Events who send assigned events can include - CSIRT triage staff - CSIRT hotline staff - CSIRT manager - Help desk staff - Incident handling staff - IT staff - Information security officer - Coordination center	Automated tools from R: Respond receive event information.	Electronic	- Email - Electronic reporting interface	---

Respond Process Workflow Description

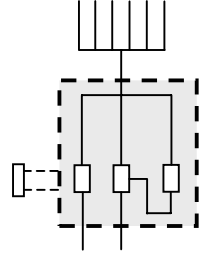
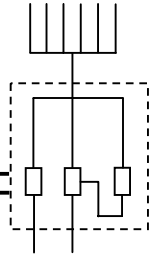
Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To resolve events and incidents – within defined time constraints – while handling information appropriately (e.g., within security, legal, and investigative contexts) – according to established policy, procedures, and quality requirements	When assigned events arrive	When technical, management, and legal responses are complete (e.g., no further response actions remain, the event or incident is closed, or the event or incident is reassigned outside of the incident handling process) Note: The technical, management, and legal responses might not close at the same time.	- CSIRT/IT policies - Organizational security policies (including HR and PR) - Security-related regulations, laws, guidelines, standards, and metrics - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform. - Designated personnel document and track results in accordance with CSIRT and organizational policies and procedures. - When an event is part of an incident that has previously been closed, designated personnel can reopen the closed incident if appropriate.

Inputs		
Input	Description	Form
Assigned events	This includes all information that is passed to R: Respond for a given event. It can include event information received by T: Triage Events, the event's category and priority, and assigned responsibility for incident handling. Some events may be identified as incidents during T: Triage Events, while other events are passed to R: Respond for further evaluation.	Verbal, electronic, or physical

Outputs			
Decision	Output	Description	Form
A postmortem review of the incident is required Internal and external stakeholders need to be notified Response is reassigned outside of the incident management process	Response information	This includes all relevant response-related data tailored for a specific audience (e.g., for a postmortem, for stakeholders, for other organizational personnel).	Verbal, electronic, or physical
	Response actions and decisions	This includes the following data about the response: - technical, management, or legal actions taken - technical, management, or legal decisions made	Verbal, electronic, or physical
A postmortem review of the incident is required	Proposed CSIRT process changes	This includes projected modifications to an existing CSIRT process. When the decision to conduct a postmortem is made, proposed CSIRT process changes are forwarded from R: Respond to PC: Prepare/Sustain/Improve.	Verbal, electronic, or physical
Event is reassigned outside of the incident management process	Reassigned events	This includes all information related to an event that is reassigned outside of the incident management process. It can include information received by R: Respond, any preliminary analysis performed on the information, and the rationale for reassigning the event. When applicable, it can also include the response strategy, as well as any actions and decisions made during the response.	Verbal, electronic, or physical
The response is complete	Response documentation	This includes all information related to the response. It is recorded once the response is complete.	Electronic or physical
	Formal notification of closure	This is an official notice to everyone who participated in the response that it is complete.	Verbal, electronic, or physical

Note: An asterisk (*) after an input to or an output of a subprocess indicates that it is also an input to or an output of the overall process. When an input to or an output of a subprocess is not followed by an asterisk, it indicates that the input or output is internal to the process.

Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology	Other/Miscellaneous
R1: Respond to Technical Issues	- Designated personnel analyze each event and plan, coordinate, and execute the appropriate technical response across involved sites and other relevant parties. - Designated personnel decide that the technical response is complete, all appropriate personnel are notified, and the incident is closed. - Automated tools execute preplanned technical responses when appropriate. Inputs - Assigned events* Outputs - Technical response information* - Technical response actions and decisions* - Technical response documentation* - Reassigned events*	- Designated personnel follow incident handling procedures when analyzing, planning, coordinating, and responding to events. - Designated personnel use predefined guidelines when responding to specific types of events. - Designated personnel follow appropriate procedures for closing incidents. - Automated response tools are designed to execute preplanned technical responses for specific types of events or incidents.	- Designated personnel for responding to technical issues can include - CSIRT staff - IT staff (system and network administrators) - security staff (physical and cyber) - SWES/trusted experts - information security officer - vendors - other CSIRTs - ISPs/network service providers - CSIRT constituency - victim or involved sites - coordination center	- Designated personnel can use the following technology when responding to technical issues: - security tools (e.g., log analysis tools, event monitoring tools, antivirus tools, file integrity checkers, vulnerability scanning tools, DNS query tools, whois, port number lists forensics, and other investigative tools) - infrastructure components (firewalls, intrusion detection systems, routers, filters) - knowledge bases (CERT/CC, CVE) - system and network administration tools (tools for configuration management, patch management, and user management) - incident handling database/tracking system - communication channels, encrypted when appropriate (email, mailing lists, newsgroups, web, XML RSS channels, automated call distribution system) - Automated response tools can be used to automatically execute a preplanned technical response.	- Periodic quality assurance checks are performed on automated tools. - Designated personnel use appropriate procedures and security measures when configuring and maintaining automated tools. - Designated personnel can recategorize and reprioritize incidents when appropriate.
R2: Respond to Management Issues	- Designated personnel analyze each event and plan, coordinate, and execute the appropriate management response. - Designated personnel decide that the management response is complete, all appropriate personnel are notified, and the incident is closed. - Designated personnel trigger a legal response when appropriate. Inputs - Assigned events* Outputs - Management response information* - Management response actions and decisions* - Management response documentation* - Reassigned events*	- Designated personnel follow organizational procedures (e.g., project management, IT governance, policy management) for coordinating and responding to events. - Designated personnel follow appropriate procedures for closing incidents. - Designated personnel follow human resource procedures when dealing with staffing issues. - Designated personnel follow PR procedures when dealing with media issues. - Designated personnel follow risk and audit procedures when dealing with liability and compliance issues. - Designated personnel follow quality assurance procedures when dealing with quality issues.	- Designated personnel for responding to management issues can include - upper management of the CSIRT constituency, business and functional units, IT management, etc. - CSIRT manager - HR staff - PR staff - auditors, risk management staff, compliance staff - SWES/trusted experts - victim or involved sites - coordination center	- Designated personnel can use the following technology when responding to management issues: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - decision support tools	- Designated personnel use executive and technical summaries as aids in decision making. - Designated personnel can recategorize and reprioritize incidents when appropriate.
R3: Respond to Legal Issues	- Designated personnel analyze each event and plan, coordinate, and execute the appropriate legal response regarding legal advice, investigation, and prosecution. - Designated personnel decide that the legal response is complete, all appropriate personnel are notified, and the incident is closed. Inputs - Assigned events* Outputs - Legal response information* - Legal response actions and decisions* - Legal response documentation* - Reassigned events*	- Designated personnel follow appropriate guidelines and procedures, regulations, and laws when - providing legal advice - conducting investigations - collecting evidence - prosecuting perpetrators - Designated personnel follow appropriate procedures for closing incidents.	- Designated personnel for responding to legal issues can include - legal counsel for constituency and CSIRT - inspectors general - attorneys general - law enforcement (state, local, federal, international) - criminal investigators - forensics specialists - victim or involved sites	- Designated personnel can use the following technology when responding to legal issues: - communication channels, encrypted when appropriate (email, videoconferencing, groupware, web) - forensics and other investigative tools - knowledge bases (case law, judicial precedents, laws, regulations, integrated justice systems) - any technologies that support the legal process	---

Subprocess	Subprocess Requirements	Written Procedures	Key People	Technology	Other/Misc.
Coordinate Technical, Management, and Legal Responses 	- Designated personnel plan, coordinate, and execute their response by providing advice, developing and disseminating recommendations, sharing data, and giving directions and assigning actions. - Designated personnel decide that the coordinated response is complete, all appropriate personnel are notified, and the incident is closed. Shared Information - Technical, management, and legal response information* - Technical, management, and legal response actions and decisions* Output - Response information* - Response actions and decisions* - Response documentation* - Reassigned events*	- Designated personnel follow procedures required for technical, management, and legal responses. - Designated personnel follow appropriate procedures for coordinating technical, legal, and management responses. - Designated personnel follow information disclosure policies, guidelines, and procedures.	- Designated personnel for coordinating technical, management, and legal responses can include - Key people involved in the technical, management, and legal responses	- Designated personnel can use the following technology when coordinating technical, management, and legal responses: - communication channels, encrypted when appropriate (email, phone, fax, XML RSS, videoconferencing, groupware, web) - data sharing tools, formats, and standards (web, IODEF, XML, IDMEF, CAIF) - documentation and publication technologies	---
External Communication with Others 	Designated personnel communicate with external parties as part of the response. This communication can include queries for additional information about an incident, recommendations for addressing an incident, information required for coordinating the response with external parties, and required reporting to designated entities.	- Designated personnel follow procedures required for communicating with external parties. - Designated personnel follow appropriate procedures for working with external parties. - Designated personnel follow information disclosure policies, guidelines, and procedures.	- Designated personnel for communicating with external parties can include - key people involved in the technical, management, and legal responses - external people who might be involved in the response (e.g., media, other CSIRTs, vendors, SMEs, ISPs, NAPs, MSSPs, law enforcement, ISACs, other compliance organizations) - people from all involved sites	- Designated personnel can use the following technology when communicating with external parties: - communication channels, encrypted when appropriate (email, phone, fax, XML RSS, videoconferencing, groupware, web, special reporting systems) - data sharing tools, formats, and standards (web, IODEF, XML, IDMEF, CAIF) - documentation and publication technologies	---

