Carnegie Mellon University
Software Engineering Institute

The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities

Justin Novak
David Mcintire
Angel Hueca
Brittany Manley
Sharon Mudd
Tracy Bills

February 2021

TECHNICAL REPORT

CMU/SEI-2021-TR-002

DOI: 10.1184/R/10.1184/R1/13624148

CERT Division

http://www.sei.cmu.edu

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

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

DM21-0108

Table of Contents

Executive Summary **v**

Abstract **vii**

Introduction **1**

1 Satisfy the Prerequisites **5**
1.1 Understand the Need for a Sector CSIRT 5
1.2 Understand the National Cybersecurity Ecosystem 7
1.2.1 Understand the Role of the National CSIRT 7
1.2.2 Establish Trust 8
1.3 Identify and Define the Sector 9
1.3.1 What Is the Sector? 9
1.3.2 Who Belongs to the Sector? 10
1.4 Host the Capability 11
1.4.1 Gain Knowledge of the Current Environment 11
1.4.2 If the Host Entity is Known or Predetermined 12
1.4.3 If the Host Entity is Unknown or Not Determined 12
1.4.4 Standalone Capabilities 13
1.4.5 Other Host Factors 13
1.5 Understand Legislation and Legal Authority or Guidance 14
1.6 Set Goals and Objectives 16

2 Gather Information **18**
2.1 Define the Constraints to Information Gathering 18
2.2 Understand the Process and Gather Information 19
2.2.1 Define the Scope of the Process 19
2.2.2 Establish Information Gathering Goals 20
2.2.3 Conduct Open Source Research 20
2.2.4 Conduct Interviews 21

3 Organize the Information and Evaluate the Gaps **24**
3.1 Choose an Analysis Approach and Techniques for Evaluating Gaps 24
3.2 Examine the As-Is and To-Be States 25
3.3 Analyze the Gaps 26
3.4 Consolidate Gap Information and Determine Priorities 27

4 Build a Roadmap **28**
4.1 Understand the Purpose of a Roadmap 28
4.2 Outline the Steps Needed to Create a Roadmap 29
4.2.1 Define and Understand the Goal of the Roadmap 29
4.2.2 Consider Terminology and Approach 29
4.2.3 Apply the Framework 29
4.2.4 Transition from As-Is to To-Be 30
4.3 Identify Roadmap Considerations and Create the Roadmap 30
4.3.1 Outline the Services Offered 30
4.3.2 Address the CSIRT's Role Within the National Cybersecurity Ecosystem 31
4.3.3 Develop Policies 31
4.3.4 Address Training Gaps 32

4.3.5 Define Milestones and Metrics 32
4.3.6 Create the Roadmap 32

5 Plan and Implement the Sector CSIRT 34
5.1 Gather Implementation Expertise 34
5.2 Plan for Implementation 35
5.3 Consider and Execute Specific Services 36
5.3.1 Information Security Event Management Service Area 36
5.3.2 Information Security Incident Management Service Area 37
5.3.3 Vulnerability Management Service Area 37
5.3.4 Situational Awareness Service Area 38
5.3.5 Knowledge Transfer Service Area 38
5.4 Communicate Implementation Progress 38
5.5 Integrate with the National Cybersecurity Ecosystem 39
5.5.1 Public/Private Considerations 40

6 Conduct Post-Implementation Activities 41
6.1 Review the Implementation Process 41
6.2 Use Metrics 43
6.3 Report the Results of Implementation 44
6.4 Plan for the Future 45
6.4.1 Remain Flexible for Future Growth 45

7 Conclusion 47

Appendix A: Resources for CSIRT Development 49

Appendix B: Information Gathering Topics and Design 53

Appendix C: Organizing Information and Documenting Gaps 57

Appendix D: *FIRST CSIRT Services Framework* Summary 63

Appendix E: CSIRT Services Implementation Considerations 66

References 71

List of Figures

Figure 1:	Framework Process	4
Figure 2:	Step 1—Satisfy the Prerequisites	5
Figure 3:	Step 2—Gather Information	18
Figure 4:	Step 3—Organize the Information and Evaluate the Gaps	24
Figure 5:	CSIRT Capacity Continuum	25
Figure 6:	Step 4—Build a Roadmap	28
Figure 7:	CSIRT Services Framework: Service Areas [FIRST 2019]	31
Figure 8:	Roadmap Example: Parallel Work Tracks for a Sector CSIRT Development Team	33
Figure 9:	Step 5—Plan and Implement the Sector CSIRT	34
Figure 10:	Step 6—Conduct Post-Implementation Activities	41
Figure 11:	CSIRT Services Framework Service Areas, Services, and Functions	65

List of Tables

Table 1:	Gap Analysis Template	27
Table 2:	Questions Revisited During Implementation	39
Table 3:	After-Action and Post-Mortem Reviews	42
Table 4:	Example Grouping Strategies for Organizing Gap Information	62

Executive Summary

The growth of Computer Security Incident Response Teams (CSIRTs) has largely followed the rapid expansion of the Internet into every facet of modern life and the digital economy. As the use of technology has grown and becomes more pervasive and specialized, CSIRTs have also grown and become more specialized. An emerging trend of this increased specialization in the realm of incident response and coordination is the adoption of *sector CSIRTs*—CSIRTs responsible for facilitating incident response and management for a particular sector of a country or economy (e.g., financial, energy, or government).[1]

These specialized entities enable public and private sector stakeholders to come together to address the risks, threats, and other challenges that are unique to the organizations and individuals in a particular sector.

In addition to establishing sector CSIRTs and effectively addressing risks and opportunities, public and private sector entities also continue to evolve cybersecurity and incident response approaches to incorporate stakeholders from critical infrastructure (CI) sectors into national cybersecurity ecosystems.[2]

Sector CSIRTs are at the forefront of these efforts. To that end, the U.S. Department of State, Office of the Coordinator for Cyber Issues commissioned the Software Engineering Institute (SEI) to develop the *Sector CSIRT Framework* to guide interested parties through the process of developing a sector CSIRT and integrating it into the national cybersecurity ecosystem.

This framework addresses the sector CSIRT's creation and integration process using the following six steps:

- **Step 1: Satisfy the Prerequisites.** To build a sector CSIRT from the ground up, certain prerequisites, such as a clear definition of the sector, must first be met. This step covers those prerequisites, including how to (1) ensure that all prerequisites are established, (2) understand the context of the new sector CSIRT, and (3) define the role the sector CSIRT will play within the national cybersecurity ecosystem.
- **Step 2: Gather Information.** Having the right information is essential for defining the *as-is* and *to-be* states of the process. This step outlines the type of information that should be gathered and how to effectively gather it.

---

[1] While sector CSIRTs often focus on critical infrastructure (CI) sectors defined by a government, development of sector CSIRTs that support sectors that are not necessarily deemed as critical can be considered; in such circumstances, this framework can also be used.

[2] A national cybersecurity ecosystem is the collective group of agencies, teams, and stakeholders working to protect the cybersecurity and information assets of a nation or economy.

- **Step 3: Organize the Information and Evaluate the Gaps.** Once the information is gathered, it must be organized, categorized, and analyzed to understand the differences (gaps) between the as-is and to-be states. This step highlights how to categorize information and identify and prioritize gaps.
- **Step 4: Build a Roadmap.** A roadmap is a step-by-step guide for bridging the identified gaps from the as-is state to the to-be state. This step describes how to build a roadmap and provides the tools needed to be successful.
- **Step 5: Plan and Implement the Sector CSIRT.** Planning and implementing a sector CSIRT transforms the research and development conducted into a functioning, operational incident response team. This step addresses implementation considerations—including tackling challenges that arise during this part of the process, and establishing and operationalizing the team's services, thereby integrating the CSIRT into its broader national cybersecurity ecosystem.
- **Step 6: Conduct Post-Implementation Activities.** Capturing lessons learned and reporting the final outcomes of the overall process are important closing activities after implementation is complete. This step is important for the future of the sector CSIRT since it enables future growth and cycles of additional capacity and capability development. This step covers how and why to capture lessons learned and how to prepare a sector CSIRT for success and growth.

This framework guides the development and implementation of a sector CSIRT. The desired outcome of this process is an organization—the sector CSIRT—that can fulfill its mission by providing clearly outlined services to a clearly defined constituency. By doing so, the *Sector CSIRT Framework* enriches global incident response and the cybersecurity community while enabling sector stakeholders to increase their own capabilities and capacity to coordinate and share information.

Abstract

The U.S. Department of State, Office of the Coordinator for Cyber Issues commissioned the Software Engineering Institute (SEI) to create the *Sector CSIRT Framework* for (1) developing a sector-based computer security incident response and coordination capability and (2) integrating this capability into a larger national cybersecurity ecosystem as applicable. The framework is a guide for helping interested parties develop the policies, processes, and procedures necessary to operationalize a *sector Computer Security Incident Response Team (CSIRT)*, a uniquely adapted, specialized incident response team. The framework outlines a process that moves the sector CSIRT from concept to reality. The framework helps the team developing the sector CSIRT understand the current conditions of incident response in the sector (i.e., the *as-is* state) and how to move it to a robust operating state (i.e., the *to-be* state). It bridges the gap between these two states using a well-defined roadmap and implementation process.

The *Sector CSIRT Framework* is intended for individuals and organizations—including CSIRT managers, national CSIRTs, and others—who are developing or implementing a sector CSIRT. Using this framework, these individuals or organizations can move a sector CSIRT from a concept to the reality of a fully operational team.

Introduction

As governments and critical infrastructure (CI) operators incorporate more connected technologies, cybersecurity risks continue to increase. In response to these risks, many governments around the world have begun to dedicate more resources toward cybersecurity as well as the protection of CI and critical sectors of their countries or economies.

Critical infrastructure, and the sectors and subsectors associated with it, are different for each country or economy. For example, there are 16 CI sectors in the United States (U.S.).[3] The Cybersecurity and Infrastructure Security Agency (CISA) defines U.S. critical sectors as follows:

> *Critical sectors of the economy are defined as infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.*

The *European Union (EU) Directive on Security of Network and Information Systems* (NIS Directive) defines, at a minimum, seven CI sectors.[4] The NIS Directive mandates the following:

> *Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to Annex II.*

Regardless of sector prioritization or which sectors are defined as critical by a country or economy, cybersecurity threats to CI can have devastating consequences. Therefore, to effectively address risks at a national level, national cybersecurity ecosystems must continue to evolve and incorporate CI stakeholders.

Fundamentally, a sector CSIRT is a body that facilitates incident response and management for a subset of a country or economy. In rare cases, a sector CSIRT can be transnational. Regardless of its scope and orientation, a sector CSIRT provides key advantages that other bodies—including national CSIRTs, national cybersecurity coordination centers, Security Operations Centers (SOCs), Product Security Incident Response Teams (PSIRTs), and private CSIRTs—cannot. Benefits of sector CSIRTs include bridging the gap between public and private sectors, and providing a mechanism or platform for cooperation, information sharing, and trust building.

---

[3] CISA lists the following 16 U.S. CI sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Material, and Waste; Transportation Systems; and Water and Wastewater Systems [CISA 2020].

[4] NIS Directive, Annex II lists the following CI sectors: Energy, Transport, Banking, Financial Market, Health, Drinking Water Supply and Distribution, and Digital Infrastructure. These sectors are further divided into subsector and type of entity [OJEU 2016].

A sector CSIRT performs vital tasks and functions related to computer security incidents that occur in the sector it supports. The list of functions can include the following:

- leading or facilitating incident response[5]
- communicating and coordinating with members of the sector and other stakeholders
- coordinating with the national CSIRT and within the national cybersecurity ecosystem
- disseminating information before and after incidents
- convening meetings and facilitating discussions among stakeholders
- providing or leading training
- ensuring trust and confidentiality among members

Purpose of This Document

This document helps cybersecurity stakeholders develop and implement sector-based incident response capabilities and effectively integrate them into a national cybersecurity ecosystem.

To successfully integrate sector CSIRTs into a national cybersecurity ecosystem, stakeholders must clearly understand and agree to what a sector CSIRT is, what its functions should be, and what its relationship to national bodies should be. Stakeholders must also clearly define and satisfy the prerequisites for developing the sector CSIRT's capabilities.

Scope

This document focuses on *sector-based* incident response capabilities and provides guidance on how to develop and implement a sector CSIRT. It covers the foundational steps of identifying and defining a sector through implementing a sector CSIRT and integrating it into a national cybersecurity ecosystem. The appendices contain related guidance and point to additional resources.

It is important to note that terminology may vary. This document uses the term *sector CSIRT* to broadly refer to any organization that is responsible for incident response and management for a subset of a country or economy. However, some entities use the terms *sectoral CSIRTs*, *sector-based Cybersecurity Centers*, *Sector CERTs (Computer Emergency Response Teams)*, or *Information Sharing and Analysis Centers (ISACs)*. This document uses the term *sector CSIRT* throughout. In addition, each country or economy may define its CI differently.[6] Regardless of the terminology used or the prioritization of CI within a country or economy, this document focuses on sector-based incident response capabilities.

---

[5] A sector CSIRT may provide in-depth incident response services, or it may serve only as a coordinator. These functions, and the possible roles of sector CSIRTs, are discussed throughout this document.

[6] The act of defining CI acknowledges that a particular sector or entity is critical to the well-being of a country or economy; however, the definition of CI, and which sectors are deemed critical, will vary.

Audience

This document was written primarily for sector CSIRT development teams[7] (whether or not a national CSIRT is operationalized). A development team is the organization leading the establishment and initial operation of the sector CSIRT. A development team can vary in composition and makeup (e.g., public vs. private sector) and can consist of the following members:

- cybersecurity governance stakeholders
- cybersecurity policy makers
- cybersecurity strategy developers
- cybersecurity stakeholders responsible for establishing or operating a sector CSIRT
- CI managers and operators
- cybersecurity centers or national CSIRTs

The framework includes key considerations for sector and national CSIRTs when developing sector-based capabilities. Thus, it can be a valuable resource to both audiences. When establishing a sector CSIRT, members of the development team are commonly involved in and participate in a national CSIRT. National CSIRTs often have established relationships with CI sector stakeholders and often have authority over and insights about incident response in those areas. Often, the national CSIRT's role is to serve as a bridge between the sector CSIRT and the broader national cybersecurity ecosystem. Even though this document was primarily written for development teams, it also provides some considerations that national CSIRTs can find valuable.

This document may be useful to others who interact with a sector CSIRT, including members of the CSIRT's constituency, law enforcement, and other cybersecurity and incident response teams directly or indirectly affected by the services of a sector CSIRT.[8]

Document Structure

Each section in the remainder of this document describes a step in the sector CSIRT development and implementation process.

- Step 1: Satisfy the Prerequisites
- Step 2: Gather Information
- Step 3: Organize the Information and Evaluate the Gaps
- Step 4: Build a Roadmap
- Step 5: Plan and Implement the Sector CSIRT
- Step 6: Conduct Post-Implementation Activities

The appendices provide related guidance and point to additional resources:

---

[7] Throughout this document, we refer to the *sector CSIRT development team* as simply the *development team*.

[8] See Section 1.3, "Identify and Define the Sector," for more information about a sector CSIRT's stakeholders, constituency, and community.

- Appendix A provides resources for developing CSIRTs.
- Appendix B supplements the activities associated with Step 2 (Gather Information).
- Appendix C supplements the activities associated with Step 3 (Organize the Information and Evaluate the Gaps).
- Appendix D summarizes the *FIRST CSIRT Services Framework*, which describes the services and functions of incident response teams in a high-level framework.
- Appendix E outlines specific implementation considerations associated with each of the areas outlined in the *FIRST CSIRT Services Framework.*

In this document, a roadmap graphic, depicted in Figure 1, illustrates the framework's six steps.

Figure 1: Framework Process

1 Satisfy the Prerequisites

A development team leads the establishment and initial operation of the sector CSIRT. Prior to initiating development of a sector CSIRT, the development team must weigh and carefully consider a number of *prerequisites* (i.e., questions and other issues) that help determine how the sector CSIRT will run and who will run it. While these prerequisites do not have to be *fully* addressed, they must at least be factored into the development team's approach.

These prerequisites are the foundation the sector CSIRT is built on. Without this strong foundation in place *before* establishing and operationalizing the sector CSIRT, the development team runs the risk of creating a flawed and/or ineffective organization.

Figure 2 summarizes the prerequisites associated with Step 1.

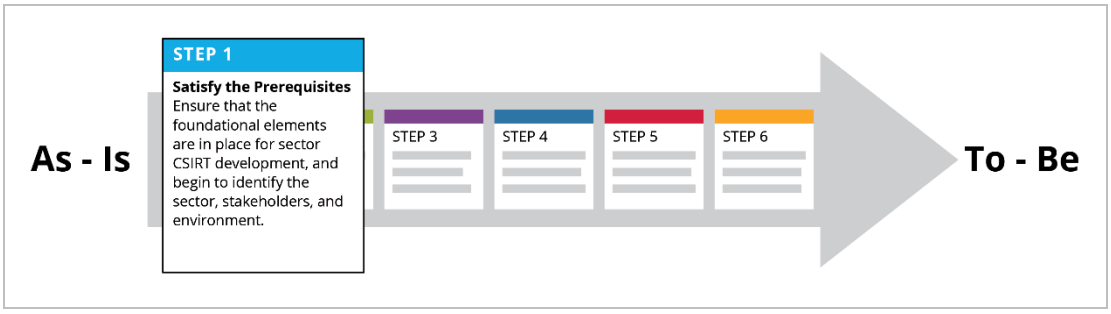

Figure 2: Step 1—Satisfy the Prerequisites

When examining these prerequisites, the development team can avoid potential negative outcomes by addressing two critical questions:

1. What is the current (as-is) state of cybersecurity and incident response in the given sector?
2. What is the desired (to-be) end state after the sector CSIRT is fully operational?

The prerequisites are organized into five categories, which are described in the following sections:

- 1.1: Understand the Need for a Sector CSIRT
- 1.2: Understand the National Cybersecurity Ecosystem
- 1.3: Identify and Define the Sector
- 1.4: Host the Capability
- 1.5: Understand Legislation and Legal Authority or Guidance
- 1.6: Set Goals and Objectives

1.1 Understand the Need for a Sector CSIRT

Fundamentally, a sector CSIRT is an organization that is responsible for incident response and management for a subset of a country or economy. In rare cases, a sector CSIRT can be transnational. Regardless of its scope and orientation, a sector CSIRT provides key advantages that other

bodies, including national CSIRTs, national cybersecurity coordination centers, Security Operations Centers (SOCs), Product Security Incident Response Teams (PSIRTs), and private CSIRTs cannot. While these advantages are wide ranging, the most important one is the sector CSIRT's ability to bridge the gap between the public and private sectors. Another key advantage is that sector CSIRTs provide a mechanism or platform for sharing information and building trust.

