Carnegie Mellon University
Software Engineering Institute

Improving Sector Based Incident Response

A New Framework for Developing Sector CSIRTs and Integrating with National Cybersecurity Ecosystems

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

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

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

DM22-0479

Agenda

- **Challenge(s): Defining and Defending Sectors**
- **Existing Approach: Building CSIRTs**
- **A New Perspective: The National Ecosystem**
- **The Sector CSIRTs Framework: Application and Case Study**

Introduction – The Security Operations Team

The Security Operations (SecOps) Team within CERT helps security operations and cybersecurity centers develop, operationalize, and improve their incident management capabilities to prevent and mitigate cybersecurity threats.

- SecOps supports the following activities:
  - implementing and improving sustainable incident response capabilities with teams around the world
  - enhancing state-of-the-art techniques and practices in the cyber threat information-sharing field and applying this knowledge in a regional setting to promote trust-based incident response communities
  - developing the global cybersecurity workforce through tailored capacity building and mentoring

Infrastructure, Critical Infrastructure, and Sectors

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.

Challenges:

- Sectors can be segmented, fragmented, complex and diverse IT landscapes,
- Range of maturity levels
- <u>Some Sectors may not be designated as ‘critical’</u>!

How to provide Sector Specific IR/IM Capabilities?

Trends in Incident Response follow those of the information economy:

- Rapid expansion of the Internet into every facet of modern life and the digital economy has led to increased use of technology, which has also become more pervasive and specialized.
- In turn, CSIRTs have also grown and become more specialized. An emerging trend of this increased specialization is the adoption of sector CSIRTs

Why Sector CSIRTs?

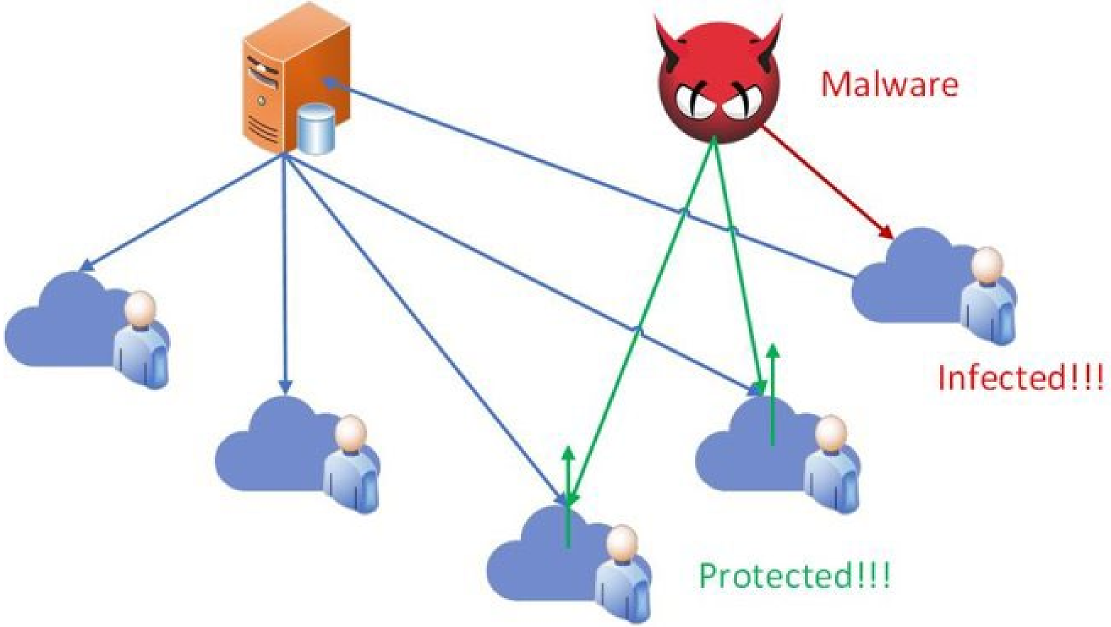
Definition: A sector CSIRT is a body that is responsible for incident response and management for a subset of a country or economy. In rare cases, a sector CSIRT may be transnational in nature. One (of many) key advantages is that sector CSIRTs provide a mechanism or platform for sharing information and building trust.