Handoff from R: Respond to PC: Prepare/Sustain/ Improve

Mission/Objectives	Triggers	Completion Criteria	Policies and Rules	General Requirements
- To successfully send proposed CSIRT process changes, response information, and response actions and decisions from R: Respond to PC: Prepare, Sustain, and Improve CSIRT Process. – within defined time constraints – while handling information within the appropriate security context – while tracking the handoff in an appropriate manner	- When the decision to conduct a postmortem review of an incident is made - When proposed CSIRT process changes, response information, and response actions and decisions are ready to be passed to PC: Prepare, Sustain, and Improve CSIRT Process	- When proposed CSIRT process changes, response information, and response actions and decisions have been sent to PC: Prepare, Sustain, and Improve CSIRT Process - When proposed CSIRT process changes, response information, and response actions and decisions have been received (optional)	- CSIRT/IT policies - Security-related regulations, laws, guidelines, standards, and metrics - Organizational security policies - Organizational policies that affect CSIRT operations - Reporting requirements (critical infrastructure protection, government, financial, academic, military)	- Designated personnel use appropriate procedures, technology, and office space when secure handling of event information is required. - Designated personnel receive appropriate training in procedures and technologies related to the tasks they are required to perform.

Processes Involved		Objects Being Transported/Transmitted	
Sending Process	Receiving Process	Object	Description
R1: Respond to Technical Issues R2: to Legal Issues Respond to Management Issues R3: Respond	PC9: Conduct Postmortem Review	Proposed CSIRT process changes	This includes projected modifications to an already existing CSIRT process. When the decision to conduct a postmortem is made, proposed CSIRT process changes are forwarded from R: Respond to PC: Prepare, Sustain, and Improve CSIRT Process.
		Response information	This includes all relevant response-related data tailored for a specific audience (e.g., for a postmortem, for stakeholders, for other organizational personnel).
		Response actions and decisions	This includes the following data about the response: - technical, management, or legal actions taken - technical, management, or legal decisions made

Person to Person Handoff

Handoff Requirements	Written Procedures	Sending Actor	Receiving Actor	Transmission/Transportation Modes	Transmission/Transportation Mechanisms	Other/Misc.
- Designated personnel in R: Respond send incident information and response actions and decisions to designated personnel in PC: Prepare, Sustain, and Improve CSIRT Process. - Designated personnel in R: Respond provide confirmation that proposed CSIRT process changes, response information, and response actions and decisions were received. - Designated personnel in R: Respond and PC: Prepare, Sustain, and Improve CSIRT Process verify the integrity of transmitted incident information and response actions and decisions.	- Designated personnel follow operational procedures for sending and receiving CSIRT process improvements. - Designated personnel follow organizational or CSIRT change management processes or guidelines.	Designated personnel in R: Respond who send proposed CSIRT process changes, response information, and response actions and decisions can include the following people: – key people involved in the technical, management, and legal responses	Designated personnel in PC: Prepare, Sustain, and Improve CSIRT Process who receive proposed CSIRT process changes, response information, and response actions and decisions can include the following people: – CSIRT manager – IT staff – IT manager – business function managers – CSIRT constituency – representatives from administrative operations (e.g., legal, HR, PR, compliance) – auditors, risk management staff, compliance staff	Verbal Electronic Physical	- Phone - Face-to-face communication - Email - Fax - Electronic reporting system (e.g., special change management system) - Hard copy passed from one person to another (e.g., change management forms and reports)	---

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE October 2004		3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE Defining Incident Management Processes for CSIRTs: A Work in Progress			5. FUNDING NUMBERS F19628-00-C-0003	
6. AUTHOR(S) Chris Alberts; Audrey Dorofee; Georgia Killcrece; Robin Ruefle; & Mark Zajicek				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213			8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2004-TR-015	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116			10. SPONSORING/MONITORING AGENCY REPORT NUMBER ESC-TR-2004-015	
11. SUPPLEMENTARY NOTES				
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS			12B DISTRIBUTION CODE	
13. ABSTRACT (MAXIMUM 200 WORDS) This report presents a prototype best practice model for performing incident management processes and functions. It defines the model through five high-level incident management processes: Pre-prepare/Sustain/Improve, Protect Infrastructure, Detect Events, Triage Events, and Respond. Workflow diagrams and descriptions are provided for each of these processes. One advantage of the model is that it enables examination of incident management processes that cross organizational boundaries, both internally and externally. This can help computer security incident response teams (CSIRTs) improve their ability to collaborate with other business units and other organizations when responding to incidents. Future reports will extend this work and provide additional guidance to enable both newly forming and existing incident management capabilities to use the model to determine where gaps exist in their current processes and to develop plans for creating, improving, or restructuring their incident management capabilities and processes. Although the processes defined in this document were originally developed for internal CSIRTs, the models and information presented here are applicable to other types of CSIRTs and other types of incident management and security management capabilities.				
14. SUBJECT TERMS CSIRT, computer security incident response team incident handling, incident response, computer emergency response team, incident management incident response management, CERT/CC, CERT Coordination Center, CSIRT process			15. NUMBER OF PAGES 250	
16. PRICE CODE				
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	