

June 2022

Computer Security Incident Response Team (CSIRT)
Services Roles and Competencies
Version 0.9.0 for review!



Notice: This document describes what the Forum of Incident Response and Security Teams, Inc. (FIRST.Org) believes are best practices. These descriptions are for informational purposes only. FIRST.Org is not liable for any damages of any nature incurred as a result of or in connection with the use of this information.



Table of Contents

<u>1</u> <u>F</u>	PURPOSE AND INTRODUCTION	8
<u>2</u> <u>E</u>	BACKGROUND	10
2.1	UNDERSTANDING THE NICE WORKFORCE FRAMEWORK FOR CYBERSECURITY	10
2.2	MAPPING THE FIRST CSIRT SERVICES FRAMEWORK	11
2.3	DESCRIPTION OF ROLES AND COMPETENCIES	12
<u>3</u> <u>I</u>	HOW TO USE THIS DOCUMENT	14
4 9	SERVICE AREA: INFORMATION SECURITY EVENT MANAGEMENT	16
4.1	Role: Data Manager	17
4.1.1	1 DESCRIPTION	17
4.1.2	2 GENERAL TASKS	17
4.1.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	17
4.1.4	4 GENERIC COMPETENCIES	17
4.1.5	5 ROLE-SPECIFIC COMPETENCIES	17
4.2	ROLE: SYSTEM AND SENSOR ADMINISTRATOR	18
4.2.1	1 DESCRIPTION	18
4.2.2	2 GENERAL TASKS	18
4.2.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	19
4.2.4	4 GENERIC COMPETENCIES	19
4.2.5	5 ROLE-SPECIFIC COMPETENCIES	19
4.3	Role: Use Case Manager	19
4.3.1	1 Description	19
4.3.2	2 GENERAL TASKS	20
4.3.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	20
4.3.4	4 GENERIC COMPETENCIES	20
4.3.5	ROLE-SPECIFIC COMPETENCIES	20
<u>5</u> <u>9</u>	SERVICE AREA: INFORMATION SECURITY INCIDENT MANAGEMENT	22
5.1	Role: Communication Liaison	22
5.1.1	1 DESCRIPTION	22
5.1.2	2 GENERAL TASKS	23
5.1.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	23
5.1.4		23
5.1.5	5 ROLE-SPECIFIC COMPETENCIES	24
5.2	ROLE: INCIDENT ANALYST	24
5.2.1	1 DESCRIPTION	24
5.2.2	2 GENERAL TASKS	25



5.2.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	25
5.2.4	GENERIC COMPETENCIES	25
5.2.5	ROLE-SPECIFIC COMPETENCIES	25
5.3	ROLE: INCIDENT RESPONDER	26
5.3.1	DESCRIPTION	26
5.3.2	GENERAL TASKS	26
5.3.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	26
5.3.4	GENERIC COMPETENCIES	27
5.3.5	ROLE-SPECIFIC COMPETENCIES	27
5.4	ROLE: INCIDENT TRIAGE COORDINATOR	28
5.4.1	DESCRIPTION	28
5.4.2	GENERAL TASKS	28
5.4.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	28
5.4.4	GENERIC COMPETENCIES	29
5.4.5	ROLE-SPECIFIC COMPETENCIES	29
5.5	Role: IT Administrator	30
5.5.1	DESCRIPTION	30
5.5.2	GENERAL TASKS	30
5.5.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	30
5.5.4	GENERIC COMPETENCIES	30
5.5.5	ROLE-SPECIFIC COMPETENCIES	31
5.6	ROLE: MALWARE / FORENSIC ANALYST	31
5.6.1	DESCRIPTION	31
5.6.2	GENERAL TASKS	31
5.6.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	31
5.6.4	GENERIC COMPETENCIES	32
5.6.5	ROLE-SPECIFIC COMPETENCIES	32
<u>6</u> <u>S</u>	ERVICE AREA: VULNERABILITY MANAGEMENT	33
6.1	ROLE: IT SECURITY ADMINISTRATOR	34
6.1.1	DESCRIPTION	34
6.1.2	GENERAL TASKS	34
6.1.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	34
6.1.4	GENERIC COMPETENCIES	34
6.1.5	Role-Specific Competencies	34
6.2	Role: Vulnerability Analyst	35
6.2.1		35
6.2.2		35
	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	35
6.2.4		35
6.2.5		36
	ROLE: VULNERABILITY ASSESSMENT ANALYST	36



6.3.1	DESCRIPTION	36
6.3.2	GENERAL TASKS	36
6.3.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	37
6.3.4	GENERIC COMPETENCIES	37
6.3.5	ROLE-SPECIFIC COMPETENCIES	37
6.4	ROLE: VULNERABILITY COORDINATOR	38
6.4.1	DESCRIPTION	38
6.4.2	GENERAL TASKS	38
6.4.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	38
6.4.4	GENERIC COMPETENCIES	38
6.4.5	ROLE-SPECIFIC COMPETENCIES	39
6.5	ROLE: VULNERABILITY DISCLOSURE COORDINATOR	39
6.5.1	DESCRIPTION	39
6.5.2	GENERAL TASKS	40
6.5.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	40
6.5.4	GENERIC COMPETENCIES	40
6.5.5	ROLE-SPECIFIC COMPETENCIES	41
6.6	ROLE: VULNERABILITY RESEARCHER	41
6.6.1	DESCRIPTION	41
6.6.2	GENERAL TASKS	41
6.6.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	41
6.6.4	GENERIC COMPETENCIES	41
6.6.5	ROLE-SPECIFIC COMPETENCIES	42
6.7	ROLE: VULNERABILITY TRIAGE COORDINATOR	42
6.7.1	DESCRIPTION	42
6.7.2	GENERAL TASKS	42
6.7.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	43
6.7.4	GENERIC COMPETENCIES	43
6.7.5	ROLE-SPECIFIC COMPETENCIES	43
<u>7</u> <u>SE</u>	ERVICE AREA: SITUATIONAL AWARENESS	45
7.1	Role: Risk & Continuity Advisor / Risk Analyst	45
7.1.1	DESCRIPTION	45
7.1.2	GENERAL TASKS	46
7.1.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	46
7.1.4	GENERIC COMPETENCIES	46
7.1.5	ROLE-SPECIFIC COMPETENCIES	47
7.2	ROLE: SITUATIONAL AWARENESS DATA ANALYST	47
7.2.1	DESCRIPTION	47
7.2.2	GENERAL TASKS	48
7.2.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	48
7.2.4	GENERIC COMPETENCIES	48



7.2.5	ROLE-SPECIFIC COMPETENCIES	48
7.3	ROLE: SITUATIONAL AWARENESS MANAGER	49
7.3.1	DESCRIPTION	49
7.3.2	GENERAL TASKS	49
7.3.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	49
7.3.4	GENERIC COMPETENCIES	49
7.3.5	ROLE-SPECIFIC COMPETENCIES	50
7.4	ROLE: THREAT WARNING ANALYST	50
7.4.1	DESCRIPTION	50
7.4.2	GENERAL TASKS	51
7.4.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	51
7.4.4	GENERIC COMPETENCIES	51
7.4.5	ROLE-SPECIFIC COMPETENCIES	51
<u>8</u> <u>SE</u>	ERVICE AREA: KNOWLEDGE TRANSFER	53
8.1	Role: Awareness Coordinator	53
8.1.1	DESCRIPTION	53
8.1.2	GENERAL TASKS	53
8.1.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	54
8.1.4	GENERIC COMPETENCIES	54
8.1.5	ROLE-SPECIFIC COMPETENCIES	54
8.2	ROLE NAME: POLICY ADVISOR	55
8.2.1	DESCRIPTION	55
8.2.2	GENERAL TASKS	55
8.2.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	55
8.2.4	GENERIC COMPETENCIES	55
8.2.5	ROLE-SPECIFIC COMPETENCIES	56
8.3	Role: Staff Developer	56
8.3.1	DESCRIPTION	56
8.3.2	GENERAL TASKS	56
8.3.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	57
8.3.4	GENERIC COMPETENCIES	57
8.3.5	ROLE-SPECIFIC COMPETENCIES	57
8.4	Role: Technical Policy Advisor	58
8.4.1	DESCRIPTION	58
8.4.2	GENERAL TASKS	58
8.4.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	58
8.4.4	GENERIC COMPETENCIES	58
8.4.5	ROLE-SPECIFIC COMPETENCIES	59
8.5	ROLE: TRAINING DEVELOPER	59
8.5.1	DESCRIPTION	59
8.5.2	GENERAL TASKS	59



8.5.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	60
8.5.4	GENERIC COMPETENCIES	60
8.5.5	ROLE-SPECIFIC COMPETENCIES	60
8.6	ROLE: TRAINING INSTRUCTOR	60
8.6.1	DESCRIPTION	60
8.6.2	GENERAL TASKS	61
8.6.3	ASSOCIATED FUNCTIONS FROM THE FIRST CSIRT SERVICES FRAMEWORK	61
8.6.4	GENERIC COMPETENCIES	61
8.6.5	ROLE-SPECIFIC COMPETENCIES	61
<u>9</u> PF	RACTICAL CONSIDERATIONS	63
9.1	COMBINING MULTIPLE ROLES INTO SINGLE STAFF POSITIONS	63
9.2	ADDRESSING ROLE CONFLICTS	64
	SOME REMARKS ABOUT "MANAGEMENT" AND "MANAGERS"	64
ANNE	X 1: ACKNOWLEDGMENTS	66
ANNE	X 2: TERMS AND DEFINITIONS	67
ANNE	X 3: SUPPORTING RESOURCES	70
<u>ANNE</u>	X 4: CROSS-REFERENCE SERVICES VS. ROLES	72
ANNE	X 6: CROSS-REFERENCE ROLES VS. COMPETENCIES	76



Roles and Competencies Within the Context of the CSIRT Services Framework

1 Purpose and Introduction

The FIRST Computer Security Incident Response Team (CSIRT) Services Framework is a high-level document describing in a structured way a collection of cyber security services and associated functions that Computer Security Incident Response Teams and other teams providing incident management related services may provide. The framework was developed by recognized experts from the FIRST community with strong support from the Task Force CSIRT (TF-CSIRT) Community, and the International Telecommunications Union (ITU). Today it is maintained by the FIRST CSIRT Framework Development Special Interest Group (SIG).¹



Figure 1: Overview of Service Areas and Services (based on CSF v2.1)

1

Here after called the CSIRT SIG - https://www.first.org/global/sigs/csirt/



The mission and purpose of the FIRST CSIRT Services Framework is to facilitate the establishment and improvement of CSIRT operations, especially in supporting teams that are in the process of choosing, expanding, or improving their service portfolio. The services described are those potential services a CSIRT could provide. No CSIRT is expected to provide all described services. Each team will need to choose services that support their mission and constituents, as described by their mandate.²

The Framework seeks to assist teams by identifying and defining core categories of services and their sub-components. While this is an important part in defining the CSIRT as a whole, it does not give any insights or recommendations for providing any such service, that type of information is left to other public documents and training. Based on questions and input from the community the SIG volunteers decided to develop supplemental documentation that identified CSIRT Services related roles and competencies required for those roles. This process is explained in chapter 2 in more detail.

This document should be seen as an add-on to the existing FIRST CSIRT Services Framework. It helps to clarify the needs and requirements for CSIRT roles and will enable the quick(er) and more consistent writing of role descriptions.³ In addition it provides a clear overview of specific competencies that are important in handling the functions and tasks related to specific services provided.

In most cases, CSIRTs do not have staffing levels to allow each role to have one person assigned. We expect that a member of the CSIRT team will perform more than one role when necessary. In this case, the competencies an individual will be required to have or achieve will be combined for their assigned roles. If different roles are performed by the same person, potentially conflict of interests need to be considered and avoided.

Similar to services we anticipate that CSIRTs will choose their own role combinations, also we expect that based on similarities in size, structure and service portfolio, similar role combinations would be chosen based on common practices. The SIG decided not to provide a catalogue of suitable or likely combinations at this time. This might be added at some later stage based on experiences and examples provided by CSIRTs themselves.

It should also be noted that roles identified in this Roles and Competencies supplemental document may actually be handled or assigned to staff outside the CSIRT, rather than team members. How roles are assigned and who performs various related services and functions will depend on the CSIRT itself, its parent organization structure and mission, and what other organizational units have been established in the parent organization. For example, there is a role "IT Administrator" and a role description and set of desired competencies in this supplemental document. In some CSIRTs this IT Administrator may be part of the CSIRT itself. In other teams, it may be part of the IT group but still provide services used by the CSIRT. This document does not attempt to explain when either scenario is best, that is the decision of the CSIRT and its parent organization depending on factors considered outside the scope of this documentation.

That there may be unique services you provide that are not covered by the FIRST CSIRT Services Framework, that is something expected for certain teams.

https://sim3-check.opencsirt.org/#/ See information about parameter H3: Skillset description



Note that this document does not explain how to select staff members or how to improve the competencies of existing staff members.

This version of the document replaces all previous versions. It makes no suggestions or recommendations about capability, capacity, maturity, or quality of staff for any particular type of CSIRT. Such topics are important for the value provided by any CSIRT towards its constituency but were intentionally not included in this document.

2 Background

The FIRST CSIRT Services Framework outlines service areas related to the performance of CSIRT and Security Operations activities. Within each service area, activities are broken out in a more detailed manner as services and functions. Once the FIRST CSIRT Services Framework was completed and published by the FIRST CSIRT Framework Development SIG, questions about its use were received from FIRST members. Members and related organizations that were looking to adopt it, wanted to know who would perform these functions, what skill sets were needed to perform the functions, and what training would they require.

To begin, existing resources were researched to see what was available as a starting or leverage point for identifying roles and competencies related to each service and its related functions. One resource that some SIG members had worked with before, that looked to be a good starting point, was the U.S. National Institute of Standards and Technologies (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity Education. This framework is commonly referred to as the NICE Framework.

"The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity education, training, and workforce development."

2.1 Understanding the NICE Workforce Framework for Cybersecurity

The CSIRT Services Roles and Competencies supplemental document was developed using the original version of the NICE Framework. That document breaks out information into Categories of Cybersecurity Work, Specialty Areas, and Work Roles.⁵

This diagram, shows the Categories and the Specialty Areas:

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

A new version of the NICE Framework was published in 2020 available at:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf, At some point this Roles and Competencies Supplemental Guide may be updated to match the new version of NICE.



Securely Provision (SP)	Risk Management (RSK)	Software Development (DEV)	Systems Architecture (ARC)	Technology R&D (TRD)	Systems Requirements Planning (SRP)	Test and Evaluation (TST)	Systems Development (SYS)
Operate and Maintain (OM)	Data Administration (DTA)	Knowledge Management (KMG)	Customer Service and Technical Support (STS)	Network Services (NET)	Systems Administration (ADM)	Systems Analysis (ANA)	
Oversee and Govern (OV)	Legal Advice and Advocacy (LGA)	Training, Education, and Awareness (TEA)	Cybersecurity Management (MGT)	Strategic Planning and Policy. (SPP)	Executive Cyber Leadership (EXL)	Program/Project Management (PMA) and Acquisition	
Protect and Defend (PR)	Cyber Defense Analysis (CDA)	Cyber Defense Infrastructure Support (INF)	Incident Response (CIR)	Vulnerability Assessment and Management (VAM)			
Analyze (AN)	Threat Analysis (TWA)	Exploitation Analysis (EXP)	All-Source Analysis (ASA)	Targets (TGT)	Language Analysis (LNG)		
Collect and Operate (CO)	Collection Operations (CLO)	Cyber Operational Planning (OPL)	Cyber Operations (OPS)				
Investigate (IN)	Cyber Investigation (INV)	Digital Forensics (FOR)					

Figure 2: Categories and the Specialty Areas

This table shows the category for Protect and Defend and the Specialty Areas of Incident Management and Vulnerability Management and the related work roles.