Cybersecurity leaders in a country or economy might wish to implement a sector CSIRT when they recognize the need for an organization that provides the above advantages or when there is a need for additional cybersecurity and incident response capacity in a sector. This additional capacity might take the form of added scalability or added expertise:

- **Scalability**. A national CSIRT's services can be difficult to scale to the owner/operator level. A sector CSIRT covers the majority of those needs for a sector so that a national CSIRT can focus on coordinating across sectors and others in the ecosystem.
- **Expertise**. Addressing CI sector incidents can require specialized knowledge and skills. A national CSIRT may not have the resources to address each sector's specific needs. However, a sector CSIRT can maintain subject matter expertise for its sector's needs.

A sector CSIRT performs vital tasks and functions related to computer security incidents that occur within the sector it supports. The list of functions can include the following:

- leading or facilitating incident response
- communicating and coordinating with members of the sector and other stakeholders
- coordinating with the national CSIRT and within the national cybersecurity ecosystem
- disseminating information before and after incidents
- convening meetings and facilitating discussions among stakeholders
- providing or leading training
- ensuring trust and confidentiality among members

Once the relevant authorities (including the development team) recognize the need for these functions, they must be integrated into a broader approach to cybersecurity and incident response. This broader approach is the responsibility of the sector CSIRT. The development team and other stakeholders must determine how the sector CSIRT can best (1) achieve a public-private partnership, (2) share information, and (3) build trust.

To establish and implement the sector CSIRT, the development team must answer the following questions:

- Who will define the sector CSIRT, and what will that definition be?
- What legal authorities, if any, will the sector CSIRT have?
- What is the scope of the responsibilities that the sector CSIRT will have?
- What will the composition of the sector CSIRT be, particularly as it relates to funding, staffing, and information acquisition and sharing?

1.2 Understand the National Cybersecurity Ecosystem

One important consideration is the degree to which the sector CSIRT will integrate with the *national cybersecurity ecosystem*. The national cybersecurity ecosystem is the collection of agencies, teams, and stakeholders that work together to protect a nation's cybersecurity and information assets. This ecosystem can include public sector entities (e.g., a national CSIRT, law enforcement, and regulatory bodies) and private sector entities (e.g., other sector CSIRTs, private cybersecurity companies, and academia).

The development team can include a national CSIRT or other parts of the national cybersecurity ecosystem. However, these stakeholders can assume additional roles, including as sources of information, collaboration, and direction during each part of the process. How involved the national cybersecurity ecosystem is depends on how involved the sector CSIRT is in that ecosystem. For example, a sector CSIRT that is created by law and housed in a government agency will likely be closely integrated with the national CSIRT and other national partners in that ecosystem. On the other hand, a sector CSIRT that is created and operated by private sector entities (e.g., an industry association or a group of CI operators) may have only loose ties to the rest of the national cybersecurity ecosystem.

1.2.1 Understand the Role of the National CSIRT

A national CSIRT is a team responsible for the cyber protection of a country or economy. There are many models of national CSIRTs; however, regardless of the model used, every national CSIRT has a broad responsibility and mission.

In contrast, a sector CSIRT is responsible for a smaller subset of the country or economy (i.e., the particular sector it serves). In many cases, this arrangement leads to an overlap of responsibilities between the sector CSIRT and the national CSIRT. Therefore, successfully integrating the sector CSIRT into the national cybersecurity ecosystem requires a strong working relationship between the two. However, in some cases—particularly in countries with nascent or developing cybersecurity capabilities—a national CSIRT may not exist.

During implementation, the development team must consider two possible scenarios:

- **A national CSIRT is established**. If a functioning, capable national CSIRT exists, it likely has an established relationship with the sector CSIRT. The nature and depth of this relationship may vary, ranging from informal information exchange to a hierarchy where the sector CSIRT is subordinate to the national CSIRT. Identifying this relationship and/or hierarchy is essential, followed by establishing rules, norms, and policies that will govern the relationship between the sector and national CSIRT, and clearly delineate the roles and responsibilities of each.
- **A national CSIRT is not yet established**. When a national CSIRT does not exist, the development team does not have access to the knowledge, experience, and resources that might otherwise guide its integration into a national cybersecurity ecosystem. The development team might need to find other entities in the national cybersecurity ecosystem it can collaborate with instead. While not ideal, developing such a relationship can be an opportunity to take a leadership role in the ecosystem and establish custom policies and plans based on its mission and its constituency's needs. On the other hand, this situation presents challenges;

other entities might seek support and expertise from the sector CSIRT because there is no national CSIRT. While the sector CSIRT's input can be valuable—such as for developing a national CSIRT or other sector CSIRTs—it is important for the sector CSIRT to operate within its scope, mission, and authority.

At this point, the development team should begin thinking about how to answer the following questions:

- What role will the national CSIRT (if there is one) play in the sector?
- What relationship will the sector CSIRT have with the national CSIRT (if one exists)?
- If there is no national CSIRT, how does this affect the sector CSIRT's role in the national cybersecurity ecosystem?
- How will the sector CSIRT address issues related to working with the public and private sectors nationwide?

If the national CSIRT is the core of the national cybersecurity ecosystem, the rest of that ecosystem comprises a diverse set of entities with a variety of roles. These entities can include public or private entities or, in some cases, public-private partnerships. Regardless, the sector CSIRT should integrate and work with existing stakeholders to build cooperation and communication channels. If the national CSIRT is already established, it can help significantly with this task.

1.2.2 Establish Trust

Another factor that affects the cybersecurity ecosystem is trust. The success of many aspects of a sector CSIRT's mission (e.g., information sharing) depends on trust. Therefore, the development team must carefully consider how the new sector CSIRT will establish and maintain trust with a variety of stakeholders from the prerequisite stage through post-implementation and beyond. These stakeholders include constituents, information sharing partners, and the national CSIRT.

Trust is generally established through one or more of the following:

- **Previously established relationships.** Working closely with other teams and organizations can develop trust among the participants.
- **Group membership.** Belonging to the same groups often indicates similar values and capabilities. Some groups (e.g., FIRST or Trusted Introducer) require membership assessments that support group trust.
- **Referral.** A referral from a known third party can help establish and verify trust.

It can be difficult to establish trust among cybersecurity organizations and individuals because of personal, political, or other longstanding reasons. Mismatched capabilities and a lack of shared values are additional reasons that trust might erode or make it difficult to build in an information sharing community. When developing a sector CSIRT and determining prerequisites, the development team must consider the importance of trust, acknowledge the current state of trust in the cybersecurity ecosystem, and address barriers to trust.

1.3 Identify and Define the Sector

For the development team to understand how to establish and operationalize a proposed sector CSIRT, it must be able to describe the sector the CSIRT will support. The development team must conduct preliminary research to determine the scope and applicability of the name chosen for the sector. It also must understand what the sector CSIRT is intended to accomplish (i.e., what type of organizations it will serve or assist). The following are the most important questions to answer during this part of the process, which are described in the following sections:

- 1.3.1 What Is the Sector?
- 1.3.2 Who Belongs to the Sector?

1.3.1 What Is the Sector?

The definition of each sector can vary from situation to situation or from country to country. For example, in one country, the financial sector may be limited to only banks. However, in other countries, the same sector may include other financial institutions, such as credit card companies or investment firms. No single definition of *sector* is appropriate for every setting; the development team should choose the definition that best fits its needs and situation. If the team does not identify the sector and its scope, it must understand who will and/or if it has already been decided.[9]

At this point, the development team can determine the overall purpose of the sector CSIRT (e.g., coordination versus information sharing versus provisioning operational incident response support), although the team can delay discussions about services until later in the process. (See Section 4.)

Before developing a sector CSIRT, the development team must broadly understand the options for the sector CSIRT's mission, goals, and purpose. Clarifying and codifying these items can happen later.

The following example illustrates how sectors can be viewed differently, depending on other factors (e.g., nature of the activity and location).

> *Many countries have a well-defined Energy Sector that has a sector CSIRT responsible for providing incident response and management services to the many public and private sector organizations active in that CI sector. However, not all countries define "Energy Sector" in the same way; some countries define it to include energy production and distribution firms—along with government ministries, power grid operators, and oil and gas concerns. Other countries have a more limited definition, or they separate these entities into several different sectors. In the U.S., for example, these entities are grouped into three areas of CI: Downstream Natural Gas, Electricity, and Oil and Gas. This approach makes sense for planners and stakeholders in the U.S., but it may not make sense in other locations.*

[9] For example, CI may already be defined in legislation for a given jurisdiction, or CI sectors may be outlined in a national strategy or similar document.

1.3.2 Who Belongs to the Sector?

Besides identifying the sector the CSIRT will support, the development team must also describe and define the entities included in the sector, ensuring that all relevant participants and stakeholders are accounted for. While the sector's *identity* (covered in Section 1.3.1, What Is the Sector?) describes what the sector is, this part of the process identifies the sector's members. These closely related concepts can be considered together, but they remain distinct ideas worthy of individual attention.

The development team must understand which organizations should be included in or consulted about the sector CSIRT. Examples include stakeholders, constituents, and community members.

- **Stakeholders.** A stakeholder is any organization or entity that has an interest in or concern about the proposed sector CSIRT. A stakeholder might not be directly served by the sector CSIRT, but it might receive significant secondary benefits. Examples of these types of stakeholders are (1) a large government agency that has a department among the sector CSIRT's constituents and (2) company employees or customers who will be constituents. Other stakeholders may see no direct or secondary benefits from the sector CSIRT, but they are included under this definition if they provide resources (e.g., funding, staffing, policy advice and guidance, or legal authority) to the sector CSIRT. Law enforcement agencies are frequently stakeholders since it is critical for law enforcement and incident responders to cooperate.
- **Constituents.** Typically, constituents are a subset of stakeholders. While stakeholders include all organizations and entities that affect or are affected by the sector CSIRT, constituents are organizations and entities that are served by the sector CSIRT (i.e., have cybersecurity and incident response services provided to them). A sector CSIRT's constituency can be defined in a number of ways. For example, a law might dictate which organizations qualify as constituents, or membership in an association or professional group may be required for an organization to be considered a constituent.[10]
- **Community Members.** The community is the broad set of tangential and related organizations that have a relationship with the sector CSIRT, but they might not fit the definitions of stakeholders or constituents. Examples include other incident response organizations, both local and regional/international. National CSIRTs, regional CSIRTs, and transnational organizations (e.g., the Forum of Incident Response and Security Teams [FIRST]) are frequently part of the sector CSIRT's community, although national CSIRTs in particular are often stakeholders. CSIRTs in neighboring countries, particularly those covering similar sectors, may also be part of the sector CSIRT's community.

Sector CSIRT stakeholders, constituents, or community members can take many different forms, including government agencies, private firms, or public interest groups. These groups generally fall into either the public sector or the private sector (described below). While some organizations (e.g., non-profit entities or public-private partnerships) may span these two definitions, it is important to understand the difference between these sectors and what each can offer the sector CSIRT in terms of strengths and weaknesses.

---

[10] For more information about constituency, see Section 2.1.2 of the *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003].

- **Public Organizations:** Examples of public organizations include government agencies, ministries, local and state/provincial agencies, and other authorities. These entities answer to the government hierarchy, which makes them subject to a number of different forces. These forces include increased oversight, political considerations, and elections; all of these can induce uncertainty and change. Conversely, public organizations have increased levels of official authority and steady funding streams. Identifying which public organizations are the sector CSIRT's stakeholders, constituents, or community members means leveraging the advantages while accounting for and mitigating the disadvantages of working with each.
- **Private Organizations**: Private organizations include private companies, associations or groups of private firms, private individuals, and non-profit organizations that do not have a public connection. Private organizations lack the formal authority of public sector agencies and may face additional legal oversight and scrutiny. However, in most jurisdictions, they have the freedom and flexibility to act and move more quickly in many situations since they are not subject to public bureaucracies. Private sector organizations often have greater and easier access to funding, although their leaders can be more willing to withdraw that funding based on the organization's needs, rather than those of the general public or the sector in general. The development team must understand how these aspects of private organizations might benefit or restrict the efficacy of the sector CSIRT.

1.4 Host the Capability

A host entity is the parent organization of a sector CSIRT. However, if a sector CSIRT is a standalone entity, it might not have a host entity or be part of a hierarchy. When a sector CSIRT is a standalone entity, the development team should consider additional factors since not having a host entity raises particular challenges. Regardless, whether determining the host entity of the sector CSIRT or considering additional factors, input is required from many stakeholders and several key issues must be considered.

Determining the sector CSIRT's host entity is not a prerequisite for planning and implementing a sector CSIRT. The development team should, however, consider the sector CSIRT's host entity and understand the issues and challenges that can result from determining the host entity or identifying that it doesn't exist.

Finally, considering where to host the sector CSIRT is also an opportunity to consider how it will fit into the national cybersecurity ecosystem and how host determination will affect this relationship. Understanding the expectations and needs of the ecosystem's other members (e.g., law enforcement, the national CSIRT) can provide valuable information about how to best position the sector CSIRT to be most effective.

1.4.1 Gain Knowledge of the Current Environment

When the development team considers where and how to host a sector CSIRT, it develops an understanding of which organizations, agencies, and other stakeholders already know the current environment as it relates to the (1) sector at large and (2) state of cybersecurity and incident response in the sector. These sources of sector knowledge are uniquely positioned to provide

guidance on many aspects of developing and operating a successful sector CSIRT. Even organizations that do not have technical- or security-related knowledge can provide valuable input from their deep historical knowledge of the operations, economics, politics, etc. of the sector. For example, a banker's association may have little insight into cybersecurity and incident response, but it can provide important information about the financial sector, such as its critical assets.

The development team should consult existing information sharing and/or coordinating bodies for their expertise and recommendations about where and how to host a sector CSIRT. These organizations can be formal or informal, and they might exist to share security and threat-related information among their members. For example, in the U.S., InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and the private sector for sharing information to help thwart threats to CI [InfraGard 2020]. Organizations like InfraGard may have knowledge of and relationships with many or all of the relevant stakeholders in one or more sectors.

1.4.2 If the Host Entity is Known or Predetermined

In many cases, the host entity for the sector CSIRT is known or determined in advance. Perhaps legislation or a government policy or directive dictates where a particular sector CSIRT should fall within an existing incident response hierarchy.[11] Or stakeholders might want to use the placement of a sector CSIRT to address another motive (e.g., maximizing funding, enhancing capabilities, or appearing impartial). Regardless, if the host entity is known, there are implications for the development team.

A predetermined host entity can eliminate other options that would be subject to stakeholder input. For example, the ability to gain stakeholder buy-in can be affected since some organizations are empowered by the decision, while others may feel excluded from the decision-making process. A predetermined host entity can also limit funding-source options and other key inputs if the process did not consider them before deciding (e.g., a host option having more reliable funding streams than another).

Conversely, a predetermined host can benefit the development team, for example, by providing the clarity of its organizational location. Another advantage is the likelihood that, along with determining the host entity, the legislation or policy directive might also address issues such as funding, staffing levels, organizational mission, constituency, or services. Addressing these issues ahead of time can be useful in other aspects of sector CSIRT implementation.

1.4.3 If the Host Entity is Unknown or Not Determined

If the development team begins work on establishing the sector CSIRT before a host entity is determined, it should strive to identify the host entity as soon as possible. Identifying the host entity reduces the need to revisit policies, procedures, and practices if the host determination is decided later in the process. For example, the development team may assume that the host entity will have certain legal authorities, but these authorities may be different if the sector CSIRT is hosted by an

[11] See Section 1.5 for more information about legislation.

entity that does not have those legal powers. Therefore, it is always better to determine the host entity as early as possible.

If the development team does not determine the host entity, it should understand that the risk of not doing so will increase as it moves through the implementation process.

1.4.4 Standalone Capabilities

A sector CSIRT may not have a host entity; it can operate as an independent agency or entity. While this approach has advantages (e.g., flexibility, agility, and independence), it is also challenging. Legal authority in an area, for example, is derived from official government positioning and affiliation in many jurisdictions. A standalone entity must find its own authority, get assistance from a relevant government agency to assert its authority, or find an alternative (e.g., voluntary sharing and cooperation agreements). The development team must consider how important each authority is and balance that need with the benefits of being a standalone sector CSIRT, particularly if the sector CSIRT is not a public sector (i.e., government) agency. The development team should also consider the sector CSIRT's role in the national cybersecurity ecosystem.

Similarly, the development team must understand that a standalone approach has important implications for funding and operating the sector CSIRT. As a standalone entity, the sector CSIRT must secure its own funding, which might require government or other public funds. Without a government host entity to advocate for funding, it is more difficult to get those funds. Private sector organizations might be more inclined to financially support a standalone sector CSIRT, or one that is a non-profit or public-private partnership, but private-sector organizations can attach demands or constraints on that funding.

A standalone sector CSIRT can face other challenges, including the following:

- establishing branding and public awareness
- gaining membership and community buy-in
- establishing relationships with other teams and partners

The development team does not need to address each of these challenges as a prerequisite; however, it should consider each challenge in advance to ensure it understands the implications.

1.4.5 Other Host Factors

There are other factors that the development team should consider when determining where and how to host a sector CSIRT. Other factors involved in establishing and operationalizing a sector CSIRT are described below:[12]

- **Mission**. There should be a clear understanding of the problem that the sector CSIRT will solve and who will directly benefit from solving the problem. The development team should also understand how the host entity will enable or restrict the sector CSIRT's ability to execute its mission.

[12] These factors are discussed in more detail in Section 5.

- **Constituency**. The development team must understand the proposed constituency of the sector CSIRT. The CSIRT's constituency is affected by its host entity since relationships, legal authorities, and the ability to connect with constituents are all affected by this choice.
- **Funding**. Different host entities might have different financial resources and funding streams available to the sector CSIRT. Government budgets can vary; one parent ministry may unlock greater potential funding than another. Private funding can also be contentious (e.g., if larger organizations are asked to pay larger shares as members of an association). Joint public and private funding or funding from constituency membership fees are other options to consider.
- **Staffing**. The staffing of a sector CSIRT is affected by funding and the choice of host entity. Host entities may lend staff directly, or their budgets (and reputations) might help or harm the sector CSIRT's ability to recruit and retain staff. The development team must carefully consider how to effectively staff the CSIRT at every decision point.
- **Facilities**. The location of the sector CSIRT needs to be carefully considered, including its physical assets as well as its network connections and location. The host entity might assist with a facility or funding for facilities. The host is not required to provide a place for the sector CSIRT to operate, but the development team must consider whether or not they will.

1.5 Understand Legislation and Legal Authority or Guidance

For a sector CSIRT to be successful, it must have legal authority to operate. This is true regardless of the exact nature and form of the sector CSIRT (e.g., private vs. public, large vs. small) and its mission. While the nature of legal authority varies from jurisdiction to jurisdiction, it is typically clear what actions the sector CSIRT can and cannot take, how it can interact with relevant government authorities, and the responsibilities it has (e.g., incident reporting requirements).