What a Sector CSIRT *actually* does:

- communicating and coordinating among members of the sector as well as with the national CSIRT and other stakeholders
- disseminating information prior to and following incidents
- convening meetings and the discussion of stakeholders
- providing or leading training
- ensuring trust and confidentiality among members

Why Sector CSIRTs?

Main Benefit – Shared Risk/Risk Avoidance



Other advantages

- **Scalability**. 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 critical infrastructure sector incidents can require specialized knowledge and skills. A sector CSIRT can maintain subject matter expertise for its sector’s needs.

Terminology

Terminology may vary:

The term sector CSIRT broadly refers to any organization that is responsible for incident response and management for a subset of a country or economy.

However, some entities use other terms including:

- Sectoral CSIRTs
- Sector-based Cybersecurity Centers
- Sector CERTs (Computer Emergency Response Teams)
- Information Sharing and Analysis Centers (ISACs).

Regardless of the terminology used or the prioritization of CI within a country or economy, our focus is on sector-based incident response capabilities

Building Sector CSIRTs

We know about building CSIRTs:

- SEI Handbook for Computer Security Incident Response Teams (CSIRTs)
- FIRST Establishing a CSIRT Handbook
- SIM3
- Etc.

We know about building industry capabilities:

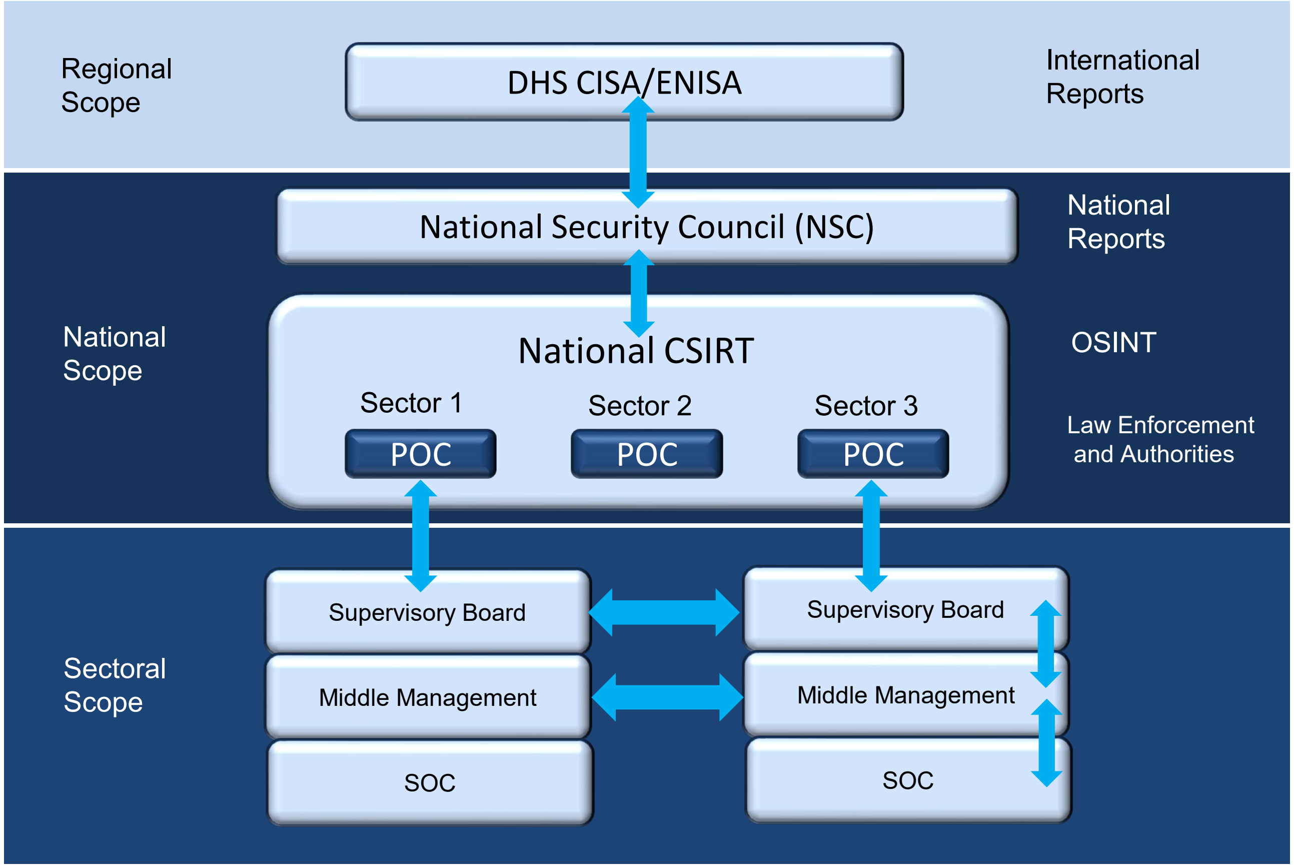
- ENISA ISAC in a box
- PSIRTs
- Etc.