NICE Specialty Area	NICE Specialty Area Description	Work Role	Work Role Description	Work Role ID	KSAs	Tasks
Incident Response (CIR)	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	Cyber Defense Incident Responder	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.	PR-CIR-001	Click to view KSAs	Click to view Tasks
Vulnerability Assessment and Management (VAM)	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.	Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or endave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.	PR-VAM-001	Click to view KSAs	Click to view Tasks

Figure 3: Example for "Specialty Areas" of NICE

In the NICE Framework, tasks for each work role were defined and then various knowledge, skills, and abilities (KSAs) were identified to define what was needed to be able to perform these work roles. Separate documents were developed by the NICE team which provided a set of competencies that could be mapped to NICE roles and KSAs. Competencies are comprised of a set of knowledge and skills. Competencies for NICE can be found in the supplemental materials:

http://www.nist.gov/document/niceframeworkksatocompetencymappingxlsx

2.2 Mapping the FIRST CSIRT Services Framework

For the initial task of the mapping roles to the FIRST CSIRT Services Framework services and functions, the SIG used work roles and tasks where appropriate, and competencies rather than the lower-level



KSAs, which may be addressed later. The NICE Framework is not comprehensive for all cybersecurity or CSIRT services, functions, and tasks. Therefore, there are roles, descriptions, and competencies in this supplemental document that the SIG added to fit the situation and general CSIRT practices. Applying the NICE Framework to Roles and Competencies

To start the mapping, the FIRST CSIRT Framework SIG broke up the service areas across the SIG Members. Each team went through the various services and functions and mapped them to a work role from NICE that was most appropriate or if there was not one that fit, a work role that did fit was created and added. Sometimes the SIG adjusted the names of NICE work roles to better fit accepted CSIRT terminology.

The first step resulted in tables such as this example (excerpt):



Figure 4: Example of table used for role identification-

Once the SIG had done that for all services and related functions, and it had been reviewed and agreed to, then we wrote up descriptions for each work role.

2.3 Description of Roles and Competencies

To make the adaptation of roles and competencies easier we decided to collect all roles within the context of the relevant CSIRT services area within a single chapter (4 to 8):

- Information Security Event Management
- Information Security Incident Management
- Vulnerability Management
- Situational Awareness
- Knowledge Transfer



For each CSIRT services area the applicable roles are listed in alphabetical order and described in more detail. The text for each role includes the following fields:

- Description Characteristics of the role context in the FIRST CSIRT Services Framework
- General Tasks List of tasks for the role based on the context, services, and service area
- Associated Functions from FIRST CSIRT Services Framework Reference to the specific functions
- **Generic Competencies (from NICE)** List of competencies in reference to the NICE Framework categories not specific to the role
- Role-Specific Competencies (from NICE) List of specific competencies for the role referenced to the NICE Framework categories

The following roles have been identified and described according to this format:

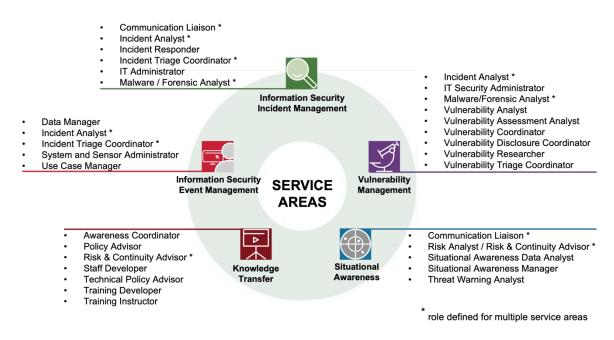


Figure 5: Overview of Roles by Service Areas

All roles discussed in the document are proficiency level-agnostic, meaning that basic mastering of all competences is expected for everyone. For teams, where proficiency grading is required, the following method to split the seniority for chosen roles is suggested.

- For each role create of three levels: lowest is created by adding "Junior" to the title, then normal as named, and finally senior role with addition of "Senior" to the title.
- Designation of Junior means that person cannot yet do independently cover fully the assigned role, more training is needed and supervision at least to some degree is necessary.



 Designation of Senior means that person is not only capable to express all needed competences, but in most of them is excelling the required threshold. Those Seniors are candidates to be mandated to provide training to junior positions, as well as handle escalations from Juniors and normal level colleagues.

Examples of proficiency leveling can be found within the NIST NICE work roles portal (https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles), where capability indicators are leveled as Entry ("junior"), Intermediary ("normal"), and Advanced ("Senior").

After we have described all potentially separated roles, we will discuss in Section 9.2 more practical topics related to the usage of this document. Initially we will identify any role conflicts to consider. Basically, such roles should not be assigned to the same person, and we will explain why.

3 How to use this Document

The FIRST CSIRT Services Framework is a high-level document to help teams to identify and define the services – linked to certain functions, tasks, and roles – which are mandated to deliver. The identified competencies should help to identify and recruit the personnel needed as well as to prepare and plan training for staff members.

As there are well-established distinctions between various "types" of teams, e. g. Coordinating CSIRTs, National CSIRTs, Internal CSIRT, the priorities and the importance of competencies for each role will also be different. It is obvious, that the same role in different types of teams can also implemented differently based on a decision to combine tasks or functions in a team-specific way. For now, no effort was made to recommend or present roles for specific "types" of teams. Still, this document shall help to identify required or suitable competencies by considering which team-specific role tasks and functions are mandated.

Overall, this document can serve many practical purposes, for example, to assist in answering at least the following questions:

1. What roles and competencies do I need in my CSIRT?

To answer this question please follow these steps which can be applied to new teams as well as for existing teams during a re-structuring effort:

- 1.1. Map own CSIRT services to services of the CSIRT Services Framework,
- 1.2. Note the names of the roles covering the mapped services,
- 1.3. Check which of your own staff positions can take single or multiple roles,
- 1.4. For each role, please compile competencies and validate if all of them are of interest and required in your context.

2. How to develop a career path and related training for staff members?

This can be applied in a context in which staff members take up additional responsibilities in new roles or in a setting in which a new staff member needs additional training to order to fulfill all tasks required in the new position:



- 2.1. A career path (or professional development) can be expressed in terms of one (or multiple) role with associated competencies,
- 2.2. Based on the competencies of the particular staff member a gap analysis shall be used to identify those competencies that need to be developed or extended further as well as specifying what the best training method would be,

Additionally, the NIST NICE should be consulted to further identify knowledge, skills and abilities that describe the desired competencies.

3. How to write a job description for a new opening?

This can be applied for new as well as for existing teams:

- 3.1. Identify the expected work activities for a particular staff position starting from the relevant list of services offered and associated functions,
- 3.2. Based on this identify the role (or roles) describing the new staff position,
- 3.3. Combine all competencies, which are required by the identified role (or roles) and create a job description for the new opening.

If needed, the NIST NICE can be consulted to identify additional competencies or knowledge, skills, and abilities to further detailing the job description.

4. How to revise a job description for an existing job position?

This is very similar to scenario 3 "How to write a job description for a new opening" except that the job position is already filled.

- 4.1. Identify the existing job description for the job position that shall be re-defined,
- 4.2. Establish a new job description draft based on scenario 3,
- 4.3. Add missing information applicable from the original existing job description to the new draft and finalize it.

Especially for new or small teams it is not unusual to not have any job descriptions at all. In such cases teams will start only when they grow or when they are building a more mature team set-up and formalize their operations. It is best in such cases to address such re-structuring efforts like the build-up of a new team. If then existing staff members are missing some competencies to fill their new role, this should be handled like scenario 2 "How to develop a career path ..." in order to identify the right set of training.



4 Service Area: Information Security Event Management

Information Security Event Management aims to identify information security incidents based on the correlation and analysis of security events from by a wide variety of event and contextual data sources. In larger organizations, this service area is sometimes fully or partially assigned to a Security Operations Center (SOC), which might additionally also perform first- or even second-level Information Security Incident Management such as initiating mitigations or adjustments of security controls. As any Information Security Incident Management service depends on qualified and accurate data about information security events, the interface between a SOC and the assigned CSIRT is crucial.⁶

The following roles⁷ are considered to handle particular functions:⁸

- Data Manager
- Incident Analyst *)
- Incident Triage Coordinator **)
- System and Sensor Administrator
- Use Case Manager

*) The role as Incident Analyst is instrumental for the Service Area: Information Security Incident Management. Please refer for all further details regarding this role to section 5.1 Communication Liaison on page 22.

**) The role as Incident Triage Coordinator is also instrumental for the Service Area: Information Security Incident Management. Please refer for all further details regarding this role to section 5.4 Role: Incident Triage Coordinator on page 28.

_

Although the FIRST CSIRT Services Framework does not aim to define a SOC services framework, it is certainly expected that services from both Information Security Event and Incident Management areas will be useful and directly applicable while defining SOC services.

All list of roles and competencies are ordered alphabetically. Competencies are grouped in this order: Leadership, Professional, Operational and Technical.

If the Incident Analyst and Incident Triage Coordinator roles are applicable solely in the SOC services context, they might "only" handle Information Security Events instead of events and incidents. While the competencies required for each more specific role will most certainly not differ much from the descriptions in this report, the roles can rightfully be renamed to Event Analyst and Event Triage Coordinator, especially if different teams are working side by side in a mixed SOC/CSIRT setting.



4.1 Role: Data Manager

4.1.1 Description

Data Manager is responsible for managing contextual data throughout its lifecycle, derived from such as APIs, Configuration Management Database, Identity and Access Management, or Threat intelligence Systems.

4.1.2 General Tasks

- Analysis of data structures of sensors, API, CMDB, IAMS and Threat Intelligence Systems
- Monitoring data sources and their behavior to update contextual data
- Monitoring new data sources which may need to be included in contextual data
- Keep contextual data up to date for better detection.

4.1.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Event Management
 - Monitoring and Detection
 - Contextual Data Management (5.1.3)

4.1.4 Generic Competencies

- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
 - o Oral Communication (C036)
 - Written Communication (C060)
- Operational
 - o Business Continuity (C002)
 - Data Privacy and Protection (C014)
 - Risk Management (C044)
- Technical
 - o Problem Solving⁹ (C040)

4.1.5 Role-Specific Competencies

- Technical
 - o Computer Network Defense (C007)
 - Data Management (C013)
 - Information Assurance (C022)
 - o Information Systems and Network Security (C024)
 - Knowledge Management (C029)

Within the NIST NICE Framework the competency "Problem Solving (C040)" is assigned to the "technical" competencies. In versions prior to November 2020, it had been listed under "professional" competencies. Regardless of such association it is obvious, that solving problems is a key competency in any CSIRT or security team.



- Network Management (C033)
- Technology Awareness (C053)
- Threat Analysis (C055)
- Vulnerabilities Assessment (C057)

4.2 Role: System and Sensor Administrator

4.2.1 Description

The administration of IT systems in networks, i.e., systems to enable the CSIRT to detect information security related events is crucial. Every device or component within a network produces log data and can be used as sensor for monitoring and detecting these events. Specific sensor components like firewalls or SIEM provide data for the analysis. The management and configuration of these components is essential to identify potential incidents.

The role of the System and Sensor Administrator is to configure and maintain the components including security settings and rules to identify information security events. Such components may include not only traditional server and client computers, routers, and switches, but also IoTs, ICS devices, sensors in OT environment, or any components connected to the information systems that need configuration, updates, and maintenance. In the context of FIRST CSIRT Services Framework, this is responsible for configuration, management and maintenance of all components providing logs and log sources through the lifecycle of the equipment she or he is in charge, as described in "5.1.1 Function: Log and sensor management". The system administrator needs to closely work with other stakeholders including CSIRT, SOC, NOC, and partner organizations to accomplish such objectives.

Depending on the organization, the system administrator can also be part of another unit of the host organization, e.g., in the IT department, or an external support person, working "for" the CSIRT to carry out the required tasks.¹⁰

4.2.2 General Tasks

- Install, configure, and maintain IT systems with focus on security event logging
- Install, configure, and maintain sensor components
- Configure and maintain rule sets for monitoring and logging of information security events on behalf of the asset owner of the equipment over the life cycle of the equipment in charge from deployment through the end of its operation.
- Monitor, identify, and resolve the outages, log data quality/scope, and system configuration issues, working with other stakeholders such as other system administrators, CSIRT, SOC, NOC or other partners including vendors.
- Monitor vulnerabilities and implement patches or mitigation until patches become available, to keep the system up to date and secure.

In this case it is not expected that the CSIRT will be responsible to identify and define competencies of this role but might provide input or requirements for either the staff position or service provider.



4.2.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Event Management
 - Monitoring and Detection
 - Log and sensor management (5.1.1)

4.2.4 Generic Competencies

- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
- Operational
 - Business Continuity (C002)
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Organizational Awareness (C037)
 - Risk Management (C044)
- Technical
 - o Problem Solving (C040)

4.2.5 Role-Specific Competencies

- Technical
 - Asset and Inventory Management (C001)
 - Computer Network Defense (C007)
 - Data Management (C013)
 - Information Assurance (C022)
 - Information Systems and Network Security (C024)
 - Network Management (C033)
 - Operating Systems (C034)
 - Operations Support (C035)
 - Software Testing and Evaluation (C046)
 - System Administration (C048)
 - Systems Integration (C049)
 - Systems Testing and Evaluation (C050)
 - Technology Awareness (C053)

4.3 Role: Use Case Manager

4.3.1 Description

Use Case Manager is responsible for managing the entire lifecycle of detection use cases as described at 5.1.2 Function: Detection use case management of FIRST CSIRT Services Framework. Since detection use case is a part of knowledge, this role can be performed by Knowledge Manager as defined by NICE Framework NIST SP 800-181. As new detection approaches are developed, tested, and improved, they

FIRST.

Forum of Incident Response and Security Teams

need to be reflected into Standard Operating Procedures (SOPs), guidance, or playbooks to update instructions for analyst to triage, qualify, and correlate events and incidents, while obsoleted or outdated use cases need to be improved, redefined, or removed. Use Case Manager or Knowledge Manager needs to keep monitoring both new and existing use cases to keep SOPs up to date for improved and efficient triage, qualification and correlation as described.

4.3.2 General Tasks

- Evaluate detection use cases on validity, relevance, and efficiency.
- Keep monitoring new approaches and confirm if and how they are developed, tested, and deployed.
- Assess how relevant each new approach is to constituencies
- Define Standard Operating Procedures (SOP) for detection use cases and update them when needed.
- Determine whether the existing Standard Operating Procedures (SOPs) or guidance need to be updated based on the assessment of new approaches or new use cases which may help improve triage, qualification and/or correlation.

4.3.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Event Management
 - Monitoring and Detection
 - Detection use case management (5.1.2)

4.3.4 Generic Competencies

- Professional
 - Conflict Management (C009)
 - o Critical Thinking (C011)
 - Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational
 - Business Continuity (C002)
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Organizational Awareness (C037)
 - o Policy Management (C038)
 - Risk Management (C044)
- Technical
 - o Problem Solving (C040)

4.3.5 Role-Specific Competencies

- Technical
 - Asset and Inventory Management (C001)



- o Computer Network Defense (C007)
- Data Management (C013)
- o Information Assurance (C022)
- o Information Systems and Network Security (C024)
- o Intelligence Analysis (C027)
- o Knowledge Management (C029)
- Network Management (C033)
- Operating Systems (C034)
- o Requirements Analysis (C043)
- o Technology Awareness (C053)
- Threat Analysis (C055)
- Vulnerabilities Assessment (C057)



5 Service Area: Information Security Incident Management

This service area is at the heart of any CSIRT and consists of services that are vital in helping constituents during an attack or incident. CSIRTs must be prepared to help and support. Through this unique position and expertise, they are able to not only collect and evaluate information security incident reports, but also to analyze relevant data and perform detailed technical analysis of the incident itself and any artefacts used.