One key item often addressed in legislation is the sector the CSIRT supports. (See Section 1.3.1 for more details.) This is especially true when the sector CSIRT is a public or government-run body or when it supports *critical infrastructure* since its authority can be defined in a law or other legally binding policy. Regardless, the development team must understand the legal and legislative environment where the sector CSIRT is established and operates.[13]

Before the development team begins gathering information focused on sector cybersecurity, it should review current and prospective legislation to uncover the following factors:

- **Current authority level.** What, if any, authority does the cybersecurity framework for the nation or economy provide for managing cybersecurity in the sector that the CSIRT supports?

---

[13] The absence of enabling legislation should not stop or slow sector CSIRT creation and implementation. Many successful sector CSIRTs operate well without such legislation. However, particularly when the sector CSIRT is government operated or government affiliated, enabling legislation can provide significant clarity and guidance about assigning roles and responsibilities, among other things. While most legislation is relevant to sector CISRTs housed within a government entity, for standalone CSIRTs, authority may come from memoranda of understanding (MOUs) or legal agreements between the CSIRT and its members. A standalone CSIRT may also be established as a not-for-profit entity that has different legal requirements (from a business operating standpoint). In short, there are many options for establishing authority, and the development team should choose the path that makes the most sense for its particular situation and environment.

- **Proposed authority level**. Do draft policies or regulations exist? How do those draft documents alter the authority that a nation or economy has to manage cybersecurity in the sector that the CSIRT supports?
- **Enforcement.** What are the current enforcement mechanisms for proposed and current legislation, policy, or regulation?

The development team should understand that legal authority does not always come in the form of a legislative edict. Executive orders; agency or ministry rules and regulations; and other official, binding policy directives should be examined as part of the legal landscape where the sector CSIRT will reside. These types of legal guidance establish the limits and requirements that the sector CSIRT must adhere to.

The development team may also find non-mandatory, unofficial guidance that the sector's cybersecurity stakeholders use. This guidance is especially useful for constraining information gathering activities if it is widely used in particular sectors. Cybersecurity practitioners in a particular country can move among industries, and practitioners can use known guidance even if it is not directly applicable to their industry. The development team should search for widely used cybersecurity guidance across a nation or economy, even if it does not serve the sector's cybersecurity environment.

The development team must also consider international standards, regulations, and legislation. Cybersecurity practitioners often use foreign legislation or standards as guidance for creating cybersecurity requirements. Before analyzing a sector framework, the development team must gather information about foreign regulatory or legal frameworks.

Since a sector CSIRT is often closely tied to the CI definitions of a country or economy, the development team should be aware that these definitions can vary. Likewise, the relationship between the sector CSIRT and CI will also vary. It is common in many countries for CI to be defined in legal terms. Therefore, the development team and other sector CSIRT stakeholders must consider the legislation and legal requirements addressing these important terms.

At this point in the process, the development team should consider the following CI-related questions:

- Which critical industry sectors are priorities for the country?
- Are there documented technical and process capability requirements for individual sector CSIRTs?
- What other members of the national cybersecurity ecosystem have equity in CI? How will the sector CSIRT interact with them?
- What regional or international organizations cooperate with the country's national CSIRT and/or the country's sector CSIRTs?
- Is there guidance for a country's existing or potential sector CSIRTs?
- Is there guidance that can be applied to a country's sector CSIRTs?

In addition to existing laws, policies, and other regulations, there are other factors, detailed below, that can be tangential to forming the sector CSIRT. The development team should consider these factors during this phase. Understanding the following factors from the onset of sector CSIRT development can mitigate unforeseen challenges.

- **What level of authority does existing legislation or regulation mandate?** Legal environments can be complicated. Statutory compliance (i.e., compliance with laws) is different from regulatory compliance (i.e., compliance with rules). Security laws can differ from privacy laws. Legal *requirements* have different implications than legal *guidelines*. Understanding what level of authority and what type of compliance is required are important parts of setting the groundwork for an effective, functional sector CSIRT.
- **Is legislation drafted but not implemented?** Establishing a sector CSIRT under one legal framework only to see that legal framework significantly change shortly before or after sector CSIRT operations begin can lead to duplicated effort. The development team should know if significant legal changes are coming soon, and it should consider waiting to proceed until these changes become official.
- **Is legislation/regulation enforced?** Regulations and legal edicts may not be enforced for many reasons (e.g., political issues, lack of interest or capacity on the part of law enforcement, and court rulings). Understanding if and why laws and regulations are not enforced leads to better assumptions and choices about how to position the sector CSIRT.

1.6 Set Goals and Objectives

The final phase the development team must complete to satisfy the prerequisites involves setting goals and objectives for establishing the sector CSIRT. These goals and objectives drive the succeeding steps of the process; they are separate from the operational goals of the sector CSIRT itself. While the goals and objectives considered during the prerequisites phase focus on the process, they ultimately affect the sector CSIRT's final form, so there may be some overlap with later operational goals.

To enable the process of establishing the sector CSIRT, these goals and objectives must consider the as-is and to-be states:

- **The as-is state** defines existing cybersecurity capabilities within a nation or economy, the absorptive capacity within a country or economy, and the specific cybersecurity capabilities and absorptive capacity within targeted CI sectors. To meet the goals and objectives of the process, the as-is state must accurately assess the status of cybersecurity practices within the new sector CSIRT's national cybersecurity ecosystem and target sector.
- **The to-be state** defines the specific goal status of the cybersecurity capabilities and absorptive capacity of the targeted CI sector within a nation or economy. The to-be state defines generally what the *end* state and capabilities will be for a targeted sector.

Now is the appropriate time to understand and consider these states in the context of beginning the process of establishing the sector CSIRT. The development team and other stakeholders should be able to outline the current incident response capabilities in the sector (i.e., the as-is state) and the projected capabilities once the sector CSIRT is operational (i.e., the to-be state).

Moving from one state to the other (by conducting a gap analysis, creating a roadmap, and implementing changes) is covered in Sections 3 through 5 of this framework.

Once the development team understands the as-is and to-be states, it can begin defining goals and objectives for the sector CSIRT creation process. The development team should consider the following additional factors when it develops these goals and objectives:

- **What is the current gap between the legal authority given to sector stakeholders and their ability to impact cybersecurity practice in critical infrastructure?** Answering this question helps ensure that the sector CSIRT creation process addresses weaknesses in the sector's cybersecurity framework.
- **What is the plan for addressing the time periods between planning for and implementing the sector CSIRT?** Goals and objectives can be affected because of the period of time between the beginning and end of the sector CSIRT implementation process.
- **What time period is allotted to the development team to design the sector CSIRT?** This answer can affect the scope of goals and objectives because of the time needed to manage other critical parts of the process (e.g., analyzing and constructing a roadmap).
- **What support is expected from the sector CSIRT?** Developing and implementing a sector CSIRT requires a different skill set than ongoing support for an established sector CSIRT. Therefore, the development team should carefully consider goals that require future support since they must be addressed not only by the development team, but also by those providing ongoing support. The individuals or group providing that ongoing support may have needs or requests; they should be part of the process, and their needs should be considered.

The development team should share the draft goals and objectives for the process with collaborators and other stakeholders to get their consensus. This consensus-building process can happen in many ways, but it should be the final step in evaluating whether all prerequisites for establishing a sector CSIRT are in place.

2 Gather Information

This step describes the information to be gathered, how it should be gathered, and who should gather it.

Once prerequisites are considered and the development team is certain that the context and environment are appropriate for continuing the process, the focus shifts to *executing* the process. Defining the as-is state by gathering information helps determine current cybersecurity capabilities and capacity in the defined sector; this is known as the *gather information* step of the process.

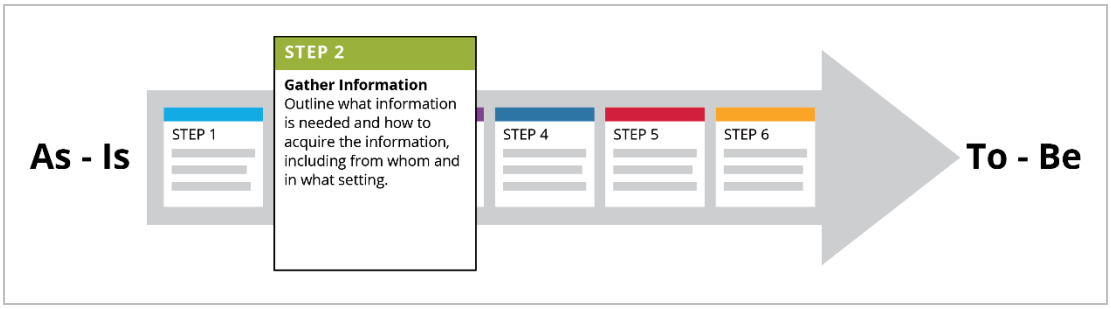

Figure 3: Step 2—Gather Information

This step can be broken into two broad parts, which are described in the following sections:

- 2.1 Define the Constraints to Information Gathering
- 2.2 Understand the Process and Gather Information

2.1 Define the Constraints to Information Gathering

In this step, the development team must gather only the information needed; it should not gather superfluous information. When implementing constraints to the information gathering process, the team should consider the following:

- **Identify varying information sources for sector CSIRTs.** Each CI sector can maintain different standards organizations, regulatory organizations, and organizations developing new technology within the sector.
- **Identify varying cybersecurity requirements for specific sectors.** Different sectors have different cybersecurity requirements and different standards, policies, or other documents governing these requirements.
- **Identify existing partners and stakeholders suitable for cooperation**. The development team should look inside and outside the CI sector for partners and stakeholders. Collaborators with cybersecurity expertise that operate in a nation but are outside a particular CI sector are likely familiar with local regulations, policies, and common community best practices.
- **Identify established national CSIRTs or other organizations with national cybersecurity responsibilities.** These organizations require leadership in, or at least situational awareness of, the national cybersecurity ecosystem. When gathering information within a sector, the information that national CSIRTs maintain for contacting cybersecurity practitioners or existing

sector CSIRTs is valuable. Many national CSIRTs also provide a coordination function between formal sector CSIRTs and informal networks, or among those within and across sectors.

Knowing and identifying sources, sector requirements, stakeholders, and national CSIRTS allows the development team to gather information that addresses all relevant issues and stakeholders while limiting the amount of data required for analysis.

2.2 Understand the Process and Gather Information

The development team can now begin gathering information, a process that consists of several steps, which are described in the following sections:

- 2.2.1 Define the Scope of the Process
- 2.2.2 Establish Information Gathering Goals
- 2.2.3 Conduct Open Source Research
- 2.2.4 Conduct Interviews

These information gathering steps will overlap and typically are not linear. For example, information gathered during interviews and discussions with cybersecurity practitioners may reveal new avenues of open source research for the development team to consider. Appendix B provides more detailed information about information gathering topics and design.

2.2.1 Define the Scope of the Process

When gathering information, the scope of activities refers to identifying priority sectors or sector CSIRTs and defining the depth of research necessary for the development effort. When defining the scope, information gathering activities that focus on a particular sector must address the following issues:

- **Which CI sector(s) will be assessed?** Limiting CI sectors for information gathering might be necessary due to a lack of accessible cybersecurity expertise in the sector, lack of available information related to a sector, or disagreements about what defines particular CI sectors.
- **What timeframe is available for conducting research and gathering information?** Assessing the cybersecurity incident response capability for CI sectors is time consuming because it requires additional research. This research includes investigating sector cybersecurity requirements and specialized cybersecurity technologies or processes that a CI sector uses.
- **What vendors or cybersecurity service providers that deliver services to CI sectors are within scope for information gathering activities?** Many organizations contract with external cybersecurity providers for some or all of their cybersecurity capabilities. The plan to gather information about contracted services should include an action to request that information either from the CI organizations that contract those services or from the external cybersecurity providers.

Some of these scope questions (e.g. Which CI sector(s) will be assessed?), are also covered in Step 1 of the framework, but others must be addressed during this step. Establishing the scope of

the process for gathering information helps the development team understand what *is* and *is not* important for defining the scope and goal setting.

2.2.2 Establish Information Gathering Goals

Defining the constraints and scope of information gathering enables the development team to develop related goals. These goals should be limited to specific sectors or cybersecurity disciplines across related sectors. The development team should consider what might help the sector CSIRT become operational and effective before firmly establishing research goals.

Below are examples of the types of information that help form information gathering goals:

- as-is and to-be states of cybersecurity capabilities
- cybersecurity practitioners' current understanding of their place in the sector and national cybersecurity ecosystem
- clarity about desired roles within the sector CSIRT framework
- role of the national CSIRT in relation to sector CSIRTs
- type of collaborative network desired in the sector CSIRT
- current and desired information sharing schema
- information sharing requirements
- primary processes and technologies used by the sector CSIRT
- current conflicts or challenges related to participating in the national cybersecurity ecosystem
- principal collaborators, desired collaborators, and entities or groups with which collaboration is limited for any reason

Research goals can shift as the team gathers information, so the development team should be flexible when setting goals. These goals should initially be communicated to stakeholders, and they must be updated immediately if there are changes. This approach ensures transparency and continued collaboration toward a common goal.

2.2.3 Conduct Open Source Research

The development team now conducts open source research (i.e., the discovery of any publicly available information) to identify current sector capabilities, absorptive capacity for creating and maintaining new capabilities, and the policy or legal cybersecurity framework surrounding the specific sector.

Resources from the cybersecurity governance structure of a nation or economy often provide information related to cybersecurity requirements for CI sectors. Open source research can happen in any order. Below are general research categories, listed from the most broad to the most granular:

- legislation, policy, and regulations
- national or economy standards
- organizational or trans-organizational governance documents
- technical specifications

- standard operating procedures (SOPs)

Open source research should include searching local news for cybersecurity incidents, CI incidents, and current best practices among particular CI sectors. Other than formal incident reports provided by sector or national incident handlers, local news may be the sole source of information related to incident types and their severities affecting a sector. Locally reported events can also impact the regulatory landscape and/or sectors in ways that help or hinder their ability to respond to cybersecurity issues.

Existing sector CSIRTs or national CSIRTs can have publicly available incident information, awareness material, or information related to the collaborative activities they participate in. Governmental or regulatory sources can also publish information about cybersecurity incidents reported within their area of responsibility or constituency.[14]

2.2.4 Conduct Interviews

After open source research is completed, interviews must be conducted to continue gathering additional information and validate the reliability of the open source information already gathered. The interview subjects selected should align with previously defined research goals. Interviews should focus on personnel who can provide valuable information about technical capability, absorptive capacity, and/or the sector governance environment.

2.2.4.1 Form Interview Questions and Topics

Information gathering interviews must have preplanned topics tied to each interview group. This framework cannot provide a full list of interview topics; however, a partial list is provided below:

- as-is and to-be states of the subject's cybersecurity capabilities
- information on cybersecurity practitioners' current understanding of their place in a sector and national cybersecurity ecosystem
- desired role within a sector
- role of a national CSIRT in relation to sector CSIRTs
- type of collaborative network desired in a sector CSIRT
- services desired by the subjects that the sector CSIRT could provide
- information sharing requirements
- information sharing schema
- primary processes and technologies employed or desired to be implemented
- current conflicts or challenges related to participation in the national cybersecurity ecosystem
- principal collaborators, desired collaborators, and entities or groups with whom collaboration is limited for any reason

[14] The sector CSIRT framework cannot attest to the veracity of government or regulatory reporting of cybersecurity incidents, but these organizations are often the sole source of quantitative information available on cybersecurity incidents.

The development team should ask questions that align with predetermined topics and the specific needs, goals, and challenges of the particular environment. Therefore, this framework cannot provide a one-size-fits-all list of interview questions. Considerations for developing tailored interview questions are provided below. Each consideration helps the development team create its own list of questions that are relevant to its particular needs.

- Consider what is "out of bounds" for the discussion or interview.
- Consider the audience; different questions are appropriate for different audiences.
- Consider if the questions, or a subset of them, can or should be provided to the interview/discussion group in advance.
- Focus on understanding the desired services or mission.
- Consider which broad questions, research, and discussion topics are applicable to any sector, and which ones are specific to certain sectors.
- Consider what must be understood about the national CSIRT's role within the sector and with the sector CSIRT, in both the as-is and to-be states.
- Consider how the sector or the sector CSIRT will share information.
- Consider future organizational and operational factors.

2.2.4.2 Determine the Interview Format and Setting

Obtaining the necessary information for developing a sector CSIRT requires successfully engaging with the stakeholders who possess that information. The interviews are critical activities, so they must be carefully planned and conducted. To get the most complete information possible, the development team should establish the format and setting of the interview.

- **Format.** The format of the interviews can help the development team get accurate and valuable information. Example formats include virtual or in-person interviews; facilitated discussions or short, structured questions; and one-on-one or group discussions.
- **Setting.** The development team should consider the setting carefully since it will likely impact the subject's ability and willingness to provide information. For example, some stakeholders may be more comfortable providing information in a private, one-on-one setting; however, group discussions can produce valuable insights from the interaction of the participants. The development team should weigh the costs and benefits of each decision about interview or discussion settings.

Generally, information gathering takes place in one of two setting categories, although there are other approaches and variations within each.

- **Scripted Interview.** In this setting, the development team asks the interviewees predetermined questions and records their answers. While there is room for unscripted discussion in this approach, it is limited. The interviewer retains control over the questions and the overall direction of the discussion. Also, because similar questions are asked of every stakeholder, it is easier to compare and contrast their responses and the efficacy of the information collected.
- **Facilitated Discussion.** In this setting, the development team might have a list of broad topics to discuss, and it might use some prompting questions. However, the discussion is left open and is allowed to veer in the direction that the interviewee desires. The development

team might not get answers to specific questions, but it may find unexpected value in unscripted responses.

The development team should also consider the following:

- how to separate the discussion between the as-is and to-be states
- whether the information obtained during interviews should be shared after the interview, either for follow-up discussion or other purposes

2.2.4.3 Conduct Interviews and Discussions

The development team is now prepared to conduct interviews and should consider the following:

- Ensure the interviewees understand the purpose and intended output of the interviews.
- Highlight the importance and value of the information interviewees provide.
- Establish trust with the interviewees by demonstrating shared values, agreeing to terms of anonymity, and providing transparency.
- Take notes; these notes serve as the raw material to be organized and inventoried in Step 3.

The outcome of interviews and discussions should be a fairly comprehensive collection of information that will aid in determining the as-is and to-be states.

3 Organize the Information and Evaluate the Gaps

The development team must now organize and inventory the information it gathered to determine the differences between the as-is and to-be states, and analyze these differences (i.e., gaps).