But we don’t know much about sector CSIRTs specifically

Existing models of CSIRT development do not address Sector-Specific needs

Back to the beginning…

Interaction can occur at many levels – between National, Regional, Sectoral and individual organizations



…Leads to a New Approach

These levels of interaction constitute a **National Cybersecurity Ecosystem**, within which any sector-based capability must operate

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)

- SEI Sector CSIRTs Framework

Understand 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 Role of the national CSIRT
- Establishing Trust
- Roles and Responsibilities
- Communication
- Information Sharing

Integrating with the National Cybersecurity Ecosystem

Integration into the national cybersecurity ecosystem is essential. However, when implementing a sector CSIRT, there is a need to continually revisit the ecosystem and how the sector CSIRT will integrate. Key questions include:

- 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 there is no national CSIRT, how does this impact 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?

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

To facilitate the development of sector CSIRTs and related capabilities, the SEI developed the sector CSIRT Framework to:

1. Help teams develop sector-based computer security incident response and coordination capabilities, and
2. Assist with integrating those capabilities into larger national cybersecurity ecosystems as applicable.

The framework is a guide for helping interested parties develop the policies, processes, and procedures necessary to operationalize a sector CSIRT, and outlines a process that moves the sector CSIRT from concept to reality.

Using the Sector CSIRT Framework to Build a new Sector Team/Capability…

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

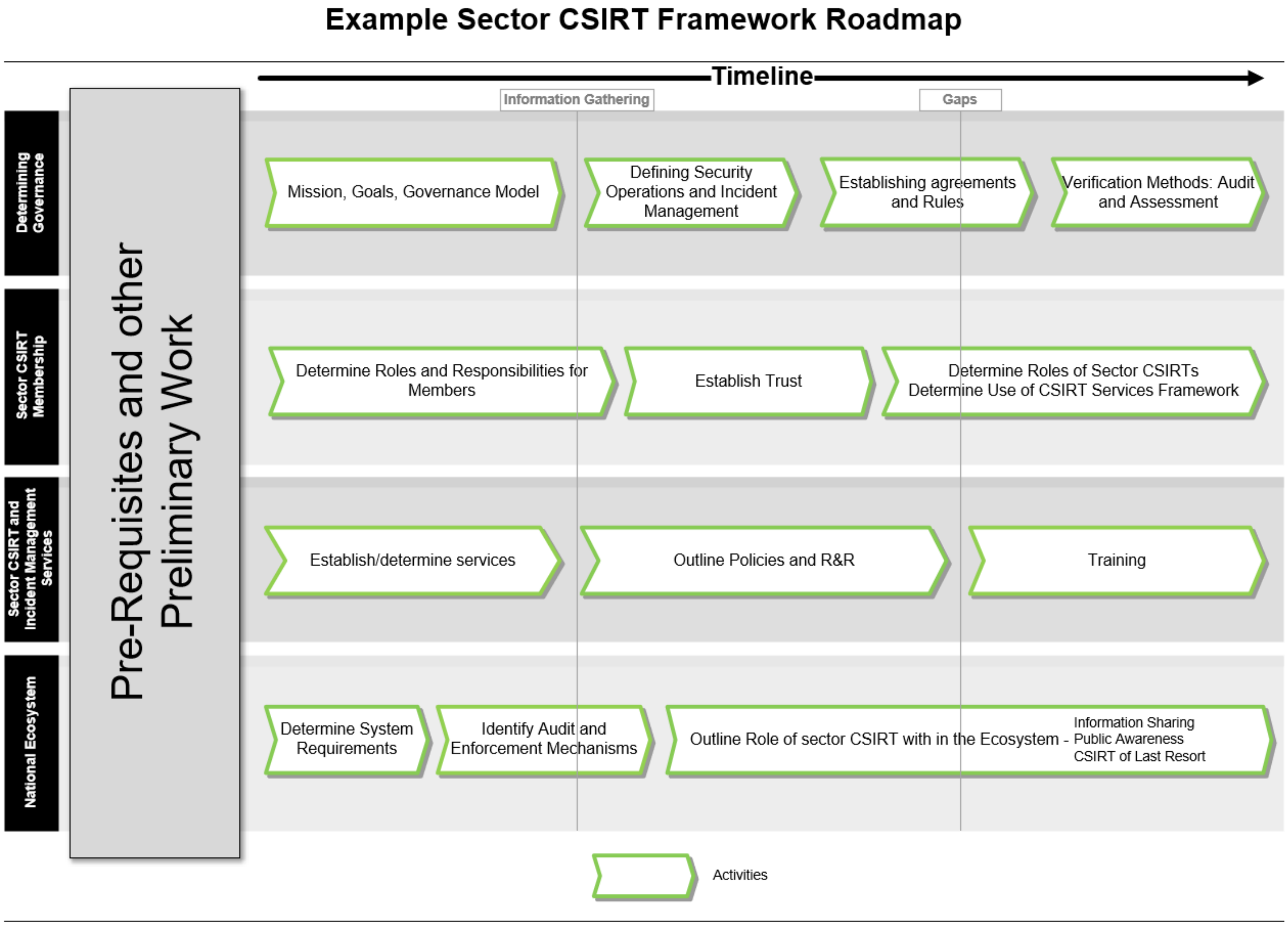
Step 6: Conduct Post-Implementation Activities