From this analysis, mitigation, and steps to recover from the incident can be recommended, and constituents will be supported in applying the recommendations. This also requires a coordination effort with external entities such as peer CSIRTs or security experts, vendors, or PSIRTs to address all aspects and reduce the number of successful attacks later on.

The special expertise CSIRTs can provide is also critical in addressing (information security) crises. While in many instances a CSIRT will not handle the crisis management, it can support any such activity. Making its contacts available, for example, can greatly improve the application of required mitigation steps or better protection mechanisms.

Applying the knowledge and the available infrastructure to support its constituency is key to improving overall information security incident management.

The following roles are considered to handle particular functions:

- Communication Liaison
- Incident Analyst
- Incident Responder
- Incident Triage Coordinator
- IT Administrator
- Malware / Forensic Analyst

5.1 Role: Communication Liaison

This particular role, Incident Analyst is another the first one (of five) within the FIRST CSIRT Services Framework that is relevant to two Service Areas: Information Security Event Management and Situational Awareness. Role descriptions, tasks, functional activities, and competencies as relates to each service area is listed below separately if applicable.

5.1.1 Description

Communicating with the media is unavoidable in many cases. While CSIRTs usually try to avoid such contact, it is important to realize that the media can help to mitigate specific types of ongoing and large-scale attacks causing information security incidents. For this it is necessary to explain what is causing the information security incidents and explain the impact on users and/or organizations. In some cases, a CSIRT might choose to provide this information already in a manner suitable for release to the public, but this certainly requires specific skills inside the CSIRT not readily available in most. In

EKSI

Forum of Incident Response and Security Teams

any case, if a CSIRT communicates with the media, it must take great care to simplify the technical issues as much as possible and leave out all confidential information.

As the response to a crisis progresses, information must be distributed and disseminated. As the CSIRT has established such resources for its own purposes, crisis management may see it as appropriate or necessary to use such resources.

Informing other entities in a timely manner about the impact caused by the crisis on currently open information security incidents provides a clear understanding of what support can also be provided by the CSIRT during the duration of the crisis and makes sure that entities understand what to expect. It also makes sure that other parties don't stop their support or interaction with the CSIRT.

If the crisis management team should decide to postpone the response to an actual information security incident due to an ongoing crisis, such decisions need to be communicated to all entities currently informed and participating in the mitigation and response to this incident. This is to avoid misunderstandings and further issues that may also lead to a loss of trust in the CSIRT and/or host organization.

5.1.2 General Tasks

- Manage communication with media
- Manage Information distribution to constituents
- Serve as a contact point for communicating with media
- Support and advise crisis management team on crisis communication
- Advise on communication strategy, processes, and procedures

5.1.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Incident Management
 - o Information Security Incident Coordination
 - Media Communication (6.5.6)
 - Crisis Management Support
 - Information Distribution to Constituents (6.6.1)
 - Strategic Decisions Communication (6.6.3)
- Service Area: Situational Awareness
 - Service Communication
 - Dissemination / Integration / Information Sharing (8.3.4)
 - Management of Information Sharing (8.3.5)
 - Feedback (8.3.6)

5.1.4 Generic Competencies

- Leadership
 - Teaching others (C052)
- Professional
 - Interpersonal Skills (C028)
- Operational



- Client Relationship Management (C003)
- Data Privacy and Protection (C014)
- Legal, Government, and Jurisprudence (C030)

5.1.5 Role-Specific Competencies

- Professional
 - Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational
 - External Awareness (C019)
- Technical
 - Knowledge Management (C029)

5.2 Role: Incident Analyst

This particular role, Incident Analyst is another the second one within the FIRST CSIRT Services Framework that is relevant to actually three Service Areas: Information Security Event Management, Information Security Incident Management and Vulnerability Management. Role descriptions, tasks, functional activities, and competencies as relates to each service area is listed below separately if applicable.

Some of the general tasks attributed to this role can instead be carried out by another – more specialized – role: Malware / Forensic Analyst (see section 5.5 on page 30) depending on the local CSIRT context.

5.2.1 Description

Information Security Events, potential and confirmed Information Security Incidents, which are reported or detected by the monitoring services need to be analyzed in order to be correctly categorized those. It is critical to identify, if information security incidents are pertaining to the same assets (e.g., systems, services, customers) or identities (e.g., users), or if those are otherwise directly related to other potential information security incidents and should be grouped together.

Once new information is identified directly related to another ongoing information security incident(s), that identified new information should be correlated to the relevant information security incident for better incident handing and response, rather than opening a new, separate information security incident.

An Incident Analyst is responsible for establishing relations and dependencies among all events and incidents or correlating new events or incidents to each other once they are identified or to research for new patterns describing new attacks.

Improving Security Together

Forum of Incident Response and Security Teams

5.2.2 General Tasks

- Analyze and understand information security events, potential and confirmed information security incidents
- Assess the potential and actual impacts and damages
- Analyze incidents to identify root cause and impact
- Conduct cross-incidents analysis
- Analyze media and perform surface analysis of artifacts
- Discover incident-related vulnerabilities used by attacks
- Identify and correlate, when appropriate, distinct but possibly related security events and/or incidents to better understand the context of the incident in a bigger picture

5.2.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Event Management
 - Event Analysis
 - Correlation (5.2.1)
- Service Area: Information Security Incident Management
 - o Information Security Incident Report Acceptance:
 - Information Security Incident Root Cause Analysis (6.2.4)
 - Cross-Incident Correlation (6.2.5)
 - Artifact and Forensic Evidence Analysis:
 - Media or Surface Analysis (6.3.1)
- Service Area: Vulnerability Management
 - Vulnerability Discovery/Research:
 - Incident Response Vulnerability Discovery (7.1.1)

5.2.4 Generic Competencies

- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
 - o Oral Communication (C036)
 - Written Communication (C060)
- Technical
 - Problem Solving (C040)

5.2.5 Role-Specific Competencies

- Operational
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - o Organizational Awareness (C037)
- Technical
 - Computer Forensics (C005)

Improving Security Together

Forum of Incident Response and Security Teams

- Computer Network Defense (C007)
- Data Analysis (C012)
- Data Management (C013)
- Incident Management (C021)
- Information Systems/Network Security (C024)
- Information Technology Assessment (C025)
- Intelligence Analysis (C027)
- Knowledge Management (C029)
- Technology Awareness (C053)
- Threat Analysis (C055)
- Vulnerabilities Assessment (C057)

5.3 Role: Incident Responder

5.3.1 Description

Analyze and gain an understanding of a confirmed information security incident. Intake, catalog, store, and track information related to the information security incident and all information security events that are considered to be part of it. Initiate and track any other technical analysis in regard to an information security incident.

Contain the information security incident as much as possible to limit the number of victims, reduce the loss and to recover from damage, avoid further attacks and further losses by removing exploited vulnerabilities or weaknesses, and improve overall cyber security.

Contain the information security incident as much as possible to limit the number of victims, reduce the loss and to recover from damage, avoid further attacks and further losses by removing exploited vulnerabilities or weaknesses, and improve overall cyber security.

5.3.2 General Tasks

- Incident report information collection and analysis coordination
- Mitigation and Recovery plan preparation and support in response actions
- Incident coordination via planning, communication, activities coordination, reporting

5.3.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Incident Management
 - o Information Security Incident Analysis
 - Information Collection (6.2.2)
 - Detailed Analysis Coordination (6.2.3)
 - Mitigation and Recovery
 - Response Plan Establishment (6.4.1)
 - Ad Hoc Measures and Containment (6.4.2)
 - Other Information Security Entities Support (6.4.4)
 - Information Security Incident Coordination



- Communication (6.5.1)
- Notification Distribution (6.5.2)
- Relevant Information Distribution (6.5.3)
- Activities Coordination (6.5.4)
- Reporting (6.5.5)

5.3.4 Generic Competencies

- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
 - o Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational
 - Client Relationship Management (C003)
- Technical
 - Problem Solving (C040)

5.3.5 Role-Specific Competencies

- Operational
 - Business Continuity (C002)
 - Data Privacy and Protection (C014)
 - o External Awareness (C019)
 - o Legal, Government, and Jurisprudence (C030)
 - Organizational Awareness (C037)
 - o Risk Management (C044)
- Technical
 - o Computer Forensics (C005)
 - o Computer Network Defense (C007)
 - Data Analysis (C012)
 - Incident Management (C021)
 - Information Systems/Network Security (C024)
 - Information Technology Assessment (C025)
 - o Intelligence Analysis (C027)
 - Knowledge Management (C029)
 - Technology Awareness (C053)
 - Threat Analysis (C055)
 - Vulnerabilities Assessment (C057)



5.4 Role: Incident Triage Coordinator

This particular role, Incident Triage Coordinator is another one within the FIRST CSIRT Services Framework that is relevant to two Service Areas: Information Event Incident Management and Information Security Incident Management.

5.4.1 Description

The Incident Triage Coordinator initially analyses and prioritizes detected information security events and/or incidents and forwards them to the incident management process based on criteria such as assessed possible impacts, potential damages, incident capabilities, and business priorities. The Incident Triage Coordinator works with and coordinates the exchange of relevant information with multiple stakeholders such as CSIRT, SOC, NOC, IT department, Business or Process owners, decision makers, external resources like vendors, or other trusted experts. This coordination should include consensus by stakeholders since triaging incidents will have direct impact on businesses, organizational risks, and possible responses to losses and actual damages.

5.4.2 General Tasks

- Analyze and determine security events true positive, false positive, and false negative
- Detect, analyze, and determine the potential security incidents among security events
- Design, configure, tune, and update the tools supporting triage to accomplish the above
- Monitor other incidents to learn lessons from them, which can help triage possible incidents on its own organization
- Review and understand vulnerability reports relevant to the information assets of the
 constituencies to obtain an initial understanding of the vulnerability in question and determine
 what to do next (e.g., process the vulnerability for further analysis, seek additional information
 from the reporter or other sources, decide that the vulnerability needs no further action).
- Escalate the output of the triage, when necessary, to other relevant subject matter experts for further analysis, or to the supervisor or the appropriate decision maker for higher decision making.

5.4.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Event Management
 - Event Analysis
 - Qualification (5.2.2)
- Service Area: Information Security Incident Management
 - o Information Security Incident Report Acceptance
 - Information Security Incident Report Receipt (6.1.1)
 - Information Security Incident Triage and Processing (6.1.2)
 - Information Security Incident Analysis
 - Information Security Incident Triage (prioritization and categorization) (6.2.1)
 - Crisis Management Support
 - Information Security Status Reporting (6.6.2)

5.4.4 Generic Competencies

- Leadership
 - Strategic Planning (C047)
 - Teaching Others (C052)
 - Workforce Management (C059)
- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
 - o Interpersonal Skills (C026)
 - Written Communication (C060)
- Operational
 - o Business Continuity (C002)
 - Risk Management (C044)
- Technical
 - o Problem Solving (C040)

5.4.5 Role-Specific Competencies

- Operational
 - Client Relationship Management (C003)
 - Data Privacy and Protection (C014)
 - o External Awareness (C019)
 - o Legal, Government, and Jurisprudence (C030)
 - Organizational Awareness (C037)
 - Policy Management (C038)
- Technical
 - Computer Forensics (C005)
 - Computer Network Defense (C007)
 - Data Analysis (C012)
 - o Incident Management (C021)
 - Information Systems/Network Security (C024)
 - Information Technology Assessment (C025)
 - o Intelligence Analysis (C027)
 - Knowledge Management (C029)
 - o Requirements Analysis (C043)
 - Technology Awareness (C053)
 - Threat Analysis (C055)
 - Vulnerabilities Assessment (C057)



5.5 Role: IT Administrator

For an internal CSIRT – especially if it is only be built in an ad-hoc fashion to respond to an information security incident – an Information Technology (IT) Administrator might become part of the CSIRT. In most other contexts most notably for coordinating CSIRTs or national CSIRTs, the functions identified in the FIRST CSIRT Services Framework to restore compromised systems etc. are carried out by the owner, not by the CSIRT that informed the owner of any such information security incident.

Therefore, we are providing here the same information as for other roles within the context of the FIRST CSIRT Services Framework, but do not expect that a CSIRT will implement such role internally, except it has a real need – participating in the response and mitigation as part of the services offered to the constituents.

5.5.1 Description

Restoring the integrity of affected systems and returning the affected data, systems, and networks to a non-degraded operational state, restoring the impacted services to full functionality. As business reality usually demands systems return to normal operation as soon as possible, there is a risk that not all means of unauthorized access have been removed successfully. Therefore, unless the analysis results are already available, even returned systems must be carefully monitored and managed. Especially if identified vulnerabilities and weaknesses cannot (yet) be eliminated, improved protection and detection mechanisms need to be applied to avoid the same or similar or types of information security incidents.

5.5.2 General Tasks

- Restore user/system data from trusted backup media
- Restore configurations from trusted backup media or recreated content
- Enable disabled services and re-establish access for users/systems/networks
- Perform functional tests to validate the capacity and capability of systems/services/networks both on an infrastructure and application level

5.5.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Incident Management
 - Mitigation and Recovery
 - System Restoration (6.4.3)

5.5.4 Generic Competencies

- Operational
 - Data Privacy and Protection (C014)
 - Organizational Awareness (C037)
 - Policy Management (C038)
- Technical
 - Problem Solving (C040)



5.5.5 Role-Specific Competencies

- Technical
 - Asset and Inventory management (C001)
 - Information Systems and Network Security (C024)
 - Network Management (C033)
 - Operating Systems (C034)
 - Operations Support (C035)
 - Software Testing and Evaluation (C046)
 - System Administration (C048)
 - Systems Integration (C049)
 - Systems Testing and Evaluation (C050)
 - Technology Awareness (C053)

5.6 Role: Malware / Forensic Analyst

This particular role, Malware / Forensic Analyst is another one within the FIRST CSIRT Services
Framework that is relevant to two Service Areas: Information Security Incident Management and
Vulnerability Management. Role descriptions, tasks, functional activities, and competencies as relates
to each service area is listed below separately if applicable.

Some of the general tasks attributed to this role can instead be carried out by another – more specialized – role: Incident Analyst (see section 5.1 on page 22) depending on the local CSIRT context.

5.6.1 Description

As part of the handling of information security incidents or vulnerabilities, digital artefacts may be found on affected systems or malware distribution sites. Artefacts may be the remnants of an intruder attack, such as executables, scripts, files, images, configuration files, tools, tool outputs, logs, live or dormant pieces of code, etc. The Malware / Forensic Analyst will analyze and gain an understanding of such artefacts related to a confirmed information security incident or vulnerability, taking into consideration the need to preserve forensic evidence.