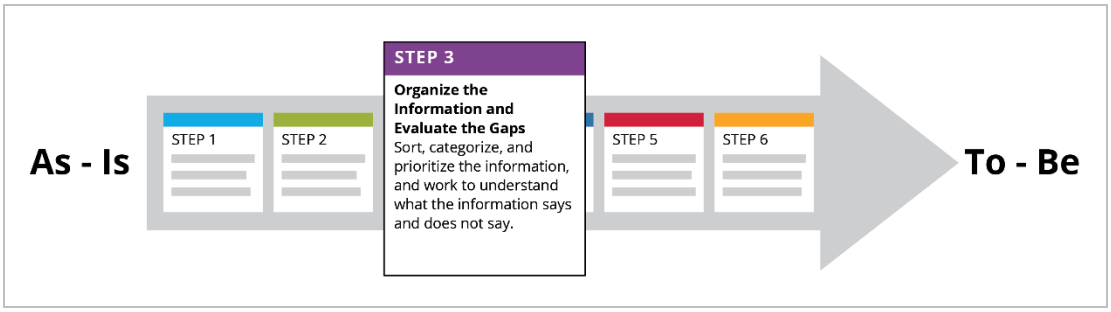

Figure 4: Step 3—Organize the Information and Evaluate the Gaps

This section describes the process the development team uses to inventory and analyze the information, and prioritize actions.

Organizing the information gathered and evaluating the gaps consist of several steps, which are described in the following sections:

- 3.1 Choose an Analysis Approach and Techniques for Evaluating Gaps
- 3.2 Examine the As-Is and To-Be States
- 3.3 Analyze the Gaps
- 3.4 Consolidate Gap Information and Determine Priorities

Organizing and analyzing information can be discouraging for the development team since it can uncover gaps in areas believed to be more mature based on interviews. This disconnect is a common challenge; the interviews can leave the development team with the impression that more is being done than the evidence indicates. Appendix C provides supplemental information to this step of the process.

3.1 Choose an Analysis Approach and Techniques for Evaluating Gaps

The value of gap analysis is that it clearly documents what is *evidenced* and aligns it against a baseline standard. Process strengths and weaknesses are highlighted, and current ad-hoc elements are identified for formalization. These gaps and findings feed into the roadmap planning exercise that follows in Section 4.

In some cases, a gap represents an item missing from the to-be state. In other cases, a gap represents an item that is not operating effectively (i.e., the item exists but is not as mature as its to-be goal state). Development teams commonly evaluate gaps using one of the following analysis approaches:

- A **Gap Analysis** is an exercise that identifies areas where there are gaps measured against specific criteria. Gaps can include missing tools, processes, or policies that hinder achieving

desired goals. Analyzing gaps also identifies weaknesses that inhibit success. Weaknesses can be due to the lack of formal policies or processes, training, or a comprehensive view of issues that can hinder a sector CSIRT's success. Using a gap analysis, the development team identifies which issues should be improved and assembles that information for use in developing a corrective action roadmap.

- A **SWOT Analysis** is a strategic planning technique that helps identify where an organization is and compares it to where it would like to be [Zeltser 2008]. The development team conducts a SWOT analysis by developing a table to evaluate current Strengths, Weaknesses, Opportunities (areas for improvement), and Threats (things that stand in the way). The team can evaluate each strategic initiative and prioritize the needed improvements.
- A **Maturity** or **Capability Analysis** helps determine where a program stands on a spectrum in relation to specific criteria. For example, Figure 5 depicts the SEI's CSIRT Capacity Development Continuum, which has six levels that indicate where a CSIRT is in its development. The OpenCSIRT Foundation published a Security Incident Management Maturity Model (SIM3) to help teams determine how well they govern, document, perform, and measure their CSIRT functions [Stikvoort 2019]. When comparing the as-is and to-be states, an item should be analyzed for both its existence and its maturity; this analysis can be done by comparing each item to the maturity/capability model and determining its effectiveness in the as-is state. If the item does not exist, or if it exists and needs to be improved, it is added to the roadmap developed as part of Step 4.

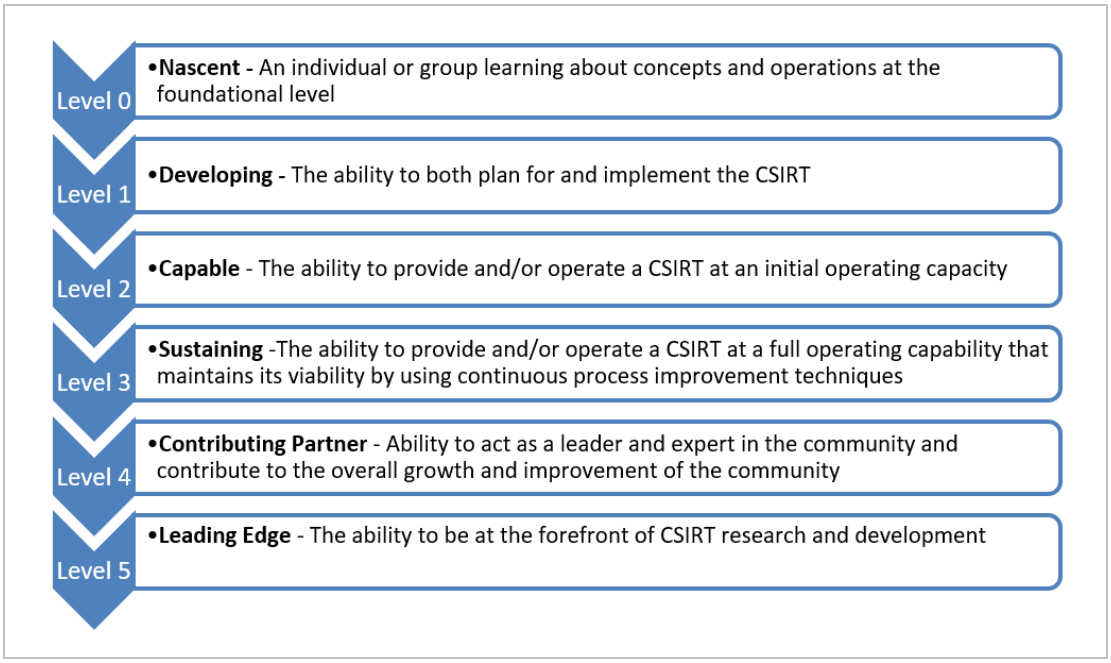

Figure 5: CSIRT Capacity Continuum

3.2 Examine the As-Is and To-Be States

Once the development team chooses an analysis approach, it evaluates the information it gathered against a baseline to document the as-is state. Appendix C provides baseline guidance that can be useful if the development team hasn't already selected another to-be state.

Using the to-be baseline, the development team examines each to-be item and determines if as-is information exists to address it. If the as-is items exist, the team determines if they align with the desired to-be state. The development team evaluates the as-is state using the following general steps:

1. Identify the information in the as-is state.
2. Review the to-be state.
3. Determine the to-be items that are missing in the as-is state (i.e., no information currently exists that addresses the to-be item) or the level of maturity of the as-is information, if it already exists.
4. Compile the actions needed to address the gaps. (These actions should be addressed in the roadmap, which is formed in Step 4.)
5. Consolidate the actions by category or focus area.
6. Prioritize the actions.

3.3 Analyze the Gaps

The development team now analyzes the gaps using the technique identified in Section 3.1. The following high-level example depicts a gap analysis using the output from the previous section.[15] For each gap identified, the development team identifies the steps needed to improve the capability to the desired operational status and notes these steps for the roadmap activities that are part of Step 4.

- **Examine governance for the sector CSIRT.** Determine if the foundational aspects of the CSIRT have been established, documented, and agreed upon. A sector CSIRT must have an established chain of authority as well as a secure and ongoing source of funding.
- **Examine planned incident management capabilities.** Determine the capability of existing processes and documentation related to incident identification, detection, response, and management.
- **Examine communication channels.** Identify the established communication channels; determine if they are documented and implemented internally and with external partners.
- **Examine the cybersecurity ecosystem.** Identify the cybersecurity organizations that will be used for information sharing or that will help with incident management. Ensure that the role of the national CSIRT is clearly defined from the sector's perspective. Determine if the roles of other CSIRTs are documented and understood.

[15] This example is not a prescriptive guide; it simply provides an example of how the process works and how the development team might apply its own selected approach. See additional details for each step in Appendix C.

3.4 Consolidate Gap Information and Determine Priorities

The development team now consolidates and organizes the gap information. Understanding which items exist and which are missing or need improvement helps the development team build the roadmap as part of Step 4.

The development team should briefly discuss each gap found, the nature of the gap, and identify actions to resolve the gap. For example, Table 1 illustrates a simplified gap analysis template. Providing an importance indicator for each gap area or section further helps the development team establish priorities.

Table 1: Gap Analysis Template

Gap Analysis Steps			
As-Is State	**To-Be State**	**Identified Gaps and Needs**	**Function/Focus Area**
Step 1: Determine and document the as-is state from the information gathered.	Step 2: Determine and document the desired state.	Step 3: Identify gaps and needs between the as-is and to-be states. These gaps and needs are then prioritized and used to develop the actions/activities of the roadmap. (See Section 4.)	Step 4: Consolidate and prioritize gaps by category or focus area (e.g., governance items like a mission statement or funding, or planned incident management capabilities).

At the end of the gap analysis, the development team should understand the gaps between the as-is and to-be states and what actions are needed to close the gaps. Each gap is prioritized and has a documented set of needs for progressing to the to-be state. This documentation drives which activities and initiatives are included in the roadmap.

4 Build a Roadmap

Gathering, categorizing, and analyzing information are significant steps in developing a sector CSIRT. However, the development team still must translate this information into a functioning incident response team or capability. A key tool that the development team uses at this stage is a *roadmap*. A roadmap is a step-by-step guide for implementing the capability.

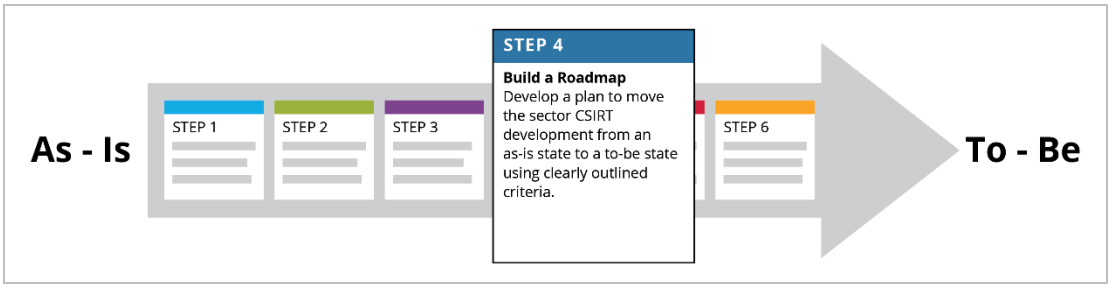

Figure 6: Step 4—Build a Roadmap

To build the roadmap, the development team breaks down the information it gathered and matches identified gaps with the actions needed to close those gaps. This section discusses several steps, which are described in the following sections:

- 4.1 Understand the Purpose of a Roadmap
- 4.2 Outline the Steps Needed to Create a Roadmap
- 4.3 Identify Roadmap Considerations and Create the Roadmap

4.1 Understand the Purpose of a Roadmap

A roadmap is a planning tool used by those implementing a strategic or long-term goal to map out how they will move an organization from an as-is state to a to-be state. A roadmap can take a variety of forms, but the goals remain the same:

- Clearly describe the actions and steps to be taken.
- Provide a mechanism and approach for taking these actions and steps.
- Form a timeline for the roadmap activities.

For sector CSIRTs, a roadmap is a tool that the development team uses to reach the desired outcome: a functional and effective sector CSIRT. The development team's roadmap is the mechanism it uses to move the sector CSIRT from *concept* to *reality*; it is used to plan and implement the sector CSIRT as part of Step 5.

This step of the sector CSIRT framework helps the development team *apply* what it learned up to this point in the process. The first part of this section describes how to develop a roadmap. The second part describes the *components* of the roadmap.

4.2 Outline the Steps Needed to Create a Roadmap

To successfully build a roadmap that guides the development team from concept to reality, the team must complete some preparatory steps:

- 4.2.1 Define and Understand the Goal of the Roadmap
- 4.2.2 Consider Terminology and Approach
- 4.2.3 Apply the Framework
- 4.2.4 Transition from As-Is to To-Be

To complete these steps, the team can coordinate and collaborate with a national CSIRT or other stakeholders.

4.2.1 Define and Understand the Goal of the Roadmap

A roadmap is not the final outcome of this framework, nor does successfully developing a roadmap guarantee the successful creation of a sector CSIRT. Rather, the roadmap documents the knowledge, information, and other stakeholder input required to implement a sector CSIRT that was gathered, organized, and is ready to be put to work.

The development team must clearly understand what a roadmap is and what it is designed to do. Understanding what should be in the roadmap, how it should be constructed, and how it will be translated into implementation are all critical parts of the process. A roadmap for establishing a CSIRT should also consider any constraints or stakeholder requirements that might be incompatible with the sector CSIRT; incompatibilities may cause problems as sector CSIRT functions evolve.

4.2.2 Consider Terminology and Approach

The development team can use multiple documents and tools to build a new capability—a roadmap is just one of them. Others include action plans and implementation plans; they can be used with a roadmap, but they should not replace it. A roadmap defines the as-is state, to-be state, and the checkpoints or indicators that mark the path from one state to the other. An action plan describes the specific actions for reaching checkpoints and the to-be state. An implementation plan[16] outlines how these actions are implemented, who implements them, and when they should be implemented.

4.2.3 Apply the Framework

Constructing an effective sector CSIRT roadmap is not possible until the development team completes the previous steps in the framework. Having prerequisites in place ensures that the conditions for success are in place. Gathering information (e.g., open source research, facilitated discussions, and intensive document review) ensures that a complete picture of the environment is

[16] Section 5 describes how to plan and implement the sector CSIRT; Section 5 can be used with or instead of an implementation plan.

developed and all relevant stakeholders are consulted, including the national CSIRT. Using analytic techniques (e.g., gap analysis) helps the development team understand what items should be considered and how to assemble them.

4.2.4 Transition from As-Is to To-Be

When developing a roadmap, the development team must leverage what it learned and defined to develop clear as-is and to-be states for the transition process. Once these states are well defined and the development team conducts a gap analysis, the roadmap process links these actions from point to point. The development team should clearly define and describe how the sector CSIRT is formed, what services it might (or might not) offer, how it works with other stakeholders in the environment, and what timeline it expects to adhere to.

4.3 Identify Roadmap Considerations and Create the Roadmap

This section describes considerations for and an example of a sector CSIRT roadmap. Many initiatives and milestones can be conducted simultaneously; conversely, some milestones might have dependencies on others. In any case, the required actions identified during the gap analysis should serve as the starting point for developing milestones and aligning them to the roadmap.

4.3.1 Outline the Services Offered

When developing a sector CSIRT and creating a roadmap, the development team must determine which services to offer the constituency. This process involves naming and defining each desired service to understand the activities that must be incorporated into the roadmap. The development team must select services that support the constituents' missions and the CSIRT's purpose.

Each sector CSIRT is different because each provides services based on its mission, purpose, and constituency. There are many services that a sector CSIRT can offer. Determining which services to offer as part of the roadmap process is critical to Step 5 (Plan and Implement the Sector CSIRT) of the framework.

The services the sector CSIRT offers determine the resources, skill sets, and partnerships the CSIRT needs to function properly. The services offered should be those that the CSIRT can realistically provide based on its size and expertise. In general, CSIRTs should begin by offering a small set of services that it can provide and support very well instead of offering many services it might not be able to provide or properly support. As a CSIRT gains the trust and respect of its constituency, it can expand its services as staff and funding permit.

While many teams develop their own services and frameworks, FIRST developed the *CSIRT Services Framework*, depicted in Figure 7. This framework groups CSIRT services into five areas

with supporting services and functions within each. Generally, a CSIRT does not provide all of these services; instead it provides the services that best align with its mission and constituents.[17]

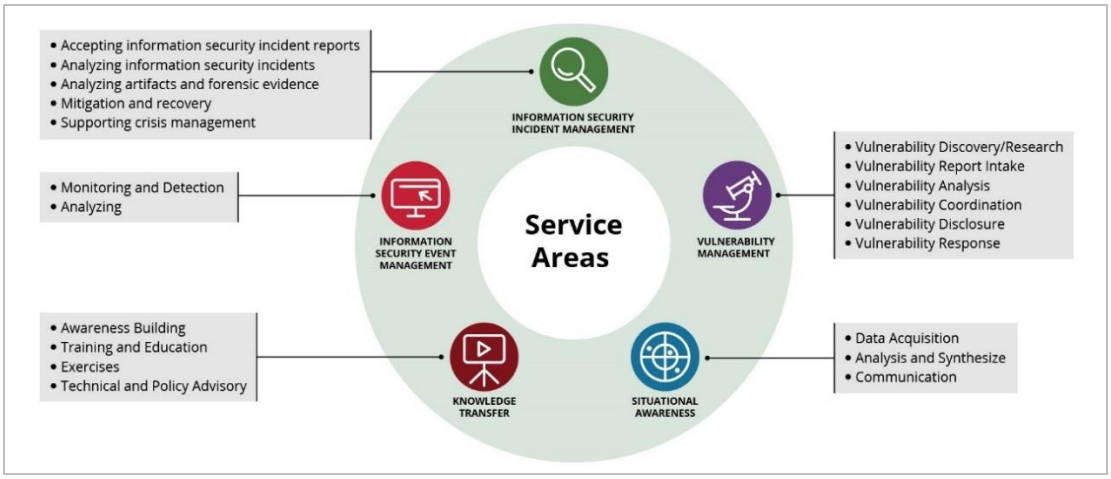

Figure 7: CSIRT Services Framework: Service Areas [FIRST 2019]

4.3.2 Address the CSIRT's Role Within the National Cybersecurity Ecosystem

A key function of a sector CSIRT—and a determinant of its effectiveness—is the role it plays in sharing information within its sector and national cybersecurity ecosystem. A sector CSIRT's ability to collaborate, coordinate, and share information within a national cybersecurity ecosystem ensures its success. How a sector CSIRT performs these functions must be considered while the roadmap for the sector CSIRT implementation is being developed. Also, requirements from the national CSIRT can help the sector CSIRT determine how it collects, uses, and shares information.

Understanding the expectations of the national CSIRT and sector CSIRT helps develop a realistic and achievable roadmap that aligns with national cybersecurity objectives. The development team must understand the desired roles, responsibilities, and capabilities of the sector CSIRT—including how the sector CSIRT will interact with the national CSIRT—to capture items that should be a part of the roadmap.[18]

4.3.3 Develop Policies

To address gaps and operationalize a sector CSIRT, the development team must acknowledge and develop internal and external organizational policies that are critical to perform the required actions and activities on the roadmap. These policies depend on the gaps identified, services offered,

---

17 FIRST service areas are summarized in Appendix D and addressed in further detail in Section 5 of the framework. More information about the *FIRST CSIRT Services Framework* is available on the FIRST website [FIRST 2019].

18 See Sections 1 and 5 for more information about sector CSIRT integration within the national cybersecurity ecosystem.

and the expected roles and responsibilities of the sector CSIRT. They typically outline the general cybersecurity expectations and the roles and responsibilities of the sector CSIRT.