As - Is
STEP 1
STEP 2
STEP 3
STEP 4
STEP 5
STEP 6
To - Be

…within the National Cybersecurity Ecosystem

Framework Step	Core Task	National Cybersecurity Ecosystem (NCE) Considerations
Step 1: Satisfy the Prerequisites	Ensure that the foundational elements are in place for the sector CSIRT development, and begin to identify the sector, stakeholders, and environment	Defining the sector, addressing legal authorities and legislative requirements
Step 2: Gather Information	Outline what information is needed and how to acquire the information, including from whom and in what setting	Understanding sector specific requirements, identifying stakeholders across the NCE
Step 3: Organize the Information and Evaluate the Gaps	Sort, categorize, and prioritize the information, and work to understand what the information says and does not say	How will changes affect stakeholders across the NCE, what does the NCE look like in as-is and to-be states
Step 4: Build a Roadmap	Develop a plan to move the sector CSIRT development from an as-is state to a to-be state using clearly outlined criteria	What NCE input is needed, what assistance is available, what impacts will be felt
Step 5: Plan and Implement the Sector CSIRT	Select services, implement the plan outlined in the roadmap, and establish an operational capability aligned with the national cybersecurity ecosystem as needed	Deconfliction of service offerings, establishment of communication and coordination mechanisms, clarification of roles across NCE
Step 6: Conduct Post-Implementation Activities	Use metrics to assess impact and progress, and outline future steps and growth	How did implementation affect NCE, what problems were solved, and which new challenges have emerged