5.6.2 General Tasks

- Conduct Artifact and Forensic Evidence Analysis via different methods (Runtime and Dynamic analysis, Reverse Engineering, Comparative Analysis, Media, and Surface Analysis)
- Analyze malware samples to identify characteristic behavior of the artefacts or compromised systems, how the artefacts or compromised systems establish connectivity with the target or evaded detection
- Conduct vulnerability discovery, relating to incident investigation
- Conduct cross-incident / cross-vulnerability analysis and correlation

5.6.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Information Security Incident Management
 - o Information Security Incident Analysis



- Cross-Incident Correlation (6.2.5)
- o Artifact and Forensic Evidence Analysis
 - Media or Surface Analysis (6.3.1)
 - Reverse Engineering (6.3.2)
 - Runtime or Dynamic Analysis (6.3.3)
 - Comparative Analysis (6.3.4)
- Service Area: Vulnerability Management
 - Vulnerability Discovery/Research
 - Incident Response Vulnerability Discovery (7.1.1)

5.6.4 Generic Competencies

- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
 - Written Communication (C060)
- Technical
 - Problem Solving (C040)

5.6.5 Role-Specific Competencies

- Operational
 - o Data Privacy and Protection (C014)
 - o External Awareness (C019)
 - o Legal, Government, and Jurisprudence (C030)
 - Organizational Awareness (C037)
- Technical
 - o Computer Forensics (C005)
 - Computer Network Defense (C007)
 - Data Analysis (C012)
 - Data Management (C013)
 - Incident Management (C021)
 - Information Systems/Network Security (C024)
 - Information Technology Assessment (C025)
 - Intelligence Analysis (C027)
 - Knowledge Management (C029)
 - Technology Awareness (C053)
 - Threat Analysis (C055)
 - Vulnerabilities Assessment (C057)



6 Service Area: Vulnerability Management

The Vulnerability Management Service Area includes services related to the discovery, analysis, and handling of new or reported security vulnerabilities in information systems. The Vulnerability Management Service Area also includes services related to the detection of and response to known vulnerabilities in order to prevent them from being exploited. Therefore, this service area encompasses services related to both new and known vulnerabilities.

Although the term "vulnerability management" is sometimes used to refer to the process of simply preventing known vulnerabilities from being exploited (e.g., "scan and patch"), in the FIRST CSIRT Services Framework, those activities are considered as functions and sub-functions under a service called Vulnerability Response, which is just one possible service that a CSIRT might provide. For many CSIRTs, those vulnerability response functions are the responsibility of other roles that scan for and remediate security vulnerabilities.

Other roles also may be involved in the discovery of new vulnerabilities: for example, an Incident Analyst (or an Incident Responder) may first learn of a new vulnerability while analyzing or responding to a reported incident; or a Malware / Forensics Analyst may learn of a new vulnerability while analyzing some malware, intruder exploit, or other digital media while conducting their functions.

The following roles are considered to handle particular functions:

- Incident Analyst *)
- IT Security Administrator
- Malware/Forensic Analyst **)
- Vulnerability Analyst
- Vulnerability Assessment Analyst
- Vulnerability Coordinator
- Vulnerability Disclosure Coordinator
- Vulnerability Researcher
- Vulnerability Triage Coordinator
- *) The role Incident Analyst is also instrumental for the Service Area: Information Security Incident Management. Please refer for all further details regarding this role to section 5.2 Role: Incident Analyst on page 24.
 - **) The role Malware/Forensic Analyst is also instrumental for the Service Area:
 Information Security Incident Management. Please refer for all further details regarding this role to section o Software Testing and Evaluation (C046)
 - System Administration (C048)
 - Systems Integration (C049)
 - Systems Testing and Evaluation (C050)
 - Technology Awareness (C053)

Role: Malware / Forensic Analyst on page 31.



6.1 Role: IT Security Administrator

For an internal CSIRT – especially if it is only be built in an ad-hoc fashion to respond to an information security incident – an Information Technology (IT) Administrator might become part of the CSIRT. In most other contexts most notably for coordinating CSIRTs or national CSIRTs, the functions identified in the FIRST CSIRT Services Framework to restore compromised systems etc. are carried out by the owner, not by the CSIRT that informed the owner of any such information security incident.

Therefore, we are providing here the same information as for other roles within the context of the FIRST CSIRT Services Framework, but do not expect that a CSIRT will implement such role internally, except it has a real need – participating in the response and mitigation as part of the services offered to the constituents.

6.1.1 Description

The Information Technology (IT) Security Administrator will remediate or mitigate vulnerabilities to prevent them from being exploited, typically through the timely application of vendor-provided patches or other solution.

6.1.2 General Tasks

- Deploy and install vendor-provided solutions in the form of software updates or patches.
- Apply alternative mitigation or workaround as a countermeasure to prevent exploitation of the vulnerability when patches are unavailable or cannot be deployed.

6.1.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Vulnerability Management
 - Vulnerability Response
 - Vulnerability Remediation (7.6.2)

6.1.4 Generic Competencies

- Professional
 - Critical Thinking (C011)
- Operational
 - Data Privacy and Protection (C014)
 - Policy Management (C038)
- Technical
 - Problem Solving (C040)

6.1.5 Role-Specific Competencies

- Operational
 - Business Continuity (C002)
- Technical
 - Asset and Inventory management (C001)
 - Computer Network Defense (C007)

Improving Security Together

Forum of Incident Response and Security Teams

- Information Assurance (C022)
- Information Systems and Network Security (C024)
- Network Management (C033)
- Operating Systems (C034)
- Operations Support (C035)
- Software Testing and Evaluation (C046)
- System Administration (C048)
- Systems Integration (C049)
- Systems Testing and Evaluation (C050)
- Technology Awareness (C053)

6.2 Role: Vulnerability Analyst

6.2.1 Description

The Vulnerability Analyst will analyze information received or obtained from various sources regarding a suspected vulnerability and attempt to gain a better understanding of the vulnerability. Vulnerability information may be received from vulnerability researchers, incident responders, public sources, or other third-party sources.

6.2.2 General Tasks

- Learn about a new vulnerability from reading public sources or other third-party sources.
- Categorize, prioritize, and perform an initial assessment of a vulnerability.
- Understand the design or implementation flaw that causes or exposes the vulnerability to exist.
- Develop the steps necessary to fix (remediate) the underlying vulnerability or mitigate (reduce) the effects of the vulnerability from being exploited.
- Document the vulnerability analysis findings or results.

6.2.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Vulnerability Management
 - Vulnerability Discovery/Research
 - Public Source Vulnerability Discovery (7.1.2)
 - o Vulnerability Analysis
 - Vulnerability Root Cause Analysis (7.3.2)
 - Vulnerability Remediation Development (7.3.3)

6.2.4 Generic Competencies

- Professional
 - o Critical Thinking (C011)
 - Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational



- Business Continuity (C002)
- Technical
 - o Problem Solving (C040)

6.2.5 Role-Specific Competencies

- Operational
 - Data Privacy and Protection (C014)
 - o External Awareness (C019)
 - Risk Management (C044)
- Technical
 - Asset and Inventory Management (C001)
 - Computer Forensics (C005)
 - Computer Network Defense (C007)
 - Data Analysis (C012)
 - Data Management (C013)
 - Information Assurance (C022)
 - Intelligence Analysis (C027)
 - Knowledge Management (C029)
 - Technology Awareness (C053)
 - Threat Analysis (C055)
 - Vulnerabilities Assessment (C057)

6.3 Role: Vulnerability Assessment Analyst

6.3.1 Description

The Vulnerability Assessment Analyst will actively search for the presence of known vulnerabilities in deployed systems.

6.3.2 General Tasks

- Conduct vulnerability scanning and/or hunting.
- Conduct vulnerability security assessments and/or penetration testing.
- Analyze the results vulnerability assessments or penetration tests.
- Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
- Conduct and/or support authorized penetration testing on enterprise network assets.
- Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.
- Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.
- Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.



- Prepare audit reports that identify technical and procedural findings and provide recommended remediation strategies/solutions.
- Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).
- Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes).

6.3.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Vulnerability Management
 - o Vulnerability Response
 - Vulnerability Detection/Scanning (7.6.1)

6.3.4 Generic Competencies

- Professional
 - Critical Thinking (C011)
 - Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational
 - o Business Continuity (C002)
- Technical
 - o Problem Solving (C040)

6.3.5 Role-Specific Competencies

- Operational
 - Client Relationship Management (C003)
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Policy Management (C038)
 - Risk Management (C044)
- Technical
 - Asset and Inventory Management (C001)
 - Data Analysis (C012)
 - Data Management (C013)
 - Information Assurance (C022)
 - Intelligence Analysis (C027)
 - Knowledge Management (C029)
 - Technology Awareness (C053)
 - Threat Analysis (C055)



Vulnerabilities Assessment (C057)

6.4 Role: Vulnerability Coordinator

6.4.1 Description

The Vulnerability Coordinator notifies, works with, and coordinates the exchange of relevant information with multiple parties in the coordinated vulnerability disclosure (CVD)¹¹ process, including the vulnerability finders/researchers, affected vendors, developers, PSIRTs, or other trusted experts (e.g., other researchers, CSIRTs, and vulnerability coordinators) who can work together to analyze and fix a vulnerability.

The Vulnerability Coordinator coordinates the exchange of information among the participants in the CVD efforts to analyze and fix the vulnerability and prepare for the disclosure of the vulnerability. This coordination should include agreement by participants on the timing and synchronization of the disclosure.

6.4.2 General Tasks

- Exchange information and coordinate the activities with participants involved in a coordinated vulnerability disclosure (CVD) process.
- Report new vulnerability information with others who are to be involved in the CVD process.
- Conduct follow-on coordination and sharing of information among the various stakeholders and participants involved in the CVD efforts.
- Help connect researchers, vendors, and other stakeholders. This is particularly helpful when multiple parties/vendors are involved or there is difficultly contacting a party/vendor.
- Provide additional technical, impact, and scope analysis to researchers, vendors, and other stakeholders, particularly when there is disagreement.
- Develop and maintain awareness of and relationships with other coordinators.

6.4.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Vulnerability Management
 - Vulnerability Coordination
 - Vulnerability Notification/Reporting (7.4.1)
 - Vulnerability Stakeholder Coordination (7.4.2)

6.4.4 Generic Competencies

- Leadership
 - Strategic Planning (C047)
 - Teaching Others (C052)
 - Workforce Management (C059)
- Professional
 - Conflict Management (C009)

https://www.first.org/global/sigs/vulnerability-coordination/



- Critical Thinking (C011)
- o Interpersonal Skills (C026)
- Oral Communication (C036)
- Presenting Effectively (C039)
- Written Communication (C060)
- Organizational
 - Organizational Awareness (C037)
- Technical
 - Problem Solving (C040)

6.4.5 Role-Specific Competencies

- Operational
 - Client Relationship Management (C003)
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Policy Management (C038)
 - Risk Management (C044)
- Technical
 - Data Analysis (C012)
 - Information Assurance (C022)
 - Intelligence Analysis (C027)
 - Knowledge Management (C029)
 - o Requirements Analysis (C043)
 - Technology Awareness (C053)
 - Threat Analysis (C055)
 - Vulnerabilities Assessment (C057)

6.5 Role: Vulnerability Disclosure Coordinator

6.5.1 Description

The Vulnerability Disclosure Coordinator will help the organization to define their vulnerability disclosure policy and make that policy available to its constituents, stakeholders, and CVD participants, preferably by publishing it on the CSIRT's website. The Vulnerability Disclosure Coordinator will also help the organization to define, maintain, and update the processes and procedures that support the handling of vulnerabilities that are reported under the vulnerability disclosure policy.

The Vulnerability Disclosure Coordinator will disclose vulnerability information to defined constituents. The disclosure can be made through any or all of the mechanisms identified in the vulnerability disclosure policy. Dissemination mechanisms can vary depending on the needs or expectations of the

See the Vulnerability Disclosure Coordinator role for further information about 7.5.1 Function: Vulnerability disclosure policy and infrastructure maintenance.

FIRST

Forum of Incident Response and Security Teams

target audience. The communication can be in the form of an announcement or security advisory distributed via email or text messaging, a publication posted to a website or social media channel, or other communication forms and channels as appropriate.

The Vulnerability Disclosure Coordinator will also review follow-on communications or questions received from constituents about a vulnerability document. The questions may indicate a need for clarification, revision, or amendment of the vulnerability disclosure mechanism. Information from constituents may simply be an acknowledgement or receipt of the vulnerability document, or the constituent may report an issue or difficulty in deploying the suggested remediation/mitigation.

6.5.2 General Tasks

- Develop, publish, and maintain a policy that provides a framework and sets expectations for how a CSIRT handles and discloses vulnerabilities and the mechanism(s) used to disclose the vulnerability.
- Develop or update existing processes and procedures that support the implementation of the vulnerability disclosure policy and the handling (acknowledgement, triage, analysis, remediation, and resolution) of reported vulnerabilities within target timelines.
- Communicate and share information with other stakeholders (vulnerability reporters, internal stakeholders, service providers, vendor product security incident response teams [PSIRTs], etc.) in support of the vulnerability disclosure policy, processes, and procedures.
- Provide information to constituents (or the public) about a new vulnerability, so that they can detect, remediate or mitigate, and prevent future exploitation of a vulnerability.
- Coordinate the disclosure of vulnerability information.
- Receive and respond to questions or reports from constituents about a vulnerability disclosure or document.

6.5.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Vulnerability Management
 - Vulnerability Disclosure
 - Vulnerability Disclosure Policy and Infrastructure Maintenance (7.5.1)
 - Vulnerability Announcement/Communication/Dissemination (7.5.2)
 - Post-Vulnerability Disclosure Feedback (7.5.3)

6.5.4 Generic Competencies

- Leadership
 - Strategic Planning (C047)
 - Teaching Others (C052)
 - Workforce Management (C059)
- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
 - Interpersonal Skills (C026)
 - o Oral Communication (C036)

Improving Security Together

Forum of Incident Response and Security Teams

- Presenting Effectively (C039)
- Written Communication (C060)
- Organizational
 - Organizational Awareness (C037)
- Technical
 - o Problem Solving (C040)

6.5.5 Role-Specific Competencies

- Operational
 - Client Relationship Management (C003)
 - Data Privacy and Protection (C014)
 - o External Awareness (C019)
- Technical
 - Data Analysis (C012)
 - o Intelligence Analysis (C027)
 - Knowledge Management (C029)
 - o Requirements Analysis (C043)

6.6 Role: Vulnerability Researcher

6.6.1 Description

The Vulnerability Researcher will find, learn of, or search for new, previously unknown vulnerabilities, as a result of deliberate CSIRT activities or research.

The Vulnerability Researcher may discover or search for new vulnerabilities as a result of specific activities or research, such as the testing of systems or software using fuzz testing (fuzzing), or through the reverse engineering of malware.

6.6.2 General Tasks

- Discover new vulnerabilities as a result of specific activities, such as fuzz testing or through the reverse engineering of malware.
- Look for suspected vulnerabilities in response to input received from the Information Security Incident Management service area or the Situational Awareness service area.

6.6.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Vulnerability Management
 - Vulnerability Discovery/Research
 - Vulnerability Research (7.1.3)

6.6.4 Generic Competencies

- Professional
 - Critical Thinking (C011)
 - Oral Communication (C036)

Improving Security Together

Forum of Incident Response and Security Teams

- Presenting Effectively (C039)
- Written Communication (C060)
- Operational
 - Business Continuity (C002)
- Technical
 - o Problem Solving (C040)

6.6.5 Role-Specific Competencies

- Operational
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Risk Management (C044)
- Technical
 - Computer Forensics (C005)
 - o Computer Network Defense (C007)
 - Data Analysis (C012)
 - Information Assurance (C022)
 - Intelligence Analysis (C027)
 - Knowledge Management (C029)
 - o Requirements Analysis (C043)
 - Technology Awareness (C053)
 - Threat Analysis (C055)
 - Vulnerabilities Assessment (C057)

6.7 Role: Vulnerability Triage Coordinator

6.7.1 Description

The Vulnerability Triage Coordinator will accept or receive and appropriately process vulnerability information reported from constituents or third parties. The Vulnerability Triage Coordinator will initially review, categorize, prioritize, and process a vulnerability report.