Sector CSIRTs operating in heavily regulated industries must adhere to specific legal requirements that are normally unique to the legal jurisdiction where they operate.[19] These regulations must be considered for their incorporation into policy and the roadmap.[20]

4.3.4 Address Training Gaps

Sector CSIRT staff training is another roadmap consideration. Training should initially focus on bringing new staff members up to the skill level needed to undertake the work and activities defined in the roadmap. Follow-on activities during and after implementation can include broadening the abilities of staff members and keeping the overall CSIRT skill set up-to-date with emerging technologies and malicious actor trends. Undoubtedly, training gaps will exist; these gaps require actions in the roadmap to identify the overall skills needed for each team member and general skill coverage required for the sector CSIRT to complete its mission and support its constituents.

4.3.5 Define Milestones and Metrics

In the roadmap, the development team establishes key milestones and checkpoints that document and confirm progress. Specific metrics or measures are also developed with these milestones to help gauge progress; milestones are different for each roadmap and should correspond to the unique situation and needs of the sector CSIRT and its stakeholders.

In any case, the roadmap should contain a way for the development team to confirm progress on the path from the as-is to the to-be state. Key indicators can include the following:

- identifying the constituency
- determining key roles and responsibilities
- meeting and aligning with the national cybersecurity ecosystem and regulatory requirements
- selecting key technologies to assist with information sharing and incident classification

4.3.6 Create the Roadmap

Figure 8 provides a high-level example of a roadmap. Every environment, development team, and sector is unique; therefore, this example is only a generic template for the development team to tailor based on its own needs, required actions, and desired operational state.

---

[19] Examples of such legal requirements include the Health Insurance Portability and Accountability Act (HIPAA) and the Sarbanes-Oxley Act (SOX) in the U.S., and the General Data Protection Regulation (GDPR) in the European Union.

[20] For more information about legal considerations, see Section 1.5.

Many development teams and sector CSIRTs have their own programs or project management approaches and/or requirements. The sector CSIRT can also have unique business requirements, depending on how and where it is hosted. Therefore, it is not possible to provide an all-inclusive roadmap. Each one must be developed and tailored based on the gaps and required actions identified in the analysis. Figure 8 is one example of a generic roadmap.

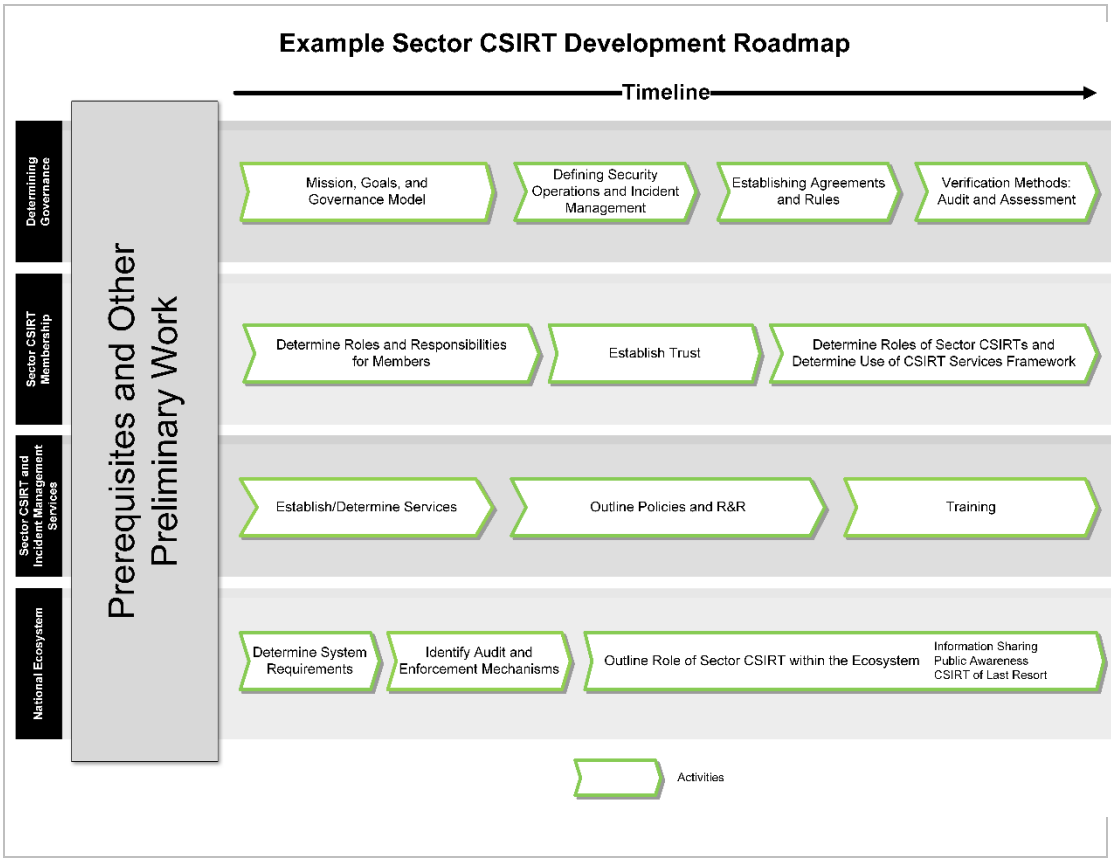

Figure 8: Roadmap Example: Parallel Work Tracks for a Sector CSIRT Development Team

5 Plan and Implement the Sector CSIRT

The final step in establishing the sector CSIRT is implementing the roadmap. This section describes the planning and implementation process and discusses how to find help along the way.

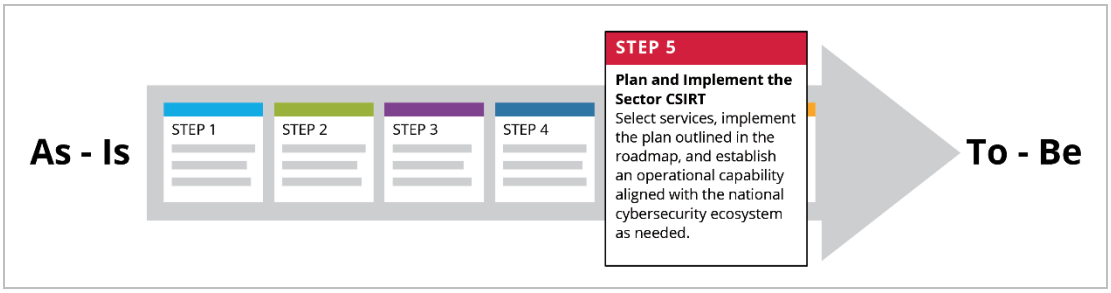

Figure 9: Step 5—Plan and Implement the Sector CSIRT

A key factor common to all implementation processes is communicating with stakeholders. Throughout the implementation cycle, the development team should communicate progress along the roadmap, identify roadblocks or concerns, and address roadmap changes with flexibility and transparency.

Broadly speaking, an implementation process involves several steps, which are described in the following sections:

- 5.1 Gather Implementation Expertise
- 5.2 Plan for Implementation
- 5.3 Consider and Execute Specific Services
- 5.4 Communicate Implementation Progress
- 5.5 Integrate with the National Cybersecurity Ecosystem

5.1 Gather Implementation Expertise

Prior to implementation kick-off, the development team should consider other inputs and resources that can help it understand the overall implementation process, common roadblocks, and implementation tools. Many countries have existing national and sector CSIRT teams. It is a best practice to arrange discussions with CSIRT members in similar regions, sectors, and/or countries. Other national or sector CSIRTs that have expertise in the geographical area may be willing to identify common challenges when implementing a CSIRT. Finding a mentor or partner to advise the development team is useful when questions or unforeseen issues arise.

The development team can find an advisor using a global or regional forum of CSIRT organizations. FIRST maintains a publicly available database of member CSIRTs across the world [FIRST 2020a]. This database can be filtered by country or name, and contact information is provided about the CSIRT. The best ways to find valuable advisors is to reach out to CSIRTs and leverage the in-country national CSIRT (if applicable).

It is helpful to review lessons learned from other teams' implementations related to the following general areas:

- Communicating the sector CSIRT plans and gaining support from the stakeholders
  - Transparency and communication are critical to building successful relationships and ensuring that all interested parties can contribute. Sharing information gathered from others' experience can provide insight and help stakeholders prepare for the future.
- Socializing the roadmap and implementation plans to gather feedback
  - Experiences from others—good and bad—can help the development team understand the possible outcomes of socializing the roadmap and implementation plans. These experiences can enable the team to proactively address potential issues with stakeholders. Feedback that others received can augment the roadmap and fill gaps that current stakeholders might not have identified.
- Understanding current technical platforms and which ones might align well with the sector's needs and priorities
  - Using technical tools similar to others in the sector is typically ideal, especially for information sharing. Ask external advisors for their experience in this area to see what they have learned. For example, if many sector participants use Linux systems, it might be advantageous to build CSIRT capabilities on Linux systems.
- Gathering information from similar implementations, including how common obstacles were overcome
  - Implementations of CSIRTs and other similar organizations have many commonalities. Gathering available information about overcoming challenges can help shorten implementation time. It is also possible that a sector CSIRT will discover challenges that are different from what others experienced. While not directly related to the information gathered in this step, discussions about challenges can yield useful ideas for the development team to consider.

5.2 Plan for Implementation

In this step, stakeholders, partners, and participants plan the implementation by gathering to discuss socializing the roadmap. The development team ensures that all parties understand the plan; the team also addresses critical foundational and administrative items associated with implementation planning. Socializing can happen with a large or small group, depending on the context of the sector CSIRT. At a minimum, these conversations should review the topics listed below:

Foundational Topics

- sector CSIRT mission, goals, and governance
- shared values of the CSIRT and its stakeholders
- agreements/rules between the sector CSIRT and its constituents, as well as between the sector CSIRT and others in the national cybersecurity ecosystem, including
  - type of documentation needed
  - MOUs needed and what they should include

  - other documents (e.g., codes of conduct, non-disclosure agreements [NDAs], Standard Operating Procedures [SOPs], and information sharing rules)
- the current roadmap, including the priorities assigned to each area
- development team members and stakeholders, including clear roles and responsibilities

Services

- services offered by the sector CSIRT
- resources and budget, including plans to hire and train staff based on the services offered
- initial policies and procedures
- available or needed equipment and tools to support the services offered
- guidelines and/or forms required by or for the constituency, depending on the services offered

Communications

- communications plan for sector CSIRT implementation
  - How will information be disseminated to, socialized with, and made available to all stakeholders? Include processes and tools that enable effective communications.
- formal announcements and kick-off activities

Trust Building

- approaches to building and extending trust between stakeholders
  - Many benefits of sector-based collaboration about cybersecurity are predicated by some level of trust among the sharing parties.
- approaches to building and maintaining trust with the community, including developing and maintaining the relationship with the national CSIRT and its integration into the cybersecurity ecosystem
- a plan for building trust at the organizational and individual level
- how to address longstanding reasons for the lack of trust between organizations

5.3 Consider and Execute Specific Services

Even though the development team selects services earlier in the process, there are many implementation considerations for the sector CSIRT's selected services, including related processes, procedures, and technology. The *FIRST CSIRT Services Framework* identifies top-level considerations for each service area listed below [FIRST 2019]. Appendix E describes more detailed implementation considerations, including descriptions of minimum required tasks and general knowledge needed for each service area.

5.3.1 Information Security Event Management Service Area

Constituency Operations. Sector CSIRTs should be familiar with, or have a basic understanding of, their constituency's operating environments. The constituency should be informed of the sector CSIRT's processes for identifying events, incidents, and associated incident categorization ac-

tivities. Familiarity with a sector CSIRT's incident management process and how to share information ensures the constituency can provide event information to the sector CSIRT for analysis and coordination.

Technical Components. Sector CSIRTs should be familiar with common incident management and information sharing standards used for communicating event and incident information in information sharing communities.

Incident Management Community. Sector CSIRTs should establish relationships within the broader CSIRT information sharing community. These relationships are a source of incidents that affect others and can be early warning indicators to assist preparations within the sector. Other CSIRTs can also provide mentoring or advice to the sector CSIRT to help with incidents the constituency experiences.

5.3.2 Information Security Incident Management Service Area

Constituent Operations. Sector CSIRTs should be familiar with, or have a basic understanding of, their constituency's ability to collect, compile, and transmit system and network information related to specific timeframes or incidents.

Technical Components. Sector CSIRTs should be familiar with basic information about their constituents' current information security posture and the details of any incidents provided.

Incident Triage. Sector CSIRTs must be able to review and prioritize incoming constituent incidents. A baseline ability to do this task does not require the process to be formalized, but a sector CSIRT should be able to understand and explain its informal triage processes.

Incident Analysis. Sector CSIRTs must be able to perform analytical tasks that lead to the creation or discovery of information that allows constituents to mitigate or remediate incidents.

Incident Mitigation and Remediation. Sector CSIRTs must be able to perform at least one of the following tasks:

- Mitigate incidents on behalf of their constituents.
- Present information to constituents, allowing them to mitigate incidents.
- Remediate incidents on behalf of their constituents.
- Present information to constituents, allowing them to remediate incidents.

5.3.3 Vulnerability Management Service Area

Constituency Operations. To provide effective Vulnerability Management services, sector CSIRTs should be familiar with, or have a basic understanding of, their constituents' operating environments.

Vulnerability Technical Components. Sector CSIRTs should be familiar with the technical languages that describe vulnerabilities. In particular, the development team should ensure that sector CSIRT members are familiar with the Common Vulnerability and Exposure (CVE) system and the Common Vulnerability Scoring System (CVSS).

Mitigation Creation and/or Application. Creating, packaging, and distributing mitigations are activities sector CSIRTs should be able to perform when offering vulnerability management as a service.

Patch Management. Sector CSIRTs should be able to package and distribute patches for vulnerability management.[21]

5.3.4 Situational Awareness Service Area

Sector CSIRTs must understand how the constituency operates under normal circumstances and be able to identify abnormal operational changes. Situational awareness also means keeping current with what is happening in the greater CSIRT community so that relevant information can be passed along to the sector CSIRT's constituency.

Constituency Operations. Sector CSIRTs should be familiar with, or have a basic understanding of, their constituency's baseline operating environments to ensure they can provide effective situational awareness when needed.

Situational Awareness Technical Components. Sector CSIRTs should be familiar with the technical baselines within the constituency and how to distribute relevant information to the constituency or the global CSIRT community.

5.3.5 Knowledge Transfer Service Area

Constituent Operations. Sector CSIRTs must have known communication channels that are open and maintained with their constituency. Constituencies must be informed of the knowledge transfer activities the sector CSIRT undertakes, and updates should be communicated to the constituency regularly. Ideally, this process should be formalized, but it is not required.

Technical Components. Technical components of a sector CSIRT's knowledge sharing program consist of transmission mediums and content. Sector CSIRTs must maintain a record of knowledge transfer activities offered and eligibility requirements for participation in knowledge transfer activities.

5.4 Communicate Implementation Progress

Throughout implementation, the development team should continually review the roadmap to ensure that the roles and responsibilities are clear to all stakeholders and reasonable timelines are set for completion. The cadence and means of keeping stakeholders informed should also be part of implementation planning.

---

[21] Patch creation is excluded because it requires specific knowledge of particular applications or configurations. It is normal for CSIRTs to package and distribute patches without input into their development.)

Providing accurate updates to stakeholders maintains transparency and keeps stakeholders engaged and willing to participate in sector CSIRT activities. For each area of the roadmap, the development team should consider including the following when it reports progress to stakeholders:

- the status of each major area of the roadmap, including the percent complete and issues the team believes might impede progress prior to the next checkpoint
- progress toward milestones within each area of the roadmap, including progress related to metrics established in the roadmap
- a simple visual representation of tracked milestones and accomplishments since the last report, and priorities/goals for the next report

The progress reporting cycle can be augmented with regular discussions of the implementation as a means for requesting feedback from stakeholders and partners. This feedback should be incorporated into future activities or roadmap/implementation adjustments as needed. It can also be helpful to schedule progress discussions with advisors to get outside perspectives on how adjustments might be made to an implementation iteration.

5.5 Integrate with the National Cybersecurity Ecosystem

When implementing a sector CSIRT, it is critical for the development team to understand that this new sector CSIRT will (1) become an important part of the national ecosystem[22] and (2) can affect how other stakeholders play their part.

Integration into the national cybersecurity ecosystem is essential regardless of which sector (public or private) the CSIRT supports. However, as the development team implements the sector CSIRT, it must continually revisit the questions asked in Section 1.2.1 and address changes (indicated in the right column of Table 2) to the ecosystem during the implementation phase.

Table 2: Questions Revisited During Implementation

Original Question	Revisited Question
What role will the national CSIRT (if there is one) play in the sector?	Have roles and responsibilities changed from the early planning and prerequisite stages?
What relationship will the sector CSIRT have with the national CSIRT?	Has this relationship changed or improved since the early planning and prerequisite stages?
If there is no national CSIRT, how does this impact the sector CSIRT's role in the national cybersecurity ecosystem?	Has a national CSIRT operationalized in the time between the planning and implementation stages?
How will the sector CSIRT address issues related to working with the public and private sectors nationwide?	What activities have been identified on the roadmap for implementation as it relates to these factors? Are there additional factors to consider during implementation? Have there been any developments regarding public-private partnerships that can be leveraged?

[22] See Section 1.2 for a discussion of the national cybersecurity ecosystem.

5.5.1 Public/Private Considerations

Public/private considerations and relationships are considered at the start of sector CSIRT planning. However, the development team must address the following implementation and technical considerations as well.

- **Roles and Responsibilities**. Which entities will serve which roles during an incident and throughout the incident management process?
- **Communication**. How will the sector CSIRT communicate with stakeholders across the sector? Will there be different channels for public and private entities? How will informal communications work?
- **Information Sharing**. What platforms will be used to share information? Who will operate them, and how will the data be handled and protected?

The development team should be prepared to face many challenges during the implementation stage. This stage is where actions must be established and where the "seeds" of the sector CSIRT's long-term sustainability (e.g., building trust) are "sown." By reviewing all relevant considerations and carefully considering each measure being implemented, the development team can overcome these challenges.

6 Conduct Post-Implementation Activities

While implementation is the final step in establishing a sector CSIRT, post-implementation tasks are the bridge between creation and sustainment. Creating an incident response capability does not ensure its success; there are continuing challenges and needs that the sector CSIRT must address, ranging from assuring sustained operations to expanding capacity and capabilities to meet future challenges. Operationalizing a sector CSIRT is just the beginning.