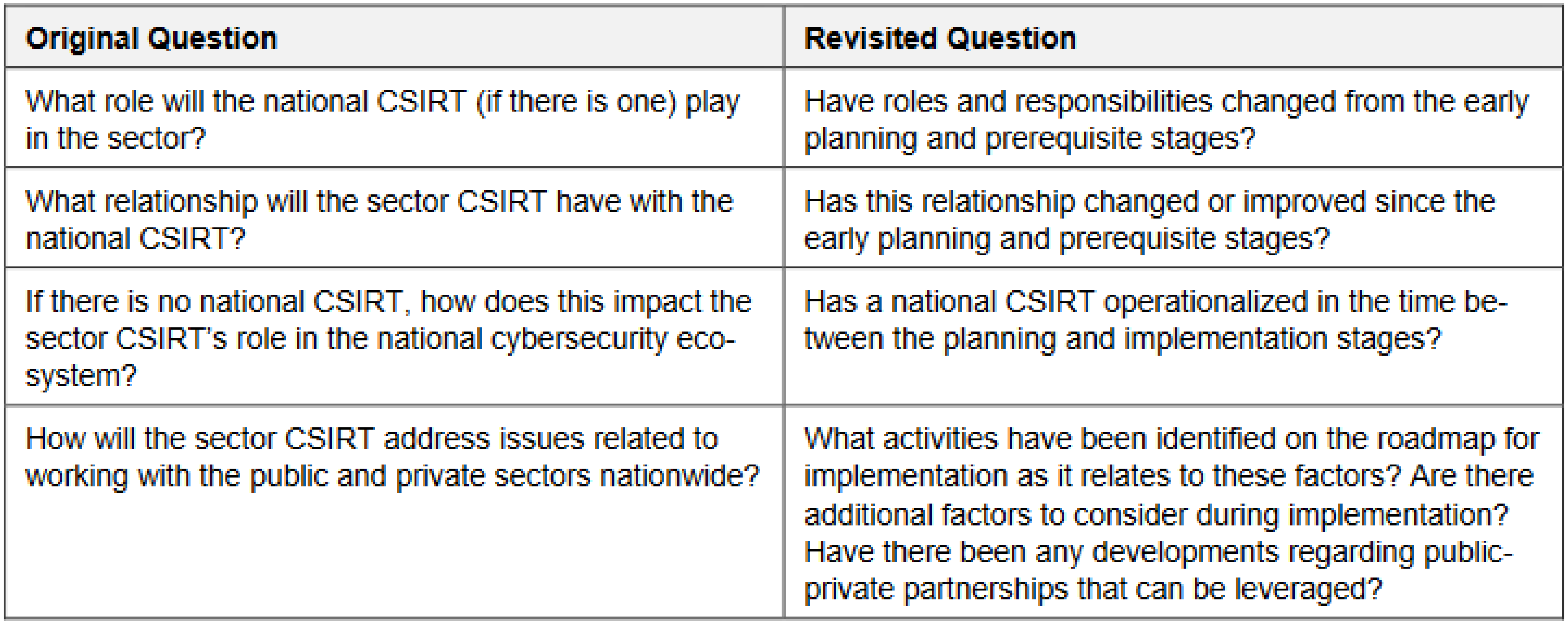
Example – Identify Considerations and Create a Roadmap


Example Sector CSIRT Framework Roadmap
Timeline
Information Gathering
Gaps
Determining Governance
Sector CSIRT Membership
Sector CSIRT and Incident Management Services
National Ecosystem
Pre-Requisites and other Preliminary Work
Mission, Goals, Governance Model
Defining Security Operations and Incident Management
Establishing agreements and Rules
Verification Methods: Audit and Assessment
Determine Roles and Responsibilities for Members
Establish Trust
Determine Roles of Sector CSIRTs Determine Use of CSIRT Services Framework
Establish/determine services
Outline Policies and R&R
Training
Determine System Requirements
Identify Audit and Enforcement Mechanisms
Outline Role of sector CSIRT with in the Ecosystem - Information Sharing Public Awareness CSIRT of Last Resort
Activities