6.7.2 General Tasks

- Accept or receive information about a vulnerability, as reported from constituents or third parties.
 - Monitor communications channels regularly, and check whether the advertised means of contacting the CSIRT are operational, and reports can be submitted.
 - Report initial acknowledgement to the submitter of the vulnerability report, request additional information if needed, and set expectations with the reporter.
- Initially review, categorize, prioritize, and process a vulnerability report.
 - Process reports and submitted data including artefacts or materials in isolation to protect
 the integrity of the working environment and avoid successful attacks on the CSIRT by such
 means.



- Update acknowledgement of reports by providing some feedback on further steps based on categorization or prioritization results available.
- Merge new information about a vulnerability already being handled with the available data to allow consistent analysis and processing.
- Categorize, prioritize, and perform an initial assessment of a vulnerability.

6.7.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Vulnerability Management
 - o Vulnerability Report Intake
 - Vulnerability Report Receipt (7.2.1)
 - Vulnerability Report Triage and Processing (7.2.2)
 - Vulnerability Analysis
 - Vulnerability Triage (Validation and Categorization) (7.3.1)

6.7.4 Generic Competencies

- Leadership
 - Strategic Planning (C047)
 - Teaching Others (C052)
 - Workforce Management (C059)
- Professional
 - Critical Thinking (C011)
 - Interpersonal Skills (C026)
 - o Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Organizational
 - Organizational Awareness (C037)
- Technical
 - Problem Solving (C040)

6.7.5 Role-Specific Competencies

- Operational
 - Client Relationship Management (C003)
 - Data Privacy and Protection (C014)
 - o External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Policy Management (C038)
 - o Risk Management (C044)
- Technical
 - Data Analysis (C012)
 - Information Assurance (C022)
 - Intelligence Analysis (C027)



- Knowledge Management (C029)
- o Requirements Analysis (C043)
- o Technology Awareness (C053)
- Threat Analysis (C055)
- Vulnerabilities Assessment (C057)



7 Service Area: Situational Awareness

Situational Awareness comprises the ability to identify, process, comprehend, and communicate the critical elements of what is happening in and around the CSIRT's area of responsibility that may affect the operation or mission of its constituency. Situational awareness includes being aware of the current state and identifying or anticipating potential changes to that state. This service area includes determining how to gather relevant information from different areas, how to integrate that information, and how to disseminate it in a timely manner to help constituents make more informed decisions. Some organizations may establish a separate team to provide Situational Awareness, but for others, the CSIRT team provides this function based on its visibility, understanding of context, technical capabilities, access to assets, external connections, and mission to prevent incidents. Situational awareness is not solely focused on responding to incidents, it is a service that ensures that data, analysis, and actions are available to other services such as Security Event Management, Incident Management, and Knowledge Transfer. It also ensures that information coming from those other services areas is properly integrated together and delivered back to appropriate constituents in a timely manner.

The following roles are considered to handle particular functions:

- Communication Liaison *)
- Risk Analyst including Risk & Continuity Advisor
- Situational Awareness Data Analyst
- Situational Awareness Manager
- Threat Warning Analyst

*) The role Communication Liaison is also instrumental for the Service Area: Information Security Incident Management. Please refer for all further details regarding this role to section 5.1 Role: Communication Liaison on page 22.

7.1 Role: Risk & Continuity Advisor / Risk Analyst

This particular role, Risk & Continuity Advisor/Risk Analyst (referred to as "Risk Analyst" for the rest of this document) is one within the FIRST CSIRT Services Framework that is relevant to two Service Areas: Situational Awareness and Knowledge Transfer. Role descriptions, tasks, functional activities, and competencies as relates to each service area is listed below separately if applicable.

Please note, that the role of a Risk Analyst / Risk & Continuity Advisor is also applicable within the Knowledge Transfer service area.

7.1.1 Description

The risk analyst is responsible for collecting and understanding the information about current and expected future status of constituency assets and activities. This includes collecting information on

- Legitimate users of internal and public facing systems and devices
- Authorized devices and what they are used for



 Approved processes and applications, where they are allowed, and how they serve the constituency

This information is used to create an asset map or inventory, highlighting functions, roles, permissible actions and key risks related to critical assets. It can also be used to identify risks to key assets and prioritize both the assets and the risks to be addressed. This information along with the baselines and environmental context defined by the situational awareness manager can be used to help define situational awareness needs and requirements. This information provides context and baselines for analysis and response functions in the Service Areas of Information Security Event Management and Information Security Incident Management.

7.1.2 General Tasks

- Collect data regarding organizational or constituency assets as an inventory that includes the functions and roles that support the assets; along with key risks to the assets and supporting functions
- Collect data regarding what is allowable activities for the assets and what is anomalous
- Communicate assets and corresponding risk or compliance posture to stakeholders
- Advise and support constituency to improve their risk management process, covering risks and threats identification, and selection of relevant risk management options
- Based on identified risks, advise and support constituency in the activities related to organizational resilience and implementation of the business continuity and disaster recovery plans
- Advise constituency on conducting an actual risk assessment
- Provide support to evaluate the results of a risk assessment

7.1.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Situational Awareness
 - Data Acquisition
 - Asset mapping to functions, roles, actions, and key risks (8.1.2)
- Service Area: Knowledge Transfer
 - o Technical and Policy Advisory
 - Risk Management Support (9.4.1)
 - Business Continuity and Disaster Recovery Planning (9.4.2)

7.1.4 Generic Competencies

- Leadership
 - Strategic Planning (C047)
 - Teaching Others (C052)
- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
 - o Interpersonal Skills (C026)
- Operational
 - Client Relationship Management (C003)



- Technical
 - o Problem Solving (C040)

7.1.5 Role-Specific Competencies

- Professional
 - o Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational
 - Business Continuity (C002)
 - Data Privacy and Protection (C014)
 - o External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Organizational Awareness (C037)
 - Policy Management (C038)
 - Risk Management (C044)
- Technical
 - Computer Network Defense (C007)
 - Incident Management (C021)
 - Information Assurance (C022)
 - Information Management (C023)
 - Information Systems and Network Security (C024)
 - Information Technology Assessment (C025)
 - Knowledge Management (C029)
 - o Requirements Analysis (C043)
 - Technology Awareness (C053)
 - Threat Analysis (C055)
 - Vulnerabilities Assessment (C057)

7.2 Role: Situational Awareness Data Analyst

7.2.1 Description

Situational Awareness Data Analysts collect security and context data from different data sources. Sources of security event information include data from Network Flow, Network Packets, Network Packet Inspection Results, Intrusion Detection, Digital Artifacts, Security Analysis of Digital Artifacts (such as a sandbox), Database logs, Virtual Private Network (VPN), Cloud hosting, User Host logs and more. Sources of business context event data include user interviews, spreadsheets, documents, communications, calendars, databases, transactions, images, and services. The data analyst assembles security and other data types into a centralized source for future analysis. This may require them to manage, tag, mark or otherwise label the security data. In larger organizations they may also work with a data lake and/or data warehouse. The size of the data involved may sometimes grow very large, and thus may require skills working with "big data" frameworks.

FIRST

Forum of Incident Response and Security Teams

Analysts will also design methods to repeatably and reliably fuse the data into informational insights by running queries and using the results to improve collection, analysis or awareness. Analysts will examine their results and compare them against established baselines. They will also communicate their results via a variety of different methods include presentations, visualizations, application systems, and written documents. They may also use tools, methods, programs, or scripts to make parts or all of the data available as a service to other parts of the organization.

7.2.2 General Tasks

- Repeatably collect and clean data of different types with a heavy focus on cybersecurity.
- Establish repeatably data processing that transform and integrate data into a centralized store for further analysis.
- Perform analysis of collected data to identify situations that do not match expectations, report trends, or warn of future issues.
- Create and run experiments that measure analysis processes and improve them to run efficiently (reduce query times, improve algorithm efficiency etc.)
- Create and communicate future situational pictures based upon analysis of collected data

7.2.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Situational Awareness
 - Data Acquisition
 - Collection (8.1.3)
 - Data Processing and Preparation (8.1.4)
 - Analysis and Synthesis
 - Projection and Inference (8.2.1)

7.2.4 Generic Competencies

- Professional
 - Critical Thinking (C011)
 - o Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Technical
 - Problem Solving (C040)

7.2.5 Role-Specific Competencies

- Operational
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Organizational Awareness (C037)
- Technical
 - Computer Network Defense (C007)
 - Data Analysis (C012)



- Data Management (C013)
- o Information Management (C021)
- Information Assurance (C022)
- Information Systems and Network Security (C024)
- Information Technology Assessment (C025)
- Intelligence Analysis (C027)
- Knowledge Management (C029)
- Technology Awareness (C053)
- Threat Analysis (C055)

7.3 Role: Situational Awareness Manager

7.3.1 Description

The situational awareness manager will research and establish the basic environment which in the organization functions, to ensure the proper context is set for what type of situational awareness materials are needed and should be collected. The situational awareness manager basically is responsible for understanding and establishing the normal operating conditions or baselines for the organization, its related stakeholders, and constituency. This includes collection, analysis, creation, of policy and situational data from various internal and external sources. They will also manage the distribution of products that provide context and visibility into current situational concerns (for example security trends or incident trends) across various disciplines, organizational silos, groups, or teams.

7.3.2 General Tasks

- Collect policy, event, trend, and future planning data from internal and external sources
- Oversee and verify establishment of normal cyber activity baselines and operational event thresholds
- Communicate baseline contexts and acceptable conditions to stakeholders
- Review intelligence products

7.3.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Situational Awareness
 - Data Acquisition
 - Policy Aggregation, Distillation and Guidance (8.1.1)

7.3.4 Generic Competencies

- Leadership
 - Strategic Planning (C047)
- Professional
 - Critical Thinking (C011)
 - o Interpersonal Skills (C028)
 - o Oral Communication (C036)

Improving Security Together

Forum of Incident Response and Security Teams

- Presenting Effectively (C039)
- Written Communication (C060)
- Technical
 - Problem Solving (C040)

7.3.5 Role-Specific Competencies

- Operational
 - Client Relationship Management (C003)
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Organizational Awareness (C037)
 - Policy Management (C038)
 - o Risk Management (C044)
- Technical
 - Asset and Inventory Management (C001)
 - Computer Network Defense (C007)
 - Data Analysis (C012)
 - Data Management (C013)
 - Information Management (C021)
 - Information Assurance (C022)
 - Information Systems and Network Security (C024)
 - Information Technology Assessment (C025)
 - Intelligence Analysis (C027)
 - Knowledge Management (C029)
 - Operations Support (C035)
 - Requirements Analysis (C043)
 - Technology Awareness (C053)
 - Threat Analysis (C055)

7.4 Role: Threat Warning Analyst

7.4.1 Description

A Threat Warning Analysts provide their organizations with insights into threat behaviors, current activity, and the potential impacts they have upon general and specific current and future operational situations. This analyst collects data to assemble a picture of threat activity supported by evidence. Such analysts may search for events or evidence of warning signs that an attack has arrived, is on its way, or that the conditions in the infrastructure will allow an attack to succeed. The analyst works with other organizations to determine what threats they are experiencing and to share information with their communities. They will create reports and communicate findings to both internal and external audiences on the analysis results and on recommended actions.

Improving Security Together

Forum of Incident Response and Security Teams

7.4.2 General Tasks

- Collect data from internal and external source to establish trends in threat behavior
- Analyze internal and external data to identify warnings
- Aggregate threat warnings and identify potential impacts on organizational infrastructure or activities.
- Use common data formats, data transmission protocols, data models, tools, taxonomies, rules, and platforms to send and receive cyber security and cyber threat warning related data.
- Communicate and deliver key findings to constituent audiences

7.4.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Situational Awareness
 - o Analysis and Synthesis
 - Event detection (through alerting and/or hunting) (8.2.2)
 - Information Security Incident Management Decision Support (8.2.3)
 - Situational Impact (8.2.4)
 - Service Communication
 - Internal and external communication (8.3.1)
 - Reporting and recommendations (8.3.2)
 - Implementation (8.3.3)

7.4.4 Generic Competencies

- Professional
 - Critical Thinking (C011)
 - o Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational
 - Business Continuity (C002)
 - Legal, Government, and Jurisprudence (C030)
- Technical
 - o Problem Solving (C040)

7.4.5 Role-Specific Competencies

- Operational
 - Data Privacy and Protection (C014)
 - o External Awareness (C019)
 - Organizational Awareness (C037)
 - Risk Management (C044)
- Technical
 - Computer Network Defense (C007)
 - Data Analysis (C012)
 - Data Management (C013)
 - Incident Management (C021)



- o Information Assurance (C022)
- o Information Systems and Network Security (C024)
- Information Technology Assessment (C025)
- o Intelligence Analysis (C027)
- o Knowledge Management (C029)
- Operations Support (C035)
- o Requirements Analysis (C043)
- o Technology Awareness (C053)
- o Threat Analysis (C055)



8 Service Area: Knowledge Transfer

Through the nature of their services CSIRTs, are in a unique position to collect relevant data, perform detailed analysis, and identify threats, trends, and risks, as well as to create best current operational practices to help organizations to detect, prevent, and respond to security incidents. Transferring this knowledge to their constituents is key to improving overall cybersecurity.

The following roles are considered to handle particular functions:

- Awareness Coordinator
- Policy Advisor
- Risk & Continuity Advisor *)
- Staff Developer
- Technical Policy Advisor
- Training Developer
- Training Instructor

8.1 Role: Awareness Coordinator

8.1.1 Description

The Awareness Coordinator works with the constituency, experts and trusted partners to raise the collective understanding of threats and actions that can be taken to prevent or mitigate the risks posed by these threats.

The Awareness Coordinator builds partnerships and promotes cooperation helping CSIRT to better understand constituents' needs and enabling fulfillment of CSIRT's mission.

8.1.2 General Tasks

- Build partnerships, promote cooperation, and engage the key stakeholders, internal or external to the constituency
 - helping the CSIRT to better understand constituents' needs and enabling fulfillment of CSIRT's mission.
 - helping the constituency and external stakeholders understand the services and benefits a CSIRT can provide.
- Communicate with the constituency and rise their awareness of:
 - events, activities, and trends that may affect their ability to operate in a timely and secure manner
 - o steps to take to detect, prevent and mitigate threats and malicious activity
 - security and operational best practices

^{*)} The role as Risk & Continuity Advisor (referred to as "Risk Analyst" in this document) is also instrumental for the Service Area: Situational Awareness. Please refer for all further details regarding this role to section 7.1 Role: Risk & Continuity Advisor / Risk Analyst on page 45.



- Research and aggregate information relevant for building awareness materials and reports, including from outcomes of other services/functions, especially from the Security Event Management, Incident Management, and Situational Awareness service areas.
- Develop materials for diverse audiences (technical staff, management, end users, etc.) and in various formats, such as presentations, short videos, cartoons, booklets, technical analysis, trend reports, and periodical reports, utilizing varied and effective delivery techniques and platforms.
- Implement and coordinate the process of information dissemination, based on the characteristics of different audiences and content.