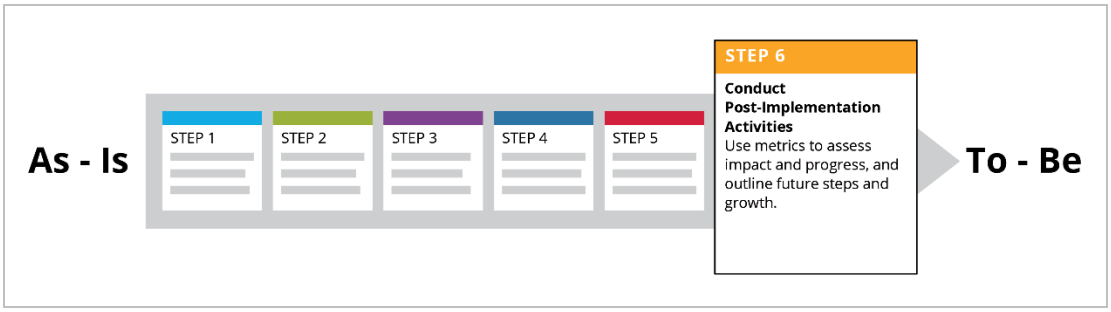

Figure 10: Step 6—Conduct Post-Implementation Activities

To ensure that a sector CSIRT can sustain operations successfully, the development team captures what was done during the process, what went as planned, what could have been done differently, and how expectations from the beginning of the process were or were not met. To capture this information, the team must revisit measures of success and think about what comes next for the sector CSIRT.

The development team should do the following after implementation:

- 6.1 Review the Implementation Process
- 6.2 Use Metrics
- 6.3 Report the Results of Implementation
- 6.4 Plan for the Future

6.1 Review the Implementation Process

After implementation, the development team must review the implementation process, both within the development team (i.e., internally) and the larger group of stakeholders (i.e., externally). In the review, the development team should assess (1) the implementation cycle, (2) changes made from the original roadmap, and (3) the remaining gaps to consider for future improvements.

Gaps can be roadmap items that were not completed, low-priority items that were deemed unnecessary for the initial implementation, issues discovered during implementation that were deferred, or stakeholder feedback that could not be included in the initial implementation cycle.

The development team should document and review these items with stakeholders to help prioritize future improvements and next steps for the sector CSIRT. The development team should also

review progress reports and feedback from stakeholders to see if there are lessons that could help improve future updates.

There are many useful approaches for conducting this review. For this framework, the two most useful approaches are After-Action Review and Post-Mortem Review. These two approaches are described briefly below, and their characteristics are summarized in Table 3.

- **After Action Review (AAR)** is a process first developed by the U.S. Army for providing feedback on training exercises [IDA 1999]. Many organizations have used the AAR and adapted it to evaluate the success (or failure) of their projects and processes. The AAR has several key characteristics that distinguish it from other review processes: (1) feedback is generally limited only to the stakeholders involved in executing a project, (2) feedback tends to be part of a cycle, and (3) feedback focuses on preparing for the next steps in the process [IDA 1999].
- **Post-Mortem Review** is a less-iterative process. These reviews are common in the software and technology industry; their purpose is determining what can be done better by evaluating what went wrong [Collier 1996]. This process is normally conducted at the end of a project; it asks all stakeholders to evaluate what went well and what did not.[23]

Table 3: After-Action and Post-Mortem Reviews[24]

	After Action Review	Post-Mortem Review
Purpose	Preparing for next steps or the next cycle	Examining and understanding what happened during the process
Occurrence	Throughout the project, gaining insight and perspective	After project completion, looking back on the entire project
Stakeholder Involvement	Limited to implementors	All stakeholders
Scope	Specific issues and challenges	The entire process
Outcome	Action plan for the next steps or next cycle	Complete report addressing the full process and any issues

The development team must ensure the review is conducted to meet its needs and those of the sector CSIRT. The team can use an AAR or post-mortem review, or it can use another review process. Regardless of the approach used, the goal remains the same: determine how successful the sector CSIRT implementation was and if additional work is needed to ensure that the desired operational capability and capacity is achieved.

---

[23] *Lessons learned* is another common term (used by NIST and others) in incident response. A lessons learned exercise is similar to a post-mortem review and can be used in similar situations.

[24] This table is adapted from the article *Emergent Learning in Action: The After Action Review* [Parry 2001].

Ultimately, the post-implementation review determines if the goals of the process were achieved. The development team should consult the process goals (developed in Section 1.6) when conducting a review. Beyond meeting the expressed goals, other questions for review include the following:[25]

- Were all stakeholders' needs met?
- Were all gaps successfully identified and closed?
- Is the sector CSIRT prepared for what comes next, whether it is sustained operation or a new round of capacity and capability development?
- What lessons were learned from the process?

6.2 Use Metrics

Section 4.3.5 defines metrics in the context of building the roadmap. In this step, the development team seeks to understand how well it met its goals and what the current status of the sector CSIRT is (e.g., what its capabilities are and what shortcomings may be present). This understanding ensures that implementors, planners, and other stakeholders can decide what comes next.

It is important to distinguish between metrics that measure sector CSIRT performance (i.e., performance metrics) and metrics that measure the process used by the development team while gathering information, completing the roadmap, and/or operationalizing the sector CSIRT (i.e., process metrics). Both types of metrics are important and can be used to gauge how successful implementation of the sector CSIRT was. However, both types of metrics should remain distinct from each other.

The focus of this framework is answering the question *Were the goals of the process met?* Only process metrics are addressed as part of the post-implementation review. As covered in Section 5.4, when implementing the roadmap, implementors should regularly report their progress toward achieving milestones in each area of the roadmap, including progress that is related to metrics established in the roadmap. When understood in this context, process metrics should focus on how successful the process was in moving from the as-is to the to-be state of developing a sector CSIRT. Final process metrics should measure if that work is complete.

If the goal of the process was to build a sector CSIRT that is capable of responding to incidents reported by constituents within the sector, the following metrics might be useful:

- Do the governing policies address incident response roles and responsibilities?
- Does the final operational capability provide the necessary tools and equipment for incident responders to do their jobs?[26]

---

[25] This list is not comprehensive and is only meant as a guide. Like many parts of the sector CSIRT framework, each implementation is different; therefore, the review process differs as well.

[26] Examples of performance metrics that can measure similar criteria include the number of incidents reported, the number of incidents resolved, or the time required to resolve incidents.

Alternatively, if the goal of the process is to build a sector CSIRT capable of coordinating response and sharing information, then useful metrics might include the number of other CSIRTs with which relationships have been established.

Other questions to consider when developing additional process metrics include the following:

- What is being measured? How precise does the measurement need to be? How will it be measured?
- Is the metric measuring what happened during sector CSIRT implementation or what resulted from the implementation process?
- What are the objectives for the sector CSIRT? Do the metrics reflect those objectives?
- How will the metric be used—to evaluate past action on developing the sector CSIRT or to set the stage for future work or next steps of the sector CSIRT?

Asking these questions when developing process metrics enables the development team to adopt metrics that are useful, accurate, and valid. This approach also increases the team's understanding of the process and its outcomes, thereby providing a map for the future.

6.3 Report the Results of Implementation

One optional action that the development team can do as part of sector CSIRT post-implementation is developing a final report that details the results of the implementation. Instead of assessing successes and failures, or needed next steps like the AAR/post-mortem processes, a final report describes the implementation process and is a capstone to the process. This report is generally provided for the record, possibly as part of a legal or administrative requirement.[27] Even though most final reports about the implementation of a sector CSIRT are similar, the following considerations can help ensure that the report targets the desired audience:

- **Public vs. Private Audience.** There can be important changes to the report depending on whether it is for a public (external) or private (internal) audience. For example, sensitive information or operational details are generally limited to a private report. A private report can provide candid insights by highlighting shortcomings or failures. A public report typically accounts for the sensitivities of outside groups or stakeholders who might read the report; sometimes public reports have legal requirements or restrictions, depending on the nature of the report.
- **Stakeholders' Goals and Needs.** A sector CSIRT has many different stakeholders; public agencies (i.e., governments) are frequently involved, and private sector firms and companies are almost always involved (except in government sector CSIRTs). Other stakeholders include future constituents and sector CSIRT implementors, funders, and collaborators (e.g., other CSIRTs). Each stakeholder wants to learn different things from a final report, so it's critical to determine the report's main audience.

[27] This requirement can come from an oversight body, funding body, or the future operators of the sector CSIRT.

Once the development team determines the report's main audience, it can decide what information to include in the report. Typical topics to address in the report include the following:

- development goals met
- operational capability and capacity of the new sector CSIRT
- adopted policies
- organizational and hierarchical standing of the sector CSIRT
- future potential challenges of the sector CSIRT
- information about hardware, software, and other infrastructure for the sector CSIRT
- staffing and funding goals and levels
- organizations that collaborate with the sector CSIRT
- stakeholder concerns

6.4 Plan for the Future

Successfully developing and implementing a sector CSIRT is a complex process that (1) involves many stakeholders and (2) examines a wide range of issues—from outlining how communication and coordination will work to establishing clear, effective policies and procedures. Successfully implementing the steps in the framework is a long, complex process that presents many challenges.

By closely following this framework, the development team can implement a sector CSIRT. What happens after implementation? The answer to that question lies beyond this framework, but the development team should consider that question at the end of the implementation process. The framework, at a minimum, provides questions to consider for future tasks.

As the development team follows the framework, it should document information the sector CSIRT may need in the future. To identify that information, the team should consider the following questions:

- **Will there be another implementation cycle?** If so, capturing lessons learned for the current cycle ensures that mistakes are not repeated and the team can build on its successes.
- **Is there an immediate goal to add capacity/capability in the near future?** Adding capabilities is distinct from the implementation cycle; however, it has many similarities and will benefit from the lessons and data captured during implementation.
- **Does anything else need to be done before the sector CSIRT moves into sustained operations?** There may be tasks or requirements outside of the implementation process that must be addressed before operations begin. Examining the implementation process in detail can help close those gaps.
- **What are the long-term goals for the sector CSIRT?** Long-term, strategic considerations should always be revisited when thinking about growing or expanding the sector CSIRT.

6.4.1 Remain Flexible for Future Growth

A sector CSIRT's ability to adapt to changes in technology, threat mitigation, and effective response affects the team's sustainability and flexibility for future growth. Training is a long-term

investment in the continuity of the team. Cross-training staff members for the same functions lessens the impact of single points of failure, changing trends, and contingencies.

Another factor is work habits over time. Staff members can become resistant to change or updates in established procedures, especially if the team hasn't changed much over time or if individuals share overlapping cybersecurity responsibilities. Complacency can also inhibit growth and long-term sustainability. A sector CSIRT's ability to react to the dynamic environment of incident response is a continuous learning process. Therefore, flexibility and innovation are necessary to deal with changing threats and determine appropriate responses. Sector CSIRTs must also be prepared to react to changing missions, constituents, and stakeholders due to the dynamic nature of cybersecurity and the changing national landscapes and ecosystems.

Policies and procedures must be routinely reviewed and validated to ensure they are still viable, applicable to the changing environment, and followed by staff members. By routinely reviewing existing policies, a team can determine if changes should be made. Often, an organization identifies acceptable time intervals for policy review and/or agrees to review policies as changes are made to the environments where the sector CSIRT is responsible.

7 Conclusion

For over 30 years, the field of cybersecurity has grown and matured significantly. One aspect of this growth and maturation has been the rise of specialization, both in individual skill sets, and team functions and missions. This reality holds true for CSIRTs, which have long been critical parts of the incident response apparatus for organizations, agencies, and governments around the world.

This framework addresses one type of CSIRT specialization—*sector CSIRTs.* These CSIRTs focus on specific CI sectors of a country or economy. Sector CSIRTs have evolved to address the specific risks, threats, and challenges each CI sector faces. They assume a variety of forms (e.g., public or private sector, government-funded or privately funded, information sharing focused or incident response focused).

Since no two sector CSIRTs are alike, the process for developing and implementing one is unique. Regardless, this framework broadly outlines a path for developing a sector CSIRT and successfully integrating it into a national cybersecurity ecosystem.

The framework applies an adaptable, flexible process to assist those seeking to establish a sector CSIRT regardless of how it is funded or what sector it supports. This process-based approach includes the following steps:

- Step 1: Satisfy the Prerequisites
- Step 2: Gather Information
- Step 3: Organize the Information and Evaluate the Gaps
- Step 4: Build a Roadmap
- Step 5: Plan and Implement the Sector CSIRT
- Step 6: Conduct Post-Implementation Activities

The goal of this framework is to (1) assist stakeholders in developing and implementing a sector CSIRT and (2) ensure that the sector CSIRT, once operational, will be effective and sustainable. Accomplishing effectiveness and sustainability requires careful consideration of the sector CSIRT's value, services, constituency, and stakeholders, as outlined in this framework.

The most critical determination the development team must make is how to integrate the sector CSIRT into the national cybersecurity ecosystem. Sector CSIRTs are likely to interact with and be involved in this national ecosystem, and there can be even more critical ties, such as CI or national security concerns. Therefore, how a sector CSIRT integrates with the national cybersecurity ecosystem is a core consideration for any development team, a fact reflected in the framework's emphasis on the national cybersecurity ecosystem integration.

This framework, while extensive, is not meant to be comprehensive. Teams that want to develop and implement a sector CSIRT should also use other guides and tools, including those referenced by the framework. Although some teams might find the framework helpful in implementing other types of CSIRTs, they must recognize that the framework was not developed for that purpose.

There are many other more appropriate resources that address non-sector CSIRTs, including the SEI's *Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 2003].

Incident response and computer security will continue to grow and evolve, as will the role of CSIRTs. The goal of this framework is to contribute to that growth by providing a mechanism that stakeholders can use to develop and implement sector CSIRTs. The framework provides a rich, enduring resource for understanding (1) the purpose of sector CSIRTs, (2) the process for implementing a sector CSIRT, and (3) how sector CSIRTs fit in with other incident response and computer security organizations.

Appendix A: Resources for CSIRT Development

The Software Engineering Institute (SEI), Forum of Incident Response and Security Teams (FIRST), and European Union Agency for Cybersecurity (ENISA) offer guidance to help organizations develop CSIRTs.

Software Engineering Institute

Cybersecurity Center Development (web page)

The SEI's cybersecurity center development team aims to increase the overall U.S. cybersecurity posture by developing, operationalizing, and improving government and industry organizations' incident management capabilities so they can protect themselves from attacks and limit the damage and scope of attacks.
https://www.sei.cmu.edu/our-work/cybersecurity-center-development/index.cfm

Resource Collection for Creating CSIRTs (collection)

To establish a computer security incident response team (CSIRT), it's important to understand what type of CSIRT is needed, the type of services that should be offered, the size of the CSIRT and where it should be located in the organization, how much it will cost to implement and support the CSIRT team, and the initial steps necessary to create the CSIRT. The resources on this page help organizations answer these and other questions.
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485643

Incident Management Capability Assessment (technical report)

Managing incidents that threaten an organization's computer security is a complex undertaking. The capabilities presented in this technical report provide a benchmark of incident management practices.
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538848

Creating a CSIRT (course)

This one-day course is designed for managers and project leaders who have been tasked with implementing a computer security incident response team (CSIRT). This course provides a high-level overview of the key issues and decisions that must be addressed in establishing a CSIRT. As part of the course, attendees will develop an action plan that can be used as a starting point in planning and implementing their CSIRT.
https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P25

Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capacity (report)

In this report, the authors provide insight that interested organizations and governments can use to develop a national incident management capability.
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9221

Handbook for Computer Security Incident Response Teams (CSIRTs) (handbook)

This handbook describes different organizational models for implementing incident handling capabilities. (Although the report was published in 2003, it continues to contain relevant and useful information and can supplement the sector-specific information contained in this sector CSIRT document.)
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

Organizational Models for Computer Security Incident Response Teams (CSIRTs) (report)

This report describes different organizational models for implementing incident handling capabilities, including each model's advantages and disadvantages and the kinds of incident management services that best fit with it. (Although the report was published in 2003, it continues to contain relevant and useful information and can supplement the sector-specific information contained in this sector CSIRT document.)
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6295

FIRST

Establishing a CSIRT (handbook)

This handbook describes the entire process—from start to finish—of how to establish a CSIRT team and how to improve the team as time goes by.
https://www.first.org/resources/guides/#Establishing-a-CSIRT

CSIRT Services Framework (Version 2.1.0) (report)

The Computer Security Incident Response Team (CSIRT) Services Framework is a high-level document that describes, in a structured way, a collection of cybersecurity services and associated functions that CSIRTs and other teams that provide incident management related services may provide.
https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Traffic Light Protocol (TLP): FIRST Standards Definitions and Usage Guidance (web page)

This web page describes the Traffic Light Protocol (TLP), which facilitates information sharing and consists of designations used to ensure that sensitive information is shared appropriately.
https://www.first.org/tlp/

Creating and Managing Computer Security Incident Response Teams (CSIRTs) (tutorial)

This tutorial provides an overview of the issues involved in creating and operating an effective computer security incident response team (CSIRT). Basic topics covered include (1) the purpose and structure of CSIRTs, (2) key steps in designing and implementing a CSIRT, (3) an overview of CSIRT services, and (4) a discussion of best practice incident handling processes.
https://www.first.org/resources/papers/conference2005/robin-ruefle-slides-1.pdf

European Union Agency for Cybersecurity (ENISA)

CSIRT Services Webpage (collection)

This collection of resources helps CSIRTs define their core services according to their available internal resources.
https://www.enisa.europa.eu/topics/csirt-cert-services

Proactive Detection: Good Practices Gap Analysis and Recommendations (report)

This report describes the available methods, tools, activities, and information sources for proactively detecting network security incidents that are used already or that could be used by incident response teams in Europe. This report describes best practices identified, a gap analysis, and recommendations.
https://www.enisa.europa.eu/publications/proactive-detection-good-practices-gap-analysis-recommendations

Proactive Detection: Measures and Information Sources (report)

This report describes the available methods, tools, activities, and information sources for proactively detecting network security incidents that are used already or that could be used by incident response teams in Europe. This report describes best practices identified, a gap analysis, and recommendations.
https://www.enisa.europa.eu/publications/proactive-detection-measures-and-information-sources

Information Sharing and Common Taxonomies between CSIRTs (report)

This report describes ways to enhance cooperation between the Member States (MS) of the European Union (EU) and related Network and Information Security (NIS) communities. This report identifies the information that can be shared between CSIRTs and Law Enforcement Agencies and how this information sharing can be achieved from a technical and organizational perspective.
https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

Roadmap on the Cooperation Between CSIRTS and Law Enforcement (roadmap)

This roadmap, written for the European Union (EU) and European Free Trade Association (EFTA), explores the cooperation across computer security incident response teams (CSIRTs)—in particular with national and governmental law enforcement (LE) and the judiciary (i.e., prosecutors and judges). The roadmap provides information on organizational, legal, technical, and cultural cooperation aspects. It identifies current shortcomings and makes recommendations to enhance cooperation.
https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation

CSIRT Maturity Assessment (web page)

This web page contains recommendations to help CSIRTS improve, mature, and be better prepared to protect their constituencies.
https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

EU Agency for Cybersecurity launches ISAC in a BOX Toolkit (web page)

ENISA developed this comprehensive toolkit, following studies on the ISAC concept, to address the need to facilitate community building and collaboration across ISACs. The toolkit aims at providing practical guidance and the means to empower industry to create new ISACs and to further develop already existing ones.
https://www.enisa.europa.eu/news/enisa-news/isac-in-a-box

Appendix B: Information Gathering Topics and Design

This appendix supplements the material provided in Section 2: Gather Information.