Implementation

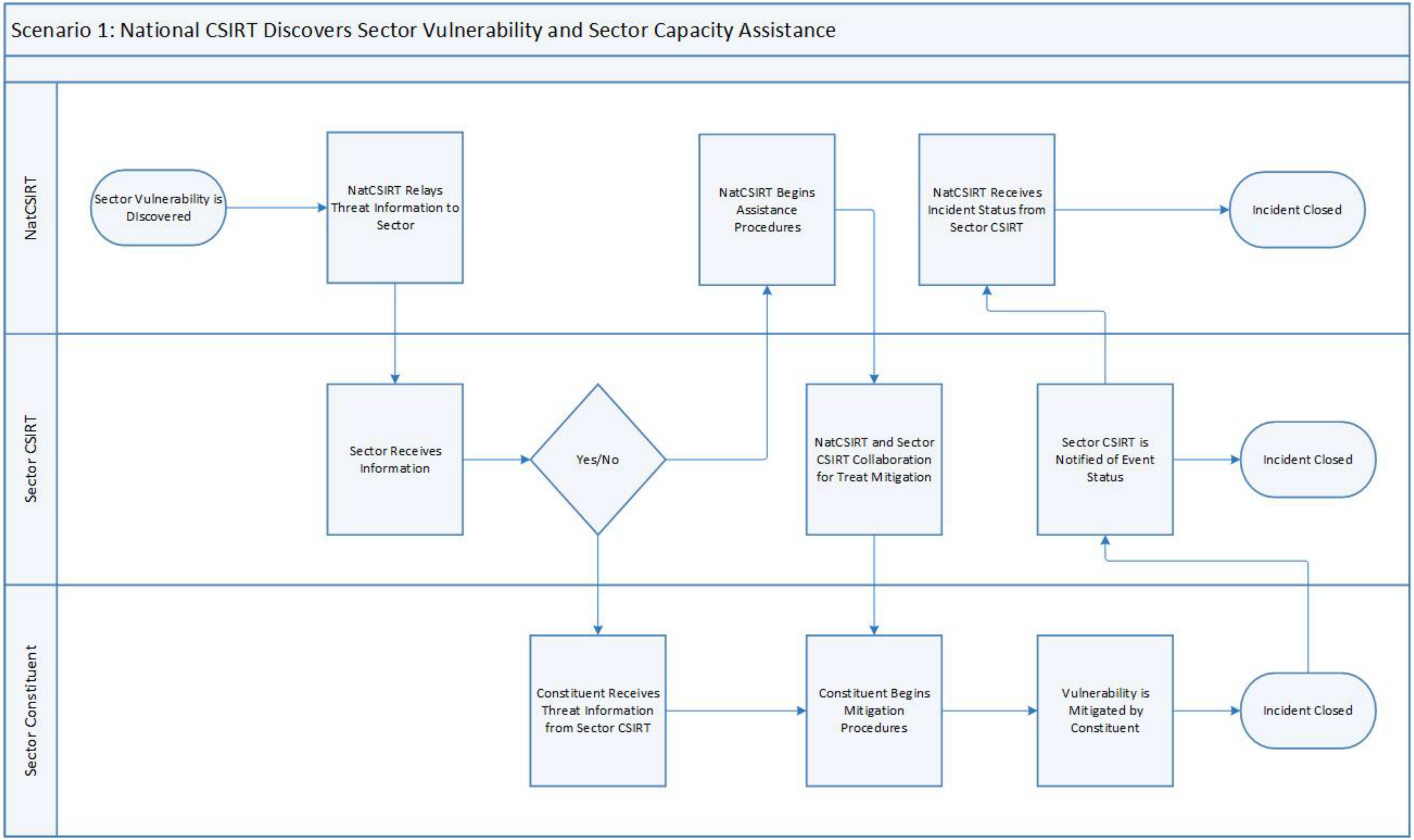
When implementing a sector CSIRT, it is critical to understand that this new sector CSIRT will (1) become an important part of the national ecosystem and (2) can affect how other stakeholders play their part.

As implementation occurs, teams must continually revisit questions asked early in the process, and address changes to the ecosystem.