8.1.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Knowledge Transfer
 - Awareness Building
 - Research and Information Aggregation (9.1.1)
 - Report and Awareness Materials Development (9.1.2)
 - Information Dissemination (9.1.3)
 - Outreach (9.1.4)

8.1.4 Generic Competencies

- Leadership
 - Teaching Others (C052)
- Professional
 - Interpersonal Skills (C026)
- Operational
 - Data Privacy and Protection (C014)
- Technical
 - o Problem Solving (C040)

8.1.5 Role-Specific Competencies

- Leadership
 - Teaching Others (C052)
- Professional
 - o Written Communication (C060)
 - Oral Communication (C036)
 - Presenting Effectively (C039)
- Operational
 - Client Relationship Management (C003)
 - External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Organizational Awareness (C037)
 - Policy Management (C038)
- Technical
 - o External Awareness (C019)



- Knowledge Management (C029)
- o Requirements Analysis (C043)
- Technology Awareness (C053)
- Threat Analysis (C055)

8.2 Role Name: Policy Advisor

8.2.1 Description

The Policy Advisor works with the CSIRT constituency and key stakeholders, internal or external to the constituency, in contributing to the creation and implementation of the constituency's policies.

8.2.2 General Tasks

- In Internal CSIRT team¹³
 - support the constituency in the development, maintenance, institutionalization, and enforcement of information security and other operating policies, based on operational security best practices that incorporate business continuity and disaster recovery best practices,
 - ensure that implemented policies enable and support incident management activities.
 Promote including incident management teams, as trusted advisors, in business decisions where appropriate.
- In coordinating and national CSIRTs team
 - o support for public policies and new legislation,
 - legitimizing the services of a CSIRT,
 - o implementing CSIRT internal policies.

8.2.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Knowledge Transfer
 - Technical and Policy Advisory
 - Policy Support (9.4.3)

8.2.4 Generic Competencies

- Leadership
 - Teaching Others (C052)
- Professional
 - Critical Thinking (C011)
- Operational

As there are well-established distinctions between various "types" of teams, e. g. coordinating CSIRTs, national CSIRTs, internal CSIRT, the priorities and the importance of competencies for each role will also be different. It is obvious, that the same role in different types of teams can also implemented differently based on a decision to combine tasks or functions in a team-specific way. For now, no effort

was made to recommend or present roles for specific "types" of teams. But for this role we found that there is such a big difference in the task objectives that we wanted to point this out, as it will also have an impact on the chosen competencies.



- Client Relationship Management (C003)
- Data Privacy and Protection (C014)

8.2.5 Role-Specific Competencies

- Leadership
 - Strategic Planning (C047)
 - Workforce Management (C059)
- Professional
 - Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational
 - External Awareness (C019)
 - Legal, Government, and Jurisprudence (C030)
 - Policy Management (C038)
 - Risk Management (C044)
- Technical
 - Information Assurance (C022)
 - Knowledge Management (C029)
 - o Requirements Analysis (C043)
 - Technology Awareness (C053)
 - Threat Analysis (C055)
 - Vulnerabilities Assessment (C057)

8.3 Role: Staff Developer

8.3.1 Description

The Staff Developer works in close relationship with experienced staff to identify knowledge gaps, training needs and to develop CSIRT staff, constituency members, or external trusted partners' employee skills.

To promote a continuous process of securing new knowledge, skills, and abilities the Staff Developer identifies appropriate skillset and supports staff professional development, based on job responsibilities, individual needs, and the overall Team environment.

To support development of trusted relationships the Staff Developer leads mentoring program by coordinating mentor-mentee activities and providing a formal guideline for mentoring process, as well informing about informal mechanisms for information sharing, skill development, insights, and life and career experiences outside of the official reporting relationship and structure of the team.

8.3.2 General Tasks

• Identify staff members training needs to develop appropriate skills and abilities, unique job responsibilities, and the overall Team environment



- Collect and distribute information about opportunities attending conferences, advanced training, and cross-training activities, both soft skills (e.g. collaboration, information sharing, presentation) and technical skills (e.g. certification programs, tools and technology, privacy concepts)
- Initiate development of internal training courses in close collaboration with #2 Training Developer
- Develop mentoring program and coordinate the activities with participants (mentor-mentee) involved in a program
- Provide a formal guideline for the mentoring process
- Support mentoring program participants with training needed to inspire information sharing and develop a needed knowledge base
- Conduct follow-on coordination and sharing of information among the various stakeholders and participants involved in training and mentoring processes

8.3.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Knowledge Transfer
 - Training and Education
 - Mentoring (9.2.4)
 - CSIRT Staff Professional Development (9.2.5)

8.3.4 Generic Competencies

- Leadership
 - Strategic Planning (C047)
- Professional
 - Conflict Management (C009)
 - Critical Thinking (C011)
 - Interpersonal Skills (C028)
 - Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Technical
 - Problem Solving (C040)

8.3.5 Role-Specific Competencies

- Operational
 - Data Privacy and Protection (C014)
 - Organizational Awareness (C037)
- Technical
 - Data management (C013)
 - Knowledge Management (C029)



8.4 Role: Technical Policy Advisor

8.4.1 Description

The Technical Policy Advisor ensures the constituency's policies and procedures include appropriate incident management considerations and, ultimately, enable the constituency to better manage risks and threats, and implement current operational and security best practices, while enabling effective incident handling activities.

The Technical Policy Advisor supports the CSIRT constituency and key stakeholders, providing technical advice and recommendations for the improvement of cybersecurity related infrastructures, tools, and services and contributing to the creation and implementation of technical policies, with the goal of improving the security posture and incident management overall.

8.4.2 General Tasks

- Define and review the framework of means required to carry out incident response activities, whether they are part of the day-to-day activity of the CSIRT or the management of a large-scale crisis
- Write and review technical and escalation procedures followed by incident responders
- Define and review service level agreements for incident response
- Conduct incident retrospectives and ensure continuous improvement of the CSIRT processes
- Conduct regular CSIRT maturity self-assessment and peer reviews
- Help Training Developer and Training Instructor write and keep exercise scenarios up to date
- Help incident responders classify and prioritize operations
- Help other teams to build and implement a common taxonomy
- Define and review policies for data encryption, password, communication, and network security
- Maintain written documentation of best practices
- Establish internal communication to raise awareness
- Measure and improve adoption of recommendations

8.4.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Knowledge Transfer
 - o Technical and Policy Advisory
 - Technical Advice (9.4.4)

8.4.4 Generic Competencies

- Professional
 - Critical Thinking (C011)
 - o Interpersonal Skills (C028)
 - Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational
 - Client Relationship Management (C003)



- Legal, Government, and Jurisprudence (C030)
- Risk Management (C044)
- Technical
 - Problem Solving (C040)

8.4.5 Role-Specific Competencies

- Operational
 - Business Continuity (C002)
 - Data Privacy and Protection (C014)
 - Policy Management (C038)
- Technical
 - Incident Management (C021)
 - Information Assurance (C022)
 - Information Systems and Network Security (C024)
 - Information Technology Assessment (C025)
 - Knowledge Management (C029)
 - o Requirements Analysis (C043)

8.5 Role: Training Developer

8.5.1 Description

The Training Developer's role is to develop training, education and exercises – primarily for the CSIRT's constituency, but also for internal use, especially in bigger teams. Trainings/education/exercises developed can range all the way from policy and organizational to deeply technical and operational. This very wide scope will necessarily be beyond the scope of one Training Developer, and therefore an important part of this role is also to liaise with other experts in (and possibly outside) the team – and, if existent, with co-developers – in order to work together on scoping and creating training, education and exercises.

8.5.2 General Tasks

- Gather requirements for training, education and exercises this can be requirements in the areas of awareness, knowledge, skills, abilities, and more
- Analyze such requirements and develop high-level plans for training, education, and exercises
- Discuss such plans inside the CSIRT (and if necessary, beyond, e.g., with the constituency), refine them, and set up a course of action
- Develop training, education and exercises based on such plans and courses of action or oversee the development when other CSIRT experts do the development, or when it is subcontracted
- Development (or oversight thereof) includes proper scoping, developing formats, defining the
 environment, developing training materials of all kinds (possibly including audio, video, games,
 pre-work, post-work and much more), develop scenarios, hands-on workshops, etcetera
- Develop outcome criteria for training, education, and exercises and ways of gauging these outcomes (e. g. evaluation, interviews, tests, exams, etcetera)
- Work together with other relevant roles in this process.



8.5.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Knowledge Transfer
 - Training and Education
 - Knowledge, Skill, and Ability Requirements Gathering (9.2.1)
 - Educational and Training Materials Development (9.2.2)
 - o Exercises
 - Requirements Analysis (9.3.1)
 - Format and Environment Development (9.3.2)
 - Scenario Development (9.3.3)
 - Exercise Outcome Review (9.3.5)

8.5.4 Generic Competencies

- Leadership
 - o Strategic Planning (C047)
- Professional
 - Critical Thinking (C011)

8.5.5 Role-Specific Competencies

- Leadership
 - Teaching Others (C052)
- Professional
 - Oral Communication (C036)
 - Presenting Effectively (C039)
 - Written Communication (C060)
- Operational
 - Client Relationship Management (C003)
 - External Awareness (C019)
 - Organizational Awareness (C037)
- Technical
 - Incident Management (C021)
 - Information Systems and Network Security (C024)
 - o Information Technology Assessment (C025)
 - Knowledge Management (C029)
 - o Requirements Analysis (C043)
 - Technology Awareness (C053)

8.6 Role: Training Instructor

8.6.1 Description

The Training Instructor's role is to deliver training, education, and exercises – primarily for the CSIRT's constituency, but also for internal use, especially in bigger teams. Trainings/education/exercises can range all the way from policy and organizational to deeply technical and operational. This very wide scope will necessarily be beyond the scope of one or two Training Instructors, and therefore in most

FIRST.

Forum of Incident Response and Security Teams

CSIRTs it is likely that people in various other roles (experts of all kinds, managers) in the team also have the role of Training Instructor, in the area of their expertise(s). Bigger teams may also have one or two full time Training Instructors.

8.6.2 General Tasks

- Prepare the execution of a given training, education, or exercise, based on existing materials and format
 - Prepare the environment/logistics usually in cooperation with logistics people, but the Training Instructor needs to set the format and requirements (room, seating arrangement, AV, breaks, etcetera)
 - Prepare the students (pre-work, etcetera)
 - In case of a bigger exercise, do all preparations needed in order to make sure that at delivery time the scenario(s) can be played out well
 - Shortly before the event, double-check all boundary conditions if possible, test
- Deliver the training, education, or exercise
 - Creating a safe environment for students and instructors
 - Catering for the needs of all types of learners
 - Ensuring a proper balance between theory and practice (what the balance is, depends on the topic)
- Gauge the outcomes of the training based on the criteria and methods defined for that
 - If necessary, the Training Instructor adds their own evaluation
- Communicate lessons learnt with the Training Developer(s) and with fellow Training Instructors
- Work together with other relevant roles in this process.

8.6.3 Associated Functions from the FIRST CSIRT Services Framework

- Service Area: Knowledge Transfer
 - Training and Education
 - Content Delivery (9.2.3)
 - Exercises
 - Exercise Execution (9.3.4)

8.6.4 Generic Competencies

- Professional
 - Critical Thinking (C011)
 - o Interpersonal Skills (C028)
- Operational
 - Data Privacy and Protection (C014)
 - External Awareness (C019)
 - Organizational Awareness (C037)

8.6.5 Role-Specific Competencies

- Leadership
 - Teaching Others (C052)



- Professional
 - o Oral Communication (C036)
 - o Presenting Effectively (C039)
 - o Written Communication (C060)



9 Practical Considerations

After we have described all potentially separated roles, we will now discuss more practical topics related to the usage of this document. Initially we will identify any role conflicts to consider before we explore ways to combine two – or more – roles for one staff position.

9.1 Combining multiple roles into single staff positions

Neither the FIRST CSIRT Services Framework nor this practice document on "CSIRT Services Roles and Competencies" assume that each role needs necessarily be assigned to or provided by one person only. Each person plays more than one role in practice, and some roles can be covered by the third-party providers. For practical reasons but also contingency, roles need to be covered by multiple persons, emphasizing again a need for persons being able to "switch" between roles as there is a need to do so.

For example, small CSIRTs usually do not have enough resources in terms of human resources and budgets. In such cases, the limited number of staff at a CSIRT may cover more roles based on their capabilities, and anything beyond that can be covered by third party professionals or one may need to reconsider the scope of their CSIRTs. For example, if a small CSIRT has people with IT or system administration experience, they can take as many roles as possible from the service areas of "Information Security Event Management" and/or "Information Security Incident Management", while they may want to rely everything else on using an outside, third-party professional services when necessary.

Middle or large CSIRTs can have more resources. While resources may not be enough, medium, or large CSIRTs can cover more roles and capabilities than smaller CSIRTs. If they cannot cover all what they need, some roles or capabilities can be covered by third party professionals constantly or on demand or may be out of scope of their CSIRT missions.

When you need to consider how each person need to cover more than one role, it is most important to understand what each person can do the best depending upon their background, profession, and capabilities.

While combining roles in a single position, it should not be only based on the capacity of a specific person and their skills and/or experience. If this person moves on, the next staff member need to have the same skills, or the tasks of this role must be re-distributed.

For this, it is useful to refer to the Appendices 4 and 5 of this CSIRT Service Roles and Competencies. For example, a person with proficient expertise and experience with triage can take over the roles of "Vulnerability Triage Coordinator" and "Incident Triage Coordinator". As another example, a person with proficient incident response expertise and experience can cover "Incident Analyst" and "Incident Triage Coordinator" as well as "Incident Responder" roles. While combining multiple roles into single staff positions depends on job descriptions, expectations from managers, experience, and expertise of each person, and how each CSIRT is operated, the Appendices 4 and 5 will help you assigning staff members to roles based on the understanding of such dependencies.



9.2 Addressing Role Conflicts

Especially in smaller CSIRT teams existing only of a few people, usually everyone is capable to handle all aspects of the functions provided by the team. The workload is distributed among the team members — often by themselves — and as there are only a few team member the capacity is not enough to support four eyes-principles. Everyone works hard towards shared objectives and is trusted to adhere to the common vision and agreed rules.

However, as a CSIRT grows into a bigger team (i.e., more than 15 staff), a more formalized approach is needed requiring better coordination and more specific roles addressing only part of the functions provided. The team management is required to manage all roles and role specific responsibilities. When enhancing operational processes in such circumstances, usually some conflicting roles are being identified. Conflicting roles are those, who if fulfilled by the same person, creates a conflict of interest. One source of such conflict is proper usage of resources or adherence to an agreed quality / service level. For example, for an effective controlling of resources used, a requestor of resources must be different from approver. Such separation is needed to protect employee's integrity, trust, and quality of outcome.

Even if roles are not conflicting, there still might be issues if the same person is doing a particular job without any supervision. For example, an Incident Responder reviews whether incidents are closed based on the agreed quality rules, but also approves the compliant closure of incidents that were handled by her/himself. Often four eyes' principles must be utilized for quality control purposes and to avoid that a single person can work around agreed rules and policies.

A typical example within a CSIRT setting can be attributed to the review and categorization of an incident:

The role "Incident Responder" is handling a new incident report about an attack, and the role "Triage Coordinator" shall observe and assure the quality of the response of the team – as defined by the work of the Incident Responder. If the two roles are assigned to the same person, this is a role conflict and must be avoided by other means. This does not mean that an Incident Responder cannot serve to the same time as triage coordinator. Only it must be ensured that the same person fulfills both roles in regard to the same incident. In general, a Triage Coordinator shall not quality control incidents for which the person was assigned as Incident Responder.

9.3 Some remarks about "Management" and "Managers"

There are some roles in this supplemental document that have the word "manager" in their title or refer in the description to "management" of service, functions, or tasks. Use of this word usually means that this role is a "project lead" or "lead" for the activities defined. It does not mean that they are a supervisory manager, that handles human resource issues or directs a team.

The Roles and Competencies document does not actually define true "Supervisory Manager" roles. That may possibly be included at a later time. However, since the term "manager" has a particular administrative or supervisory connotation, we have added optional/additional competencies and tasks into these roles, in case the person fulling the role is also a true supervisory manager.



If one of the persons fulfilling such roles is also responsible for the coordination and leadership of a service and its corresponding functions and related staff positions, the following specific organizational tasks shall be considered. It does not come as a surprise that these tasks are generic in character:

- Develop strategic direction for the team and provide oversight of mission execution
- Provide oversight and guidance to the situational awareness function and team members
- Ensure team meets objectives and stays on target
- Manage team dynamics and execution
- Execute judgement, decision-making skills, and flexibility in handling new situations, team conflicts, and customer requests
- Establish and maintain communication channels with customers and stakeholders.
- Manage sensitive or conflict-oriented situations
- Speak in public as appropriate, give executive briefings, and communicate with stakeholders

To be effectively be able to lead a service, team or group, additional competencies beyond those demanded by the service-related functions are often required. Most notably the following should be considered for those organizational managers:

Leadership

- o Project Management (C042)
- Strategic Planning (C047)
- Teaching Others (C052)
- Workforce Development (C059)

Professional

- Conflict Management (C009)
- Critical Thinking (C011)
- Interpersonal Skills (C028)
- Oral Communication (C036)
- Presenting Effectively (C039)
- Written Communication (C060)

Technical

Problem Solving (C040)

ANNEX 1: Acknowledgments

The following volunteers from the CSIRT communities contributed significantly to this new add-on to the CSIRT Services Framework. They have been listed in alphabetical order by their last name, without title but with affiliation, role, and country:

- Shin Adachi, NTT-CERT (US)
- Vilius Benetis, NRD CIRT (LT)
- Olivier Caleff, OpenCSIRT Foundation (FR)
- Cristine Hoepers, CERT.br/NIC.br (BR)
- Baiba Kaskina, CERT.LV (LV)
- Klaus-Peter Kossakowski (Editor), Hamburg University of Applied Sciences (DE)
- Franz Lantenhammer (DE)
- Samuel Perl, CERT/CC, SEI, CMU (US)
- Louis Rouxel, CERT-FR (FR)
- Robin M. Ruefle, CERT/CC, SEI, CMU (US)
- Don Stikvoort, OpenCSIRT Foundation (NL)
- Edgars Taurins, ENISA (LV)
- Sanita Vitola, CERT.LV (LV)
- Mark Zajicek, CERT/CC, SEI, CMU (US)



ANNEX 2: Terms and Definitions

This section defines certain terms used in the context of the FIRST CSIRT Services Framework including this add-on document.

Action - The description of how something is done at varying levels of detail.

Advisory¹⁴ - An announcement or bulletin that serves to inform, advise, and warn about the vulnerability of a product.

Capability - A measurable activity that may be performed as part of an organization's roles and responsibilities. For the purposes of the FIRST CSIRT Services Framework, the capabilities can either be defined as the broader services or as the requisite functions.

Capacity - The number of simultaneous process-occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

Common Vulnerability Exposures (CVE)¹⁵ - A list of entries containing an identification number, a description, and at least one public reference for publicly known vulnerabilities. Serves as a standard identifier to reference vulnerabilities.

Common Vulnerability Scoring System (CVSS)¹⁶ - A numerical score that reflects a vulnerability's severity.

Common Weakness Enumeration (CWE)¹⁷ - A formal list of software weakness types created to serve as a common language for describing software security weakness in architecture, design, or code; serve as a standard measuring stick for software security tools targeting these weaknesses; and provide a common baseline standard for weakness identification, mitigation, and prevention efforts.

Constituency - A specific group of people and/or organizations that have access to a specific set of services offered by a CSIRT.

Contextual Data Source - A source of contextual data that gives context to data points, for example to an identity, an asset, or an information security event. Specific examples include user databases, asset inventories, IP repudiation services, or threat intelligence data.

Coordinated Vulnerability Disclosure (CVD) - A term used to denote a disclosure process that includes coordination. Source: ISO/IEC 29147:2018, Terms and definitions.

Coordinator¹⁸ - An optional participant who can assist vendors and finders in handling and disclosing vulnerability information.

Version 0.9.0 for Review / TLP:WHITE

¹⁴ ISO/IEC 29147:2014 Information technology—Security techniques — Vulnerability disclosure- Terms/Definitions 3.1

¹⁵ https://cve.mitre.org/

¹⁶ https://www.first.org/cvss/

¹⁷ https://cwe.mitre.org/about/index.html

¹⁸ ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.1



Detection Use Case - A specific condition to be detected by an Information Security Event Management service area. The terminology originates in software engineering, but is now widely used in detection engineering.

Embargo - A hold on the publication of vulnerability details until affected vendors are able to release security updates or mitigations and workarounds to protect customers.

Finder¹⁹ - An individual or organization that identifies a potential vulnerability in a product or online service. Please note that finders can be researchers, reporters, security companies, hackers, users, governments, or coordinators.

Function - An activity or set of activities aimed at fulfilling the purpose of a particular service. Other definitions include: a group of related actions²⁰; to perform a specified action or activity, work, operate.²¹

Information Security Event - An observable event in an IT environment that is relevant to security; for example, a user logon or an IDS alert. Information security events typically produce some kind of evidence, such as an audit record or an entry in a log file, that can be collected and analyzed as part of the Information Security Event Management service area.

Information Security Incident²² - Any adverse information security event (or set of information security events) which indicates a compromise of some aspect of user, system, organization, and/or network information security. The definition of an information security incident may vary between organizations, but at least the following categories are generally applicable:

- Loss of confidentiality of information
- Compromise of integrity of information
- Denial of service
- Misuse of service, systems or information
- Damage to systems

Attacks, even if they failed because of proper protection, can be regarded as information security incident.

Key Performance Indicator (KPI)²³ - A measurable value that demonstrates how effectively a company is achieving key business objectives. Organizations use KPIs at multiple levels to evaluate their success at reaching targets.

Maturity - How effectively an organization executes a particular capability within the mission and authorities of the organization. It is a level of proficiency attained either in executing specific functions or in an aggregate of functions or services. The ability of an organization will be determined by the extent and quality of established policies and documentation and the ability to execute a set process.

¹⁹ ISO/IEC 29147:2014 Information technology—Security techniques — Vulnerability disclosure- Terms/Definitions 3.3

²⁰ Source: https://www.merriam-webster.com/dictionary/function

²¹ Source: https://www.dictionary.com/browse/function

²² Based on RFC2350 by considering "information security" instead of "IT security", https://tools.ietf.org/html/rfc2350.

²³ https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator



Open Source - Works that are licensed in such a way that they may be freely redistributed and modified, where the source code is made available publicly, and is freely distributed and does not discriminate against any persons, groups, or fields of endeavor, and is technology-neutral. Open source software is often maintained by a community of individuals and entities who collaboratively create and maintain it.

Product²⁴ - A system implemented or developed for sale or to be offered for free.

Remediation (or Remedy)²⁵ - A change made to a product or online service to remove or mitigate a vulnerability. A remediation typically takes the form of a binary file replacement, configuration change, or source code patch and recompile. Different terms used for "remediation" include patch, fix, update, hotfix, and upgrade. Mitigations are also called workarounds or countermeasures.

Responsible Disclosure - A term which is used to refer to a process or model where a vulnerability is disclosed only after a period of time that allows a remediation (fix or patch) to be made available. This term is not necessarily the same as "coordinated vulnerability disclosure."

Risk²⁶ - The "effect of uncertainty on objectives." In this definition, uncertainties include events (which may or may not happen) and uncertainties caused by ambiguity or a lack of information.

Risk Acceptance²⁷ - A risk response strategy whereby the project team decides to acknowledge the risk and not take any action unless the risk occurs.

Risk Register²⁸ - A document in which the results of risk analysis and risk response planning are recorded.

Service - A service is a set of recognizable, coherent functions towards a specific result. Such results might be expected or required by constituents or on behalf of or for the stakeholder of an entity.

Service Level Agreement (SLA) - A contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider.

Stakeholders²⁹ - Individuals or groups that define and modify the service areas or services and ensure an appropriate service communication strategy and groups who can benefit from services offered.

Tasks - the list of actions that must be performed to complete a specific function.

Vendor³⁰ - A person or organization that developed the product or service or is responsible for maintaining it.

Vulnerability³¹ - A weakness in software, hardware, or an online service that can be exploited.

Version 0.9.0 for Review / TLP:WHITE

²⁴ ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability disclosure-Terms/Definitions 3.5

²⁵ ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability disclosure-Terms/Definitions 3.6

²⁶ ISO 31000:2009/ ISO Guide 73:2002 Risk management — Principles and guidelines- Terms/Definitions 2.1

²⁷ The Project Management Body of Knowledge (PMBOK) Guide and Standards

²⁸ The Project Management Body of Knowledge (PMBOK) Guide and Standards

²⁹ Architecture Content Framework

³⁰ ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.7

³¹ ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.8



ANNEX 3: Supporting Resources

Alberts, David S., et.al. Understanding information age warfare. In *DOD Command and Control Research Program Publication Series*. ADA395859. Booz Allen & Hamilton, McLean, VA. 2001. https://apps.dtic.mil/docs/citations/ADA395859

Barford P., et al. (2010) Cyber SA: Situational Awareness for Cyber Defense. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, 2010. Boston, MA. ISBN 978-1-4419-0140-8 1

https://link.springer.com/chapter/10.1007/978-1-4419-0140-8 1

Boyd, John R. Destruction and Creation. Goal Systems International. September 3, 1976. http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf

Cartwright, James E. Joint Concept of Operations for Global Information Grid NetOps. *United States Strategic Command*. PDF August 10, 2005. Homeland Security Digital Library. August 10, 2005. https://www.hsdl.org/?view&did=685398

Committee on National Security Systems Instruction CNSSI 4009. *Committee on National Security Systems Website*. June 23, 2019 [accessed]. https://www.cnss.gov/cnss/

Cybersecurity Situation Awareness. *The MITRE Corporation Website*. June 25, 2019 [accessed]. https://www.mitre.org/capabilities/cybersecurity/situation-awareness

Endsley, Mica R. Toward a theory of situation awareness in dynamic systems. *Human factors* Volume 37. Number 1. March 1995 Pages 32-64.

https://journals.sagepub.com/doi/10.1518/001872095779049543

FIRST *Product Security Incident Response Team (PSIRT) Services Framework*, Version 1.0, 2018. North Carolina: First.org, 2018

https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0

FIRST Vulnerability Reporting and Data eXchange SIG (VRDX-SIG). 2013-2015. North Carolina: First.org, 2015 https://www.first.org/global/sigs/vrdx/

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure, Version 1.0, 2017. North Carolina: First.org, 2017

https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.0

Hawk, Robert. Situational Awareness in Cyber Security. [blog post]. *Hawk's Posts: Security Essentials from Robert Hawk.* June 11, 2015.

https://www.alienvault.com/blogs/security-essentials/situational-awareness-in-cyber-security

Householder, Allen D.; Wassermann, Garret; Manion, Art; King, Christopher. *The CERT® Guide to Coordinated Vulnerability Disclosure*. CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University. 2017 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330



Householder, Alan. Vulnerability Discovery for Emerging Networked Systems [blog post]. *Vulnerability discovery techniques*. November 20, 2014.

https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability disclosure*. Second Edition. ISO/IEC 29147:2018. Geneva, Switzerland: ISO: IEC. 2018 https://www.iso.org/standard/72311.html

International Organization for Standardization. *Information technology -- Security techniques -- Vulnerability handling processes*. First Edition. ISO/IEC 30111:2013. Geneva, Switzerland: ISO: IEC. 2013 https://www.iso.org/standard/53231.html

Jajodia, Sushil, et al., (Eds.). *Cyber Situational Awareness: Issues and Research*. Part of the Advances in Information Security book series (ADIS, volume 46). 2010. ISBN 978-1-4419-0140-8 https://link.springer.com/book/10.1007/978-1-4419-0140-8

Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001. ISBN: 9783831100590.

Kossakowski; Klaus-Peter & Stikvoort, Don. *A Trusted CSIRT Introducer in Europe*. Amersfoort, Netherlands: M&I/Stelvio, February, 2000.

http://www.ti.terena.nl/process/ti-v2.pdf

Manion, Art & Householder, Alan. *Vulnerability Analysis*. CERT Coordination Center (CERT/CC). May 30, 2019. https://vuls.cert.org/

McGuinness, B. &, Foy, L. A subjective measure of SA: The crew awareness rating scale (cars). In Kaber, D.B.; Endsley, M.R.; p. 286-291. *Proceedings of the First Human Performance, situation awareness and automation conference; user-centered design for the new millennium.* Savannah, Georgia, October 2000.

Salerno, John; Hinman, Michael & Boulware, Douglas. Situation awareness model applied to multiple domains. In *Proceedings of the Defense and Security Conference*, Orlando, FL, March 2005.

 $\frac{https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5813/0000/A-situation-awareness-model-applied-to-multiple-domains/10.1117/12.603735.full?SSO=1$

Stone, Steve. Data to Decisions for Cyberspace Operations. *The MITRE Corporation Website*. January 2016 https://www.mitre.org/publications/technical-papers/data-to-decisions-for-cyberspace-operations

Tadda G.P., Salerno J.S. (2010) Overview of Cyber Situation Awareness. In: Jajodia S., Liu P., Swarup V., Wang C. (eds) Cyber Situational Awareness. Advances in Information Security, vol 46. Springer, Boston, MA. 2010. ISBN 978-1-4419-0140-8

https://link.springer.com/chapter/10.1007/978-1-4419-0140-8 2

West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. CMU/SEI-98-HB-001. Software Engineering Institute, Carnegie Mellon University. 1998.

http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html



ANNEX 4: Cross-Reference Services vs. Roles

Technical and Policy Advisory	Exercises	Training and Education	Awareness Building	Service Area: Knowledge Transfer	Service Communication	Analysis and Synthesis	Data Acquisition	Service Area: Situational Awareness	Vulnerability Response	Vulnerability Disclosure	Vulnerability Coordination	Vulnerability Analysis	Vulnerability Report Intake	Vulnerability Discovery/Research	Service Area: Vulnerability Management	Crisis Management Support	Information Security Incident Coordination	Mitigation and Recovery	Artifact and Forensic Evidence Analysis	Analysis	Report Acceptance	Service Area: Information Security Incident Management	Event Analysis	Monitoring and Detection	Service Area: Information Security Event Management	
				nsfer				ireness							lanage							curity I	Г	×	curity E	System and Sensor Administrator
															ment							ncident		×	vent N	Use Case Manager
																						t Manag		×	lanager	Data Manager
														×					×	×		gement	×		ment	Incident Analyst
																×				×	×		×			Incident Triage Coordinator
																	×	×		×						Incident Responder
														×					×	×						Malware / Forensic Analyst
																		×								IT Administrator
					×											×	×									Communication Liaison
												×		×												Vulnerability Analyst
														×												Vulnerability Researcher
												×	×													Vulnerability Triage
																										Coordinator Vulnerability
											×															Coordinator
										×																Vulnerability Disclosure Coordinator
									×																	Vulnerability
																										Assessment Analyst IT Security
									×																	Administrator
							×																			Situational Awareness Manager
																										Risk & Continuity
×							×																			Advisor / Risk Analyst
						×	×																			Situational Awareness Data Analyst
					×	×																				Threat Warning
																										Analyst Awareness
			×																							Coordinator
	×	×																								Training Developer
	×	×																								Training Instructor
		×																								Staff Developer
																										Policy Advisor
×																										Technical Advisor