Interview Topics

The following list contains interview topics to consider when gathering information and planning for different interview subject groups.

Cybersecurity Practitioners' Current Understanding

1. What organizations will the CSIRT coordinate with?
2. Do any organizations coordinate sector CSIRT activities?

Role in a Sector CSIRT

What is the sector CSIRT's role in the following areas?

- information sharing
- incident response
- research and development
- tool development

Cybersecurity Capabilities: As-Is and To-Be States

1. For desired end-state capabilities, what is the top priority?
2. Which capabilities are less important to develop?

Role of a National CSIRT in Relation to Sector CSIRTs

1. If there is a national CSIRT, what role will it play in the sector CSIRT?
2. What relationship will the sector CSIRT have with the national CSIRT?
3. When there is not a national CSIRT, how is the sector CSIRT's role impacted in the national cybersecurity ecosystem?
4. Does a sector require incident information to be reported to a national CSIRT?
5. Does a sector require vulnerability or configuration issues to be shared with a national CSIRT?
6. Is information sharing among sectors and national CSIRTs required or encouraged?

Type of Collaborative Network Desired in a Sector CSIRT

What types of collaborative networks (e.g., sector CSIRT, ISAC) have cybersecurity practitioners observed or recommended?

Sector CSIRT Models

1. Public-Private: Will a hybrid model sector CSIRT be used?
2. Government: What government agency will support and/or regulate the sector CSIRT?
3. Non-Profit: How will membership and information be managed?

Services Offered by the Sector CSIRT

1. Has the future constituency of the sector CSIRT identified services that it would like the sector CSIRT to offer?
2. Which services can the sector CSIRT deliver?

Information Sharing Schema and Requirements

1. How will the sector or the sector CSIRT share information? For example, will it have voluntary or mandatory sharing? Will it offer membership models for sharing?
2. Is a particular information sharing schema desired? Is one in use, or is one planned to be implemented in the sector CSIRT?
3. Are there information sharing requirements?
4. Are there membership requirements for sharing information in the sector?

Primary Processes and Technologies Used by a CSIRT

1. What are the existing processes and technologies?
2. What are the desired processes and technologies?

Current Conflicts or Challenges Related to Participating in the National Cybersecurity Ecosystem

1. What recent incidents have most affected the sector?
2. What recently discovered vulnerabilities or configuration issues most affected the sector?

When Collaboration May Not Be Feasible or Desired

Are there any principal collaborators, desired collaborators, entities, or groups with which collaboration might not be possible or desired?

Question Design

The following considerations help the development team create its own list of questions. These considerations apply to informal information gathering, formal written questions, and in-person or virtual/online interviews.

Out of Bounds

What is "out of bounds" for the discussion or interview? For example, should capabilities be discussed? (Keep in mind that this process is different from an assessment; therefore, the questions

should be designed to encourage discussion and emphasize the need to collect helpful information.)

Considering the Audience

1. Are there questions that might lead to disputes or disagreements among the participants?
2. Are the questions appropriate for the variety of audiences? For example, management and technical audiences may be asked different questions. Or they may be asked the same questions with the expectation of getting their different perspectives.

Preparatory Questions

Should any questions be provided to the interview/discussion group beforehand, possibly as a high-level list or a simple collection of talking points? (Providing this information ahead of time creates opportunities for participants to consult with people in other parts of the organization; however, if the responses are canned, honest discussion and feedback might be hindered. Keep in mind that research might be necessary before respondents can answer some questions.)

Scope of Topics

1. What broad questions, research, and discussion topics apply to any sector?
2. Which questions apply only to certain sectors?

The National CSIRT's Role in the Sector

What information must be learned about the national CSIRT's role with the sector, both in the as-is and in the to-be states?

Membership

1. How will membership in the sector CSIRT work?
2. Will membership be required?
3. What are the benefits of membership?
4. Are there potential conflicts or disadvantages for members?

Future Organizational and Operational Factors

1. What does the regulatory setting look like?
2. What is the funding model for the sector CSIRT?
3. Are there regional regulations or treaties that must be considered?

Interview and Information Gathering Design

Interviews are formal discussions between the development team and predetermined stakeholders and/or cybersecurity practitioners. The following interview design considerations are mostly applicable to remote and in-person interviews, but some topics apply to only in-person interviews.

Discussion Format

1. Are the stakeholders familiar with the topic?
2. Will the goals of the discussion need to be reviewed?
3. Will the goals of the process for establishing a sector CSIRT need to be reviewed?
4. How much background about the topic needs to be provided?
5. Are participants familiar with the sector?
6. Are participants familiar with the concepts of cybersecurity, incident response, and CSIRT operations?
7. What should be done to prepare for the discussion?

Venue and Timing

1. How long should each discussion session be?
2. Where should the discussion or interview take place? (Hosting the discussion at a neutral third-party site can be helpful, but this approach may require an on-site facilitator. Hosting the discussion at other locations may lead to biased responses.)
3. Should the interview or discussion be conducted in person? Or is a phone call or virtual/online call sufficient?
4. Are there additional considerations (e.g., time zone differences, platform access and features) for a virtual/online setting?

Discussing the As-Is and To-Be States

Should the discussion focus on one state at a time, or should both states be discussed together?

Data Collection

Should any data collection be conducted? (For example, should responses to questions be weighed? Should votes be counted for particular issues?)

Sharing Questions and Notes

Should questions and discussion notes be shared after the engagement, either for future follow-up discussion or other purposes?

Appendix C: Organizing Information and Documenting Gaps

This appendix is a supplement to Section 3: Organize the Information and Evaluate the Gaps. This guidance provides baseline best practices (or a baseline to-be state) for standing up a sector CSIRT. It can be used to determine how to best identify and close the gaps identified in Section 3.

This section provides more in-depth information about the following topics:

1. Clarify the Sector CSIRT Prerequisites and Gathered Information
2. Choose an Analysis Approach and Techniques for Evaluating Gaps
3. Examine the As-Is and To-Be States
4. Analyze the Gaps
5. Consolidate Gap Information and Determine Priorities

Clarify the Sector CSIRT Prerequisites and Gathered Information

The development team should start with a clear understanding of what the sector CSIRT is designed to accomplish and how it will accomplish it. Providing this clarity for the sector CSIRT is essential and can be addressed by satisfying the prerequisites (Step 1) and gathering necessary information (Step 2). Helping stakeholders, partners, and others understand the sector CSIRT's functions and responsibilities is a critical component of success.

The development team first gathers information about the CSIRT's purpose and other supporting information. This activity includes defining the sector CSIRT's scope and services, and the partners that will serve as the support system for the CSIRT function. The development team should get answers to the following questions to ensure the project starts on the right path:

- What are the sector CSIRT's mission, goals, and scope?
- What are the proposed sector CSIRT's activities, services, and operational functions?
- What special circumstances should be considered? For example,
  - existing legislative/government prohibitions
  - aligning with a national CSIRT and national cybersecurity ecosystem
  - partnering with additional sector CSIRTs
- What is the sector CSIRT's desired capacity level initially and for the next level?
- Have potential mentors, partners, and stakeholders been identified?
  - in the country
  - in the region
  - internationally

Choose an Analysis Approach and Techniques for Evaluating Gaps

To understand the as-is state, the development team must compare the information it gathered with a list of common CSIRT elements. Using the following best practice expectations, the team

can identify where existing information is sufficient and where it must be improved to achieve the to-be state.

- High-level support and approvals
  - description of the approval process and support structure for establishing the CSIRT
- CSIRT Framework, including
  - mission statement
  - description of authority, including links to relevant legislation or policy
  - description of scope and responsibilities
  - description of constituency
  - funding model that shows current and future funding
  - organizational model for the CSIRT team and how/where it fits in with a parent authority
  - description of CSIRT services provided
  - description of staffing needs and a training plan for growing capabilities
  - description of the CSIRT infrastructure and the tools to be used
  - description of existing and desired external relationships
- CSIRT Strategic Plan
  - description of the administration of timelines/deadlines
  - description of the availability or constraints of resources for the project, technical and human (Are there geographic concerns? Are there conflicts with other projects?)
- Communication plan for informing others of the project and progress
- Implementation activities
  - needed resources, including hiring/training staff and purchasing/deploying the infrastructure
- CSIRT functional documentation needs
  - incident handling policy and process
  - information sharing policy and process
  - incident classification policy and process
  - procedures for incident management
    - reporting and logging incident information
    - classifying incidents
    - working an incident—owner and supporting roles
    - analyzing and acting on incidents
    - resolving incidents
    - meeting documentation requirements throughout the incident lifecycle
    - closing and archiving incident information
    - conducting post-incident analysis
  - information security standards for technical resources, including an incident management system and electronic communications
  - baseline MOU for engaging other CSIRTs, organizations, mentors, or partners
  - staff training plan, including conferences or seminars for engaging in the broader CSIRT community

Examine the As-Is State and To-Be States

The development team must identify how the information it gathered correlates with the desired to-be state. To identify gaps between the as-is state and the to-be state, the development team should create a list of each to-be area and identify where information collected about the as-is state is missing or where there is an insufficient level of maturity. For each checklist item, the development team should review the following and add to a gap list similar to the table below.

Gap Analysis Steps			
As-Is State	**To-Be State**	**Identified Gaps and Needs**	**Function/Focus Area**
Step 1: Determine and document the as-is state from the information gathered.	Step 2: Determine and document the desired state.	Step 3: Identify gaps and needs between the as-is and to-be states. These gaps and needs are then prioritized and used to develop the actions/activities of the roadmap. (See Section 4.)	Step 4: Consolidate and prioritize gaps by category or focus area (e.g., governance items like a mission statement or funding, or planned incident management capabilities).

Analyze the Gaps

This section describes a detailed process for reviewing governance, incident management capabilities, communications channels, and the role of the national CSIRT within the sector. The development team uses the considerations listed below when conducting the gap analysis and reviewing the items to be added to the roadmap for implementation.

- **Foundational Items.** Determine if the following foundational aspects of the CSIRT are established, documented, and agreed on at the highest level possible.
  - description of authority
  - mission statement
  - funding model
  - organizational model
- **Legislative or Policy Documents**. Determine if these documents are defined and supported. Evaluate the information gathered to determine if the following have been clearly documented, approved by the appropriate level, and published to reach the applicable parties.
  - list of sectors and/or CI areas
  - definition of the sector CSIRT's formation and mission
  - if the sector CSIRT has been authorized and there is an agreement for its independence (The sector CSIRT should operate independently of industry businesses within the sector to maintain autonomy and act equitably for all sector members.)
  - clear scope and list of constituencies
  - agreements (e.g., policy/procedure/memorandum of understanding) between organizations that cover sector CSIRT interactions with other CSIRTs

- sector member agreements to their financial commitment, including ongoing, documented budget and resource line items

- **National CSIRT Working Relationship.** Ensure that the sector CSIRT has an established relationship with the national CSIRT. A national CSIRT can assist with establishing the sector CSIRT and providing valuable information sharing functions. The sector CSIRT should have an agreement with the national CSIRT and an understanding of the responsibilities divided and shared between the two.
  - recognition (accredited/authorized) of the sector CSIRT by the national CSIRT, if applicable
  - information sharing agreements
  - understanding of the national CSIRT's responsibilities and pledge to participate in national activities as needed
  - clearly defined role of the national CSIRT from the sector CSIRT's perspective, including the following:
    - Responsibilities are understood and defined in legislation.
    - The mission is supported in the National Cybersecurity Strategy.
    - Sector or cross-sector CSIRT information sharing is enabled and facilitated.

- **Incident Management Plan.** Ensure that an incident management plan exists. Examine existing processes and documentation regarding incident identification, detection, response, management, and communications among CSIRTs.
  - existing documents within the sector CSIRT
    - For each document listed, determine its state and the steps required to reach the desired level of maturity in the to-be state.
  - external agreements in place with other CSIRTs
    - Common practices are documented across sectors to establish agreed-on incident information and handling.
    - MOUs are established for information sharing and other working practices between CSIRT teams.
    - Relationships are established, including informal or verbal working agreements with other teams.
  - defined and documented sector CSIRT mission that describes its
    - services offered
    - constituency
    - funding model
    - organizational structure
    - staffing and training plan
  - Information captured from incidents, including the incident
    - owner (individual leading the response activity)
    - status (over time)
    - information reported and ongoing updates
    - audit log of changes
    - reporting (for individual incidents) and trending over time for the incident management process

    - analysis from the incident handler/owner
    - lessons learned (gathered after action on the incident, when it is closed)
  - Defined incident tracking process that includes
    - data elements to be tracked
    - incident taxonomy used to classify/categorize incidents
    - incident reporting criteria for incoming reports and notifications to others when needed
    - report standardization with other organizations to support information sharing
  - Information sharing agreements and processes, including the following:
    - Common classification definitions are established between organizations.
    - Information protection guidelines have been agreed on.
    - Technical data protection controls have been defined to support electronic communications/information sharing.

- **Communication Channels.** Ensure that communication channels have been established/documented internally and with external partners. Communication plans should identify key contact information (e.g., email addresses, phone numbers, and names).
  - within sector participant organizations for
    - communication between peer organization's CSIRT teams
    - sector-wide notifications
    - communication between peer organization's leaders
    - communication with the national CSIRT
  - for information sharing among teams, which involves including or establishing
    - trust or reciprocation of trust between CSIRT teams
    - a willingness to share applicable information regarding incidents with other organizations, including potential competitors
    - agreements to share applicable incident information
    - mechanisms that enable sharing incident information
    - criteria for sharing incident information for public awareness
  - with other CSIRTs
    - CSIRTs in different sectors
    - regional or global CSIRT organizations
    - the country's national CSIRT
    - for public awareness, if needed

Consolidate Gap Information and Determine Priorities

It is useful to consolidate gap information about similar items and group items that will likely use the same resources. For example, the same individual(s) will likely address the lack of a documented scope and goals. Grouping items also helps the development team prioritize each gap area.

Adding a priority column to the gaps list is recommended. Priorities can be documented using a simple three-part scale (e.g., high/medium/low) or a more granular rating scale (e.g., 1-5). The result is a list of gaps that can be viewed by priority to help the development team as it documents the roadmap.

Table 4 lists examples of ways to group gap information.

Table 4: Example Grouping Strategies for Organizing Gap Information

National Legislative Landscape	• Legislative or policy documents • Sectors and CI definitions • Sector governance, authorizations, and support • Role of the national CSIRT recognized by the sector CSIRT • Working guidelines/agreements with the national CSIRT

Sector CSIRT Processes and Documentation	• Internal to the sector CSIRT
	  • Mission and definitions (e.g., goals, services, constituents, organizational structure, funding, staffing, training)
	  • Incident management system (e.g., required data, intake, reporting/trending, escalation)
	  • Incident handling processes (e.g., escalation internally and when to share externally)
	  • Technical controls for data protection (e.g., logically and physically)
	  • Education of staff
	• External with other CSIRTs
	  • Agreement on an incident taxonomy and information sharing mechanism
	  • Integration of incident data feeds from other organizations
	  • Documented information sharing agreement
	  • Technical controls for information sharing (e.g., encryption, channels)
	  • Public awareness process

Communications Needs	• Communications within the sector • MOUs for information sharing • Agreed-to information sharing guidelines (e.g., classifications, protection, required controls, handling) • Communications with others (e.g., national CSIRT, other sectors, international CSIRT organizations) • Public awareness

Appendix D: *FIRST CSIRT Services Framework* Summary

The *FIRST CSIRT Services Framework* describes services and functions of incident response teams within a high-level framework to assist in community-wide standardization and the selection and establishment of a team's services portfolio [FIRST 2019]. Teams are not expected to provide all services; services should be selected based on the CSIRT's mission, constituents, resources, and capacity. As a best practice, CSIRTs should choose a select few services and begin performing them well before expanding their services.

The structure of the framework is based on four elements: service areas, services, functions, and sub-functions. When implementing a sector CSIRT, refer to the *FIRST CSIRT Services Framework* to assist with setting organizational goals, understanding desired outcomes, and planning implementation.

The following information is summarized from the *FIRST CSIRT Services Framework* [FIRST 2019]. Appendix E provides follow-on implementation considerations for each of these service areas.

Information Security Event Management Service Area

The objective of the Information Security Event Management service area is to identify information security incidents based on security events analysis and data correlation. These sources can include information collected from trusted stakeholders, members, and teams, including the national CSIRT. Services included within the Information Security Event Management service area include monitoring, and detection and event analysis.

In some organizations, this service area is the responsibility of the Security Operations Center (SOC) or a different cybersecurity operations capability. This service area depends on trustworthy and accurate data regarding information security events; therefore, if applicable, effective interaction between the SOC and CSIRT are essential. Throughout the incident management process, the CSIRT may involve other teams as needed.

Information Security Incident Management Service Area

The Information Security Incident Management service area is at the core of any CSIRT; these services are critical to assisting constituents during an incident. Because of the unique role the CSIRT plays, it is able to collect and evaluate information security reports from different sources, while also analyzing relevant data and performing in-depth analysis of the incident and artifacts related to the incident.

Once the CSIRT conducts the analysis of information collected, it can recommend mitigation and recovery steps to its constituents. The CSIRT may support constituents in applying the provided recommendations. If necessary, the CSIRT may also coordinate with external entities (e.g., peer CSIRTs, the national CSIRT, SMEs, or vendors) to address all aspects of the incident and reduce the attack surface for future attacks. Service offerings in this service area include incident report

acceptance, incident analysis, forensic evidence analysis, mitigation and recovery, incident coordination, and crisis management support.

Vulnerability Management Service Area

The Vulnerability Management service area includes services and functions related to the discovery, analysis, and handling of security vulnerabilities in information systems. This service area includes services related to both new *and* known vulnerabilities. A sector CSIRT may choose to share information about vulnerabilities that were discovered within its sector, which, in turn, assists the sector in protecting its cyber footprint and awareness of cyber threats and vulnerabilities. A CSIRT may focus its services on Vulnerability Discovery/Research and Vulnerability Report Intake, then issue advisories to its constituents when needed, without necessarily participating in any vulnerability coordination or response efforts.

Situational Awareness Service Area

The Situational Awareness service area focuses on identifying, processing, understanding, and communicating the integral components of what is happening in and around the CSIRT's scope of responsibilities, which can affect how the CSIRT operates under normal conditions. Situational awareness is the comprehension of the current state and the ability to identify changes to that normal or baseline state. This service area's services include (1) gathering information, (2) analyzing that information for internal awareness, and (3) quickly distributing relevant information to constituents so that they can make appropriate decisions. Sector CSIRTs often focus on data collection and dissemination; the data from situational awareness services may integrate with the national CSIRT, other trusted CSIRTs, and/or third-party service providers. Sector CSIRTs help every team align in regards to who knows what, and what is happening across the sector. Services in the Situational Awareness service area include data acquisition, analysis and synthesis, and communication.