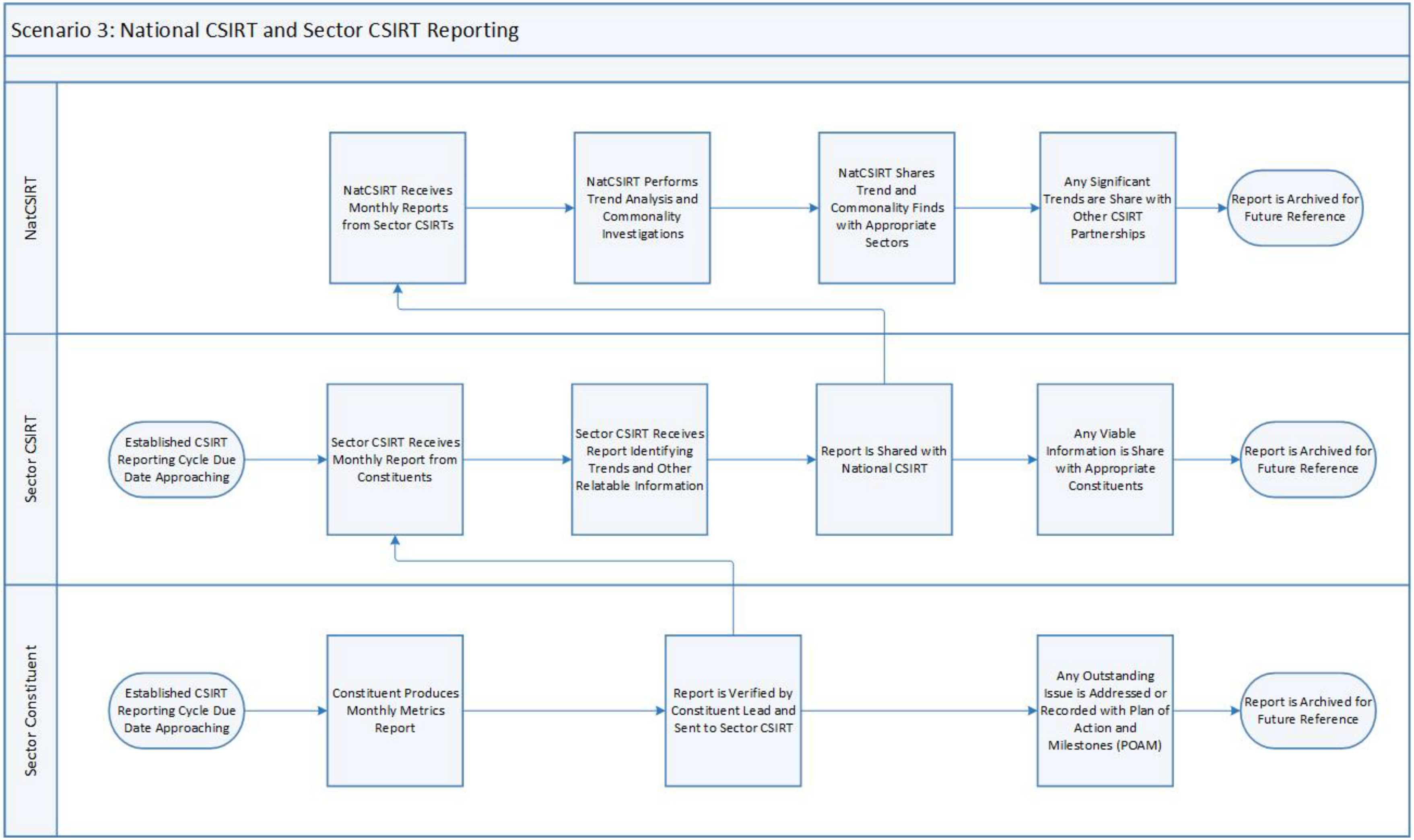
Original Question	Revisited Question
What role will the national CSIRT (if there is one) play in the sector?	Have roles and responsibilities changed from the early planning and prerequisite stages?
What relationship will the sector CSIRT have with the national CSIRT?	Has this relationship changed or 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?

Use case(s)



Scenario 1: National CSIRT Discovers Sector Vulnerability and Sector Capacity Assistance
NatCSIRT
Sector CSIRT
Sector Constituent
Sector Vulnerability is Discovered
NatCSIRT Relays Threat Information to Sector
NatCSIRT Begins Assistance Procedures
NatCSIRT Receives Incident Status from Sector CSIRT
Incident Closed
Sector Receives Information
Yes/No
NatCSIRT and Sector CSIRT Collaboration for Treat Mitigation
Sector CSIRT is Notified of Event Status
Incident Closed
Constituent Receives Threat Information from Sector CSIRT
Constituent Begins Mitigation Procedures
Vulnerability is Mitigated by Constituent
Incident Closed

Use case(s)



Scenario 3: National CSIRT and Sector CSIRT Reporting

NatCSIRT

NatCSIRT Receives Monthly Reports from Sector CSIRTs

NatCSIRT Performs Trend Analysis and Commonality Investigations

NatCSIRT Shares Trend and Commonality Finds with Appropriate Sectors

Any Significant Trends are Share with Other CSIRT Partnerships

Report is Archived for Future Reference

Sector CSIRT

Established CSIRT Reporting Cycle Due Date Approaching

Sector CSIRT Receives Monthly Report from Constituents

Sector CSIRT Receives Report Identifying Trends and Other Relatable Information

Report Is Shared with National CSIRT

Any Viable Information is Share with Appropriate Constituents

Report is Archived for Future Reference

Sector Constituent

Established CSIRT Reporting Cycle Due Date Approaching

Constituent Produces Monthly Metrics Report

Report is Verified by Constituent Lead and Sent to Sector CSIRT

Any Outstanding Issue is Addressed or Recorded with Plan of Action and Milestones (POAM)

Report is Archived for Future Reference

Thank you…

The security operations team and framework authors:

David Mcintire

Angel Hueca

Brittany Manley

Sharon Mudd

Tracy Bills

Contact:

security-operations@cert.org

Framework:

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=734783

Questions