ANNEX 5: Cross-Reference Services Functions vs. Roles

Annex 5.1: Information Security Event Management



Annex 5.2: Information Security Incident Management

Information Security Incident Management Information Security Incident Report Acaystace Information Security Incident Prings and Processing (6.1.1) Information Security Incident Prings and Processing (6.1.2) Information Security Incident Prings (Prinding Analysis (6.2.3) Information Security Incident Prings (Prinding Analysis (6.2.3) Information Security Incident Processing (6.2.3) Information Security Incident Root Cause Analysis (6.2.4) Cross-incident Correlation (6.2.3) Information Security Incident Root Cause Analysis (6.2.4) Reference Engineering (6.3.2) X X X Artifact and Forestic Evidence Analysis (6.3.3) X X X Artifact and Forestic Evidence Analysis (6.3.3) X X X Artifact and Forestic Evidence Analysis (6.3.3) X X X Artifact and Recovery Report Analysis (6.3.3) X X X Artifact and Recovery Report Analysis (6.3.3) X X X Artifact and Recovery Report Analysis (6.3.3) X X Artifact and Recovery Report			System and Sensor Administrator	Use Case Manager	Data Manager	Incident Analyst	Incident Triage Coordinator	Incident Responder	Malware / Forensic Analyst	IT Administrator	Communication Liaison	Vulnerability Analyst	Vulnerability Researcher	Vulnerability Triage Coordinator	Vulnerability Coordinator	Vulnerability Disclosure Coordinator	Vulnerability Assessment Analyst	IT Security Administrator	Situational Awareness Manager	Risk & Continuity Advisor /	Risk Analyst Situational Awareness Data	Analyst	Threat Warning Analyst	Awareness Coordinator	Training Developer	Training Instructor	Staff Developer	Policy Advisor	Technica! Advisor
Information Security incident Ranalysis (6.1.2) Information Security incident Analysis (6.2.3) Information Security incident Analysis (6.2.3) Information Security incident Ranalysis (6.2.4) Detailed Analysis (6.2.4) Cross-Incident Rococcuse (6.2.9) Information Security incident Rococcuse (6.2.9) Information Incide	Service Area: Information Security Inciden	t Management																											
Information Security incident Analysis Prioritization and Carecrostation (6.2.3) Detailed Analysis Conditiation (6.2.3) Detailed Analysis Conditiation (6.2.3) Information Security incident Root Cuses Analysis (6.2.4) Antificial and Forentic Evidence Analysis (6.2.4) Reverse Engineering (6.3.2) Reverse Engineering (6.3.2) Reverse Engineering (6.3.3) Comparathe Analysis (6.3.4) Mitigation and Recovery Response Plan Establishment (6.4.1) Ad Hock Measures and Containment (6.4.2) System Restoration (6.4.3) Other Information Security Incident Coordination (6.4.4) Notification Distribution (6.5.1) Reverse Engineering (6.3.3) Ad Hock Resurres and Containment (6.4.2) System Restoration (6.4.3) Notification Distribution (6.5.3) Ad Hock Resurres and Containment (6.4.2) System Restoration (6.4.3) Notification Distribution (6.5.3) Ad Hock Security Incident Coordination Reporting (6.5.5) Reporting (6.5.5) Reporting (6.5.5) Media Communication (6.5.6) Media Communication Coordination (6.5.6) Media Communication (6.5.6) Media Communication Coordination (6.5.6) Media Communication (6.5.6) Media Communication Coordination (6.5.6) Media Communication Coordination (6.5.6)	Information Security Incident Report Acceptance	Receipt (6.1.1) Information Security Incident Triage and																											
Information Security Incident Root Cause Analysis (6.2.4) Antitect and Forensic Evidence Analysis (6.3.1) Reverse Engineering (6.3.2) Runtime or Dynamic Analysis (6.3.3) Comparative Analysis (6.3.3) Comparative Analysis (6.3.4) Ad Hock Measures and Containment (6.4.1) Ad Hock Measures and Containment (6.4.2) System Restoration (6.4.3) Other Information Security Incident Coordination Out Officiation Distribution (6.5.1) Notification Distribution (6.5.1) Reverse Engineering (6.3.2) X X X X X X X X X X X X X	Information Security Incident Analysis	Information Security Incident Triage (Prioritization and Categorization) (6.2.1)					x	х																					
Actifact and Forentic Evidence Analysis (6. 3.1) X X X Reverse Engineering (6. 3.2) X Runtime or Dynamic Analysis (6. 3.3) X Comparative Analysis (6. 3.4) X Mitigation and Recovery Response Plan Establishment (6. 4.1) X Ad Hoc Measures and Containment (6. 4.2) X System Restoration (6. 4.3) X Other Information Security Entitles Support (6. 4.4) X Information Security Indian Coordination Communication (6. 5.1) X Notification Distribution (6. 5.2) X Relevant Information Distribution (6. 5.3) X Activities Coordination (6. 5.4) X Reporting (6. 5.5) X Recording (6. 5.6) X R		Information Security Incident Root Cause Analysis (6.2.4)						x	×																				
Reverse Engineering (6.3.2) x Runtime or Dynamic Analysis (6.3.3) x Comparative Analysis (6.3.4) x Mutigation and Recovery Response Pfan Stablishment (6.4.1) x Ad Hoc Measures and Containment (6.4.2) x System Rectoration (6.4.3) x Other Information Security Entities x Support (6.4.4) x Information Security Incident Coordination Communication (6.5.1) x Notification Distribution (6.5.1) x Notification Distribution (6.5.3) x Relevant Information Distribution (6.5.3) x Reporting (6.5.5) x Reporting (6.5.5) x Media Communication (6.5.6) x Media Communication (6.5.6) x Information Distribution (6.5.6) x Infor	Artifact and Forensic Evidence Analysis																												
Runtime or Dynamic Analysis (6.3.3) Comparative Analysis (6.3.4) X Mitigation and Recovery Response Plan Establishment (6.4.1) Ad Hoc Measures and Containment (6.4.2) System Restoration (6.4.3) Other Information Security Finities Support (6.4.4) Communication (6.5.1) X Notification Distribution (6.5.2) Relevant Information Distribution (6.5.3) Activites Coordination (6.5.4) Reporting (6.5.5) Media Communication (6.5.6) X Reporting (6.5.5) Media Communication (6.5.6) X Cotis Management Support (6.6.1) X Cotis Management Support	The state of the s					^																							
Comparative Analysis (6.3.4) Ad foot Messures and Containment (6.4.2) Ad foot Messures and Containment (6.4.2) System Restoration (6.4.3) Other Information Security Incident Coordination Information Security Incident Coordination Communication (6.5.1) Notification Distribution (6.5.3) Relevant Information Distribution (6.5.3) Activities Coordination (6.5.4) Reporting (6.5.5) Media Communication (6.5.6) Media Communication (6.5.6) Information Distribution (6.5.6)																													
Mitigation and Recovery Resignorse Plan Establishment (6.4.1) Ad thoc Measures and Containment (6.4.2) System Restoration (6.4.3) Other Information Security incident Coordination Communication (6.5.1) Notification Distribution (6.5.2) Relevant Information Distribution (6.5.3) Activities Coordination (6.5.4) Reporting (6.5.5) Media Communication (6.5.6) Media Communication (6.5.6) Media Communication (6.5.6) Media Communication (6.5.6) Information Distribution (6.5.6) X Cotist Management Support (6.6.1)																													
Ad Hot Measures and Containment (6.4.2) System Restoration (6.4.3) Other Information Security Entitles Support (6.4.4) Information Security incident Coordination Communication (6.5.1) Notification Distribution (6.5.1) Notification Distribution (6.5.3) Activities Coordination (6.5.4) Reporting (6.5.5) X Media Communication (6.5.6) X Media Communication (6.5.6) X Cities Management Support (6.6.2.1)									х																				
System Restoration (6.4.3) x Other Information Security Entitles Subcond (6.4.4) Information Security Industrian Security Industrian Security Industrian Security Industrian Security Industrian Security Industrian Security Industrian Security Industrian Security Industrian Security Industrian Security Industrian Security Industrian Industrian Industrian Industrian Industrian Industrian Industrian Indust	Mitigation and Recovery							х																					
Other Information Security Entities		Ad Hoc Measures and Containment (6.4.2)						х																					
Supon (6.4.4) X whomustain Security incident Coordination Communication (6.5.1) X Notification Distribution (6.5.2) X Relevant Information Distribution (6.5.3) X Activities Coordination (6.5.4) X Reporting (6.5.5) X Reporting (6.5.5) X Notification Distribution (6.5.6) X Notification Distribution (6.5.6) X Notification Distribution (6.5.6) X Notification Distribution (6.5.6) X Crists Management Support										х																			
Information Seauthy ledderd Coerdination Communication (6.5.1) Notification Distribution (6.5.2) Relevant Information Distribution (6.5.3) Activities Coordination (6.5.4) Reporting (6.5.5) Media Communication (6.5.6) X Coilin Management Support (6.5.1) (6.5.1) X								х																					
Relevant Information Distribution (6.5.3) X Activities Coordination (6.5.4) X Reporting (6.5.5) X Media Communication (6.5.6) X Critis Management Support Information Distribution to Constituents (6.6.1) X	Information Security Incident Coordination							х																					
Activities Coordination (6.5.4) x Reporting (6.5.5) x Media Communication (6.5.6) x Crisis Massagement Support Information Distribution to Constituents x		Notification Distribution (6.5.2)						х																					
Reporting (6.5.5) X Media Communication (6.5.6) X Childs Management Support Information Distribution to Constituents (6.6.1) X		Relevant Information Distribution (6.5.3)						х																					
Media Communication (6.5.6) x Chids Management Support Information Distribution to Constituents x (6.6.1)		Activities Coordination (6.5.4)						х																					
Crisis Management Support (5.5.1) X		Reporting (6.5.5)						x																					
Crisis Management Support (5.5.1) X		Media Communication (6.5.6)									x																		
Information Security Status Reporting (6.6.2) Strategic Decisions Communication (6.6.3) X	Crisis Management Support	(6.6.1) Information Security Status Reporting (6.6.2)					x																						

Annex 5.3: Vulnerability Management

		System and Sensor Administrator	Use Case Manager	Data Manager	Incident Analyst	Incident Triage Coordinator	Incident Responder	Malware / Forensic Analyst	IT Administrator	Communication Liaison	Vulnerability Analyst	Vulnerability Researcher	Vulnerability Triage Coordinator	Vulnerability Coordinator	Vulnerability Disclosure	Vulnerability Assessment Analyst	IT Security Administrator	Situational Awareness	Manager Risk & Continuity Advisor /	Rsk Analyst	Situational Awareness Data Analyst	Threat Warning Analyst	Awareness Coordinator	Training Developer	Training Instructor	Staff Developer	Policy Advisor	Technical Advisor
Service Area: Vulnerability Management																												
Vulnerability Discovery/Research	Incident Response Vulnerability Discovery (7.1.1) Public Source Vulnerability Discovery (7.1.2) Vulnerability Research (7.1.3)				х			x			x	x																
Vulnerability Report Intake	Vulnerability Report Receipt (7.2.1) Vulnerability Report Triage and Processing (7.2.2)												x x															
Vulnerability Analysis	Vulnerability Triage (Validation and Categorization) (7.3.1) Vulnerability Root Cause Analysis (7.3.2) Vulnerability Remediation Development (7.3.3)										x x		х															
Vulnerability Coordination	Vulnerability Notification/Reporting (7.4.1) Vulnerability Stakeholder Coordination (7.4.2)													x														
Vulnerability Disclosure	Vulnerability Disclosure Policy and Infrastructure Maintenance (7.5.1) Vulnerability Announcement / Communication / Dissemination (7.5.2) Post-Vulnerability Disclosure Feedback (7.5.3)														x x													
Vulnerability Response	Vulnerability Detection/Scanning (7.6.1) Vulnerability Remediation (7.6.2)															x	×											

Annex 5.4: Situational Awareness

		System and Sensor Administrator	Use Case Manager	Data Manager	Incident Analyst	Incident Triage Coordinator	Incident Responder	Malware / Forensic Analyst	IT Administrator	Communication Liaison	Vulnerability Analyst	Vulnerability Researcher	Vulnerability Triage Coordinator	Vulnerability Coordinator	Vulnerability Disclosure	Vulnerability Assessment Analyst	T Security Administrator	Carried American	Manager	Risk & Continuity Advisor / Risk Analyst	Situational Awareness Data	Threat Warning Analyst		Awareness coordinator	Training Developer	Training Instructor	Staff Developer	Policy Advisor	Technical Advisor
Service Area: Situational Awareness																													
Data Acquisition	Policy Aggregation, Distillation, and Guidance (8.1.11 Asset Mapping to Functions, Roles, Actions. and Kev Risks (8.1.2) Collection (8.1.3) Data Processing and Preparation (8.1.4)																		x	x	x x								
Analysis and Synthesis	Projection and Inference (8.2.1)																				х								
	Event Detection (through Alerting and/or Hunting) (8.2.2) Information Security Incident																					×							
	Management Decision Support (8.2.3)																					Х							
	Situational Impact (8.2.4) Internal and External Communication																					Х							
Service Communication	(8.3.1)																					х							
	Reporting and Recommendations (8.3.2)																					х							
	Implementation (8.3.3)																					х	4						
	Dissemination / Integration / Information Sharing (8.3.4)									х																			
	Management of Information Sharing (8.3.5)									x																			
	Feedback (8.3.6)									х																			

Annex 5.5: Knowledge Transfer

		System and Sensor Administrator	Use Case Manager	Data Manager	Incident Analyst	Incident Triage Coordinator	Incident Responder	Malware / Forensic Analyst	IT Administrator	Communication Liaison	Vulnerability Analyst	Vulnerability Researcher	Vulnerability Triage Coordinator	Vulnerability Coordinator	Vulnerability Disclosure Coordinator	Vulnerability Assessment Analyst	IT Security Administrator	Situational Awareness	Risk & Continuity Advisor /	Risk Analyst	Analyst	ThreatWarning Analyst	Awareness Coordinator	Training Developer	Training Instructor	Staff Developer	Policy Advisor	Technical Advisor
Service Area: Knowledge Transfer	Research and Information Aggrega	tion																										
Awareness Building	Research and Information Aggregation Report and Awareness Materials Develooment Information Dissemination Outreach																						x x x					
Training and Education	Knowledge, Skill, and Ability Requirements Gathering Educational and Training Materials Development Content Delivery Mentoring CSIRT Staff Professional Development																							x x	×	x x		
Exercises	Requirements Analysis Format and Environment Development Scenario Development Exercise Execution Exercise Outcome Review																							x x x	x			
Technical and Policy Advisory	Risk Management Support Business Continuity and Disaster Recovery Plannine Support Policy Support Technical Advice																		1	×							×	x



ANNEX 6: Cross-Reference Roles vs. Competencies

G = generic competency R = role-specific competency

Risk Management (C044)	Policy Management (C038)	Organizational Awareness (C037)	Legal, Government, and Jurisprudence (C030)	External Awareness (C019)	Data Privacy and Protection (C014)	Client Relationship Management (C003)	Business Continuity (C002)	Operational	Written Communication (C060)	Presenting Effectively (C039)	Oral Communication (C036)	Interpersonal Skills (C028)	Critical Thinking (C011)	Conflict Management (C009)	Professional	Workforce Management (C059)	Teaching