Knowledge Transfer Service Area

CSIRTs are in a unique position to collect relevant data; conduct analysis; and identify threats, trends, and best practices to help organizations prevent and respond to security incidents. By transferring this knowledge to their constituencies and trusted partners, CSIRTs can improve cybersecurity overall. The Knowledge Transfer service area includes activities such as building awareness, conducting training and education, developing cybersecurity exercises, and creating technical and policy advisories.

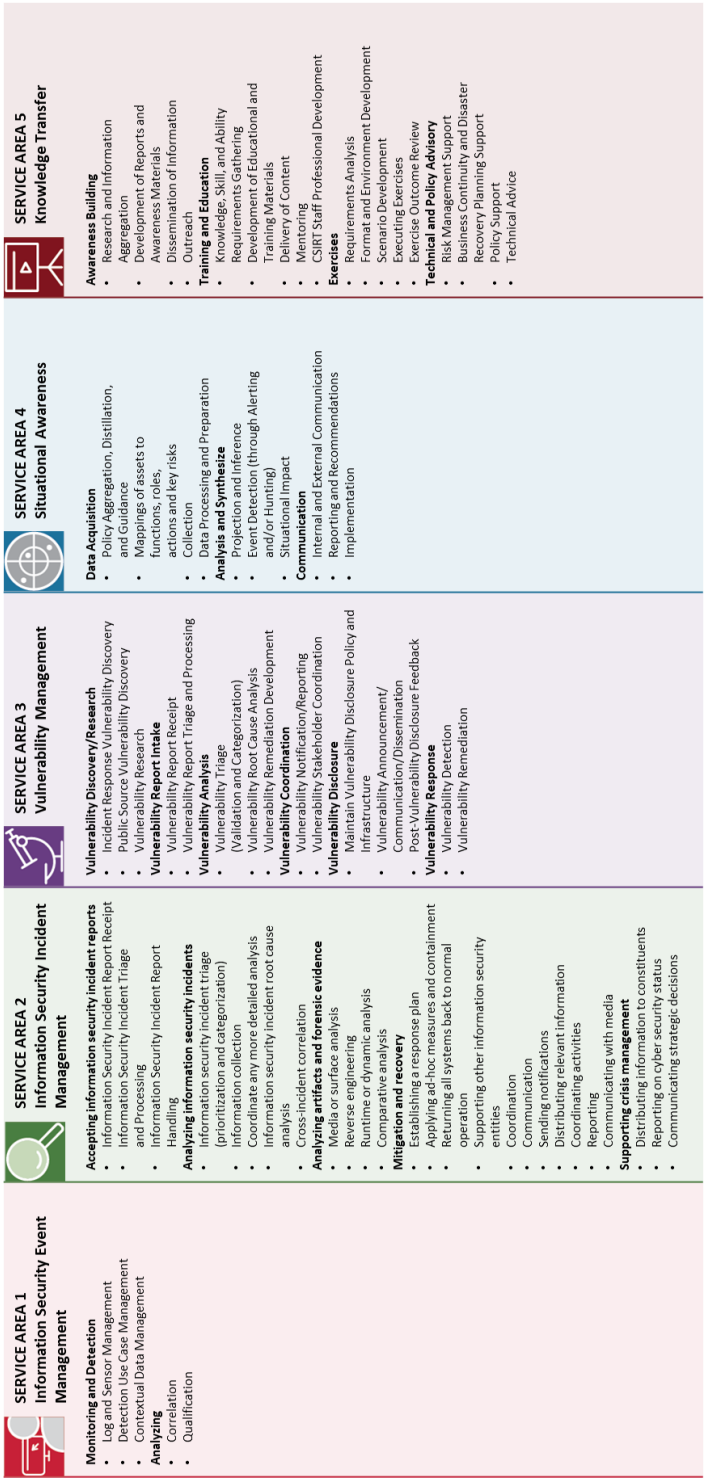

Figure 11: CSIRT Services Framework Service Areas, Services, and Functions

Appendix E: CSIRT Services Implementation Considerations

This appendix provides specific implementation considerations associated with each of the five CSIRT Service Areas outlined in the FIRST *CSIRT Services Framework*, including descriptions of minimum required tasks and general knowledge for particular service areas.[28]

This appendix can be used in conjunction with Appendix D to ensure that a sector CSIRT is able to fully provide any services selected. While Appendix D provides brief summaries of each service area, this appendix outlines what the development team (and subsequently any team operating the sector CSIRT) must do and know to offer these services.

Information Security Event Management

Sector CSIRTs that plan to offer Information Security Event Management services must consider the following topics when determining their ability to offer a current (or future) capability and should meet a minimum standard of knowledge and ability in these areas.

Constituency Operations

The constituency should be informed of the sector CSIRT's processes for identifying events and incidents, and its associated incident categorization processes. Familiarity with a sector CSIRT's incident management process and how to share information ensures the constituency can provide event information to the sector CSIRT for analysis and coordination. The development team should build its familiarity with the following topics:

- information sharing frameworks and standards in the incident management community
- monitoring capabilities and threats common across the constituency
- identifying anomalous information security events and incident categorization schemes
- information sharing systems and incident reporting policies and procedures

Incident Management Technical Components

Sector CSIRTs should be familiar with common incident management and information sharing standards used for communicating incident information in information sharing communities. Sector CSIRTs should be familiar with the following:

- Common information sharing frameworks/standards (e.g., definitions and identification of events, data used for incident categorization, and identifying and sharing incidents within the sector and the greater CSIRT community)
- Community information sharing data feeds (e.g., systems that can notify and provide information regarding events and incidents that CSIRTs outside the sector are experiencing)

[28] The summaries of each service area do not include descriptions of general networking concepts (e.g., DNS, routing, protocols), general system administration concepts (e.g., configuration management and account management), or general information security concepts (e.g., encryption and log management).

- Event/incident management system (e.g., system for collecting event and incident reporting from constituents, communicating within constituents, collecting data for individual events, and collecting event/incident metrics for reporting purposes)

Incident Management Community

Sector CSIRTs should establish one or more relationships within the broader CSIRT information sharing community. These relationships are sources of incidents affecting others and can be early-warning indicators that assist preparations within the sector. Other CSIRTs may also provide mentoring or advice to the sector CSIRT to help with incidents experienced within the constituency. Sector CSIRTs should be familiar with the following:

- Global incident management community organizations (e.g., information categorizations and labelling, information sharing protocols, information sharing technical requirements)
- Establishing goals and objectives for information sharing within the constituency
- Establishing technical requirements for information sharing within the constituency

Information Security Incident Management

Sector CSIRTs planning to offer Information Security Incident Management services must consider the following topics when determining their ability to offer a current (or future) capability and should meet a minimum standard of knowledge and ability in these areas.

Constituent Operations

Sector CSIRTs should be familiar with, or have a basic understanding of, their constituency's ability to collect, compile, and transmit system and network information related to specific timeframes or incidents. Sector CSIRTs should be familiar with the following knowledge areas:

- existing system and network logging capabilities across their constituency
- incident management transmission mediums (e.g., information sharing portals, email, automated incident intake formats, telephony, and others)

Technical Components

Sector CSIRTs should be familiar with basic information that describes their constituent's current information security posture and the details of an incident provided.

Incident Triage

Sector CSIRTs must be able to review and prioritize incoming constituent incidents. Baseline ability for this task does not require this process to be formalized, but a sector CSIRT should be capable of explaining an informal triage process to developers. Specific knowledge required to perform incident triage includes the following:

- constituent mission (i.e., understanding a constituent's mission to a degree a sector CSIRT can prioritize incidents)
- consistent assets (i.e., understanding a constituent's assets and their relative importance)

Incident Analysis

Sector CSIRTs must be able to perform analytical tasks, leading to the creation or discovery of information that allows constituents to mitigate or remediate incidents.

Incident Mitigation and Remediation

Sector CSIRTs must be able to perform at least one of the following tasks:

- mitigate incidents on behalf of their constituents
- present information to constituents that allows them to mitigate incidents
- remediate incidents on behalf of their constituents
- present information to constituents that allows them to remediate incidents

Vulnerability Management

Sector CSIRTs planning to offer Vulnerability Management services must consider the following topics when determining their ability to offer a current (or future) capability, and should meet a minimum standard of knowledge and ability in these areas.

Constituency Operations

Familiarity with a sector CSIRT's constituency ensures a sector CSIRT can provide effective Vulnerability Management services. Sector CSIRTs should ensure familiarity with the following knowledge areas:

- operating system deployment that is common across a constituency
- network appliances and architectures common across a constituency
- common administrator privileges, tools, or other administrator utilities common across a constituency

Vulnerability Technical Components

Sector CSIRTs should be familiar with the technical languages that describe vulnerabilities. Sector CSIRTs should be familiar with the following terms:

- Common Vulnerability and Exposure (CVE) – enumerating vulnerabilities and providing a common identifier for the CSIRT community
- Common Vulnerability Scoring System (CVSS) – system for describing the severity of a particular vulnerability

Mitigation Creation and/or Application

All of the following mitigation activities should be a capability for a sector CSIRT performing vulnerability management:

- Mitigation Creation – using knowledge of existing vulnerabilities and a constituent's information technology architecture to create a technical or process mitigation for a vulnerability
- Mitigation Packaging – using existing mitigation techniques or technologies to alter mitigations into formats usable by a CSIRT's constituency

- Mitigation Distribution – delivering mitigation techniques or technology to a CSIRT's constituency

Patch Management

All of the following patch-management tasks should be within the capabilities of a CSIRT performing vulnerability management. Patch creation was excluded from this list because it requires specific knowledge of particular applications or configurations. It is normal for CSIRTs to package and distribute patches without input into the patch's development.

- Patch Packaging – modifying patch format and instructions into types usable by constituent CSIRTs
- Patch Distribution – transmitting patch files to constituents with known instructions for deployment

Situational Awareness

Sector CSIRTs must maintain an understanding of how the constituency operates under normal circumstances and be able to identify abnormal operational changes. Situational awareness also means keeping current with what is happening in the greater CSIRT community so that relevant information can be passed along to the constituency. Situational awareness services require knowledge of the following topics.

Constituency Operations

Sector CSIRTs should be familiar with, or have a basic understanding of, their constituency's baseline operating environments. Familiarity with a sector CSIRT's constituency ensures the sector CSIRT can provide effective situational awareness when needed. Sector CSIRTs should be familiar with the following topics:

- baseline operating environments and monitoring capabilities across the constituency
- threats and known vulnerabilities across the constituency
- identification activities in the constituency that are outside normal operations
- ongoing threats present in the global community that may affect the constituency

Situational Awareness Technical Components

Sector CSIRTs should be familiar with the technical baselines in the constituency and how to distribute relevant information to the constituency or to the global CSIRT community. Sector CSIRTs should be familiar with the following:

- Monitoring and metrics within the constituency – systems and tools used, what constitutes normal baseline activity, and metrics that are indicators of abnormal activities
- Event correlation – looking across the constituency for common issues that may be caused by the same source or threat
- Data and knowledge management – maintaining event/incident data and threat information in the appropriate systems to build awareness of historical activities and inform present events, ensuring lessons learned are documented and applied where appropriate

- Developing security intelligence – using community reports, threat activities, and event/incident management information to curate intelligence that is relevant to the constituency, using intelligence to support preparation activities within the constituency, and sharing sector intelligence with information sharing partners as needed

Knowledge Transfer

Sector CSIRTs planning to offer Knowledge Transfer services must consider the following topics when determining their ability to offer a current (or future) capability and should meet a minimum standard of knowledge and ability in these areas.

Constituent Operations

Sector CSIRTs must have known communication channels that are open and maintained with their constituency. Constituencies must be informed of knowledge transfer activities a sector CSIRT undertakes and provide regular updates to the constituency. Although this process is not required to be formalized, ideally it should be.

Technical Components

Technical components of a sector CSIRT knowledge sharing program consist of the following:

- Transmission medium – This category is necessarily broad and includes mediums like email, telephone service, and information sharing portals. It is critical that transmission mediums are known to constituents and used when known criteria are met.
- Content – Sector CSIRTs must distribute a subset of training and education materials, awareness building materials, exercises, and advisories describing technical or policy issues to their constituencies.

A sector CSIRT must maintain a record of the following:

- Knowledge transfer activities offered – This information should be available in a format suitable to share with constituents.
- Eligibility requirements for participation in knowledge transfer activities – This information should be available in a format suitable to share with constituents.

References

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

[CISA 2020]
Cybersecurity and Information Security Agency (CISA). *Critical Infrastructure Sectors*. December 2020 [accessed]. https://www.cisa.gov/critical-infrastructure-sectors

[Collier 1996]
Collier, Bonnie; DeMarco, Tom; & Fearey, Peter. A Defined Process for Project Postmortem Review. *IEEE Software*. Volume 13. Number 4. July 1996. https://dl.acm.org/doi/10.1109/52.526833

[Dorofee 2005]
Dorofee, Audrey; Mundie, David; & Ruefle, Robin. *Creating and Managing Computer Security Incident Response Teams (CSIRTs)*. Software Engineering Institute, Carnegie Mellon University. 2005. https://www.first.org/resources/papers/conference2005/robin-ruefle-slides-1.pdf

[Dorofee 2018]
Dorofee, Audrey J.; Ruefle, Robin; Zajicek, Mark; McIntire, David; Perl, Samuel J.; Alberts, Christopher J.; Huth, Carly L.; & Walters, Pennie. *Incident Management Capability Assessment.* CMU/SEI-2018-TR-007. Software Engineering Institute, Carnegie Mellon University. 2018. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538848

[ENISA 2016]
European Union Agency for Cybersecurity (ENISA). *Information Sharing and Common Taxonomies Between CSIRTs and Law Enforcement*. December 2016. https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

[ENISA 2019]
European Union Agency for Cybersecurity (ENISA). *Roadmap on the Cooperation Between CSIRTS and Law Enforcement.* December 2019. https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation

[ENISA 2020a]
European Union Agency for Cybersecurity (ENISA). *CSIRT Maturity Assessment.* December 2020 [accessed]. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

[ENISA 2020b]
CSIRT Services. *European Union Agency for Cybersecurity (ENISA) Website*. December 2020 [accessed]. https://www.enisa.europa.eu/topics/csirt-cert-services

[ENISA 2020c]
European Union Agency for Cybersecurity (ENISA). *Proactive Detection: Good Practices Gap Analysis and Recommendations*. ENISA. May 2020. https://www.enisa.europa.eu/publications/proactive-detection-good-practices-gap-analysis-recommendations

[ENISA 2020d]
European Union Agency for Cybersecurity (ENISA). *Proactive Detection: Measures and Information Sources*. ENISA May 2020. https://www.enisa.europa.eu/publications/proactive-detection-good-practices-gap-analysis-recommendations

[FIRST 2019]
Forum of Incident Response and Security Teams (FIRST). *Computer Security Incident Response Team (CSIRT) Services Framework (Version 2.1.0)*. November 2019. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

[FIRST 2020a]
Forum of Incident Response and Security Teams (FIRST). *FIRST: Improving Security Together Website*. December 2020 [accessed]. https://www.first.org/members/teams/

[FIRST 2020b]
FIRST. *Traffic Light Protocol (TLP): FIRST Standards Definitions and Usage Guidance*. December 2020 [accessed]. https://www.first.org/tlp/

[Haller 2010]
Haller, John; Merrell, Samuel A.; Butkovic, Matthew J.; & Willke, Bradford J. *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability*. CMU/SEI-2010-SR-009. Software Engineering Institute, Carnegie Mellon University. 2010. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9221

[IDA 1999]
Institute for Defense Analyses (IDA). *Foundations of the After Action Review Process*. Institute for Defense Analyses. July 1999. https://apps.dtic.mil/docs/citations/ADA368651

[InfraGard 2020]
InfraGard: Partnership for Protection. December 2020 [accessed]. https://www.infragard.org/

[Killcrece 2003]
Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. *Organizational Models for Computer Security Incident Response Teams (CSIRTs)*. CMU/SEI-2003-HB-001. Software Engineering Institute, Carnegie Mellon University. December 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6295

[OJEU 2016]
Official Journal of the European Union. *NIS Directive (Annex II)*. 32016L1148. July 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L: 2016:194:TOC

[Parry 2001]
Parry, Charles & Darling, Marilyn. Emergent Learning in Action: The After Action Review. *The Systems Thinker*. October 2001. https://thesystemsthinker.com/emergent-learning-in-action-the-after-action-review/

[SEI 2020a]
Creating a Computer Security Incident Response Team. SEI Course. *Software Engineering Institute Website*. December 2020 [accessed]. https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P25

[SEI 2020b]
Cybersecurity Center Development. *Software Engineering Institute Website*. SEI Web Page. December 2020 [accessed]. https://www.sei.cmu.edu/our-work/cybersecurity-center-development/index.cfm

[SEI 2020c]
Resources for Creating a CSIRT. *Software Engineering Institute Website*. SEI Collection. December 2020 [accessed]. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485643

[Stikvoort 2019]
Stikvoort, Don. *SIM3 Security Incident Management Maturity Model.* May 2019. https://opencsirt.org/csirt-maturity/sim3-and-references/

[van der Heide 2017]
Van der Heide, Martijn. *Establishing a CSIRT*. ThaiCERT. November 2017. https://www.first.org/resources/guides/#Establishing-a-CSIRT

[West-Brown 2003]
West-Brown, Moira; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. CMU/SEI-2003-HB-002. Software Engineering Institute, Carnegie Mellon University. 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

[Zeltser 2008]
Zeltser, Lenny. SWOT matrix for describing security posture. *SANS ISC InfoSec Forums.* 2008. https://isc.sans.edu/forums/diary/SWOT+matrix+for+describing+security+posture/4939/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	February 2021	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities	FA8702-15-D-0002

6. AUTHOR(S)

Justin Novak, Brittany Manley, David Mcintire, Sharon Mudd, Angel Hueca, & Tracy Bills

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2021-TR-002

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

The U.S. Department of State, Office of the Coordinator for Cyber Issues commissioned the Software Engineering Institute (SEI) to create the Sector CSIRT Framework for (1) developing a sector-based computer security incident response and coordination capability and (2) integrating this capability into a larger national cybersecurity ecosystem as applicable. The framework is a guide for helping interested parties develop the policies, processes, and procedures necessary to operationalize a sector Computer Security Incident Response Team (CSIRT), a uniquely adapted, specialized incident response team. The framework outlines a process that moves the sector CSIRT from concept to reality. The framework helps the team developing the sector CSIRT understand the current conditions of incident response in the sector (i.e., the as-is state) and how to move it to a robust operating state (i.e., the to-be state). It bridges the gap between these two states using a well-defined roadmap and implementation process.

The Sector CSIRT Framework is intended for individuals and organizations—including CSIRT managers, national CSIRTs, and others—who are developing or implementing a sector CSIRT. Using this framework, these individuals or organizations can move a sector CSIRT from a concept to the reality of a fully operational team.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Computer Security Incident Response Team, CSIRT, framework, national CSIRTs	83

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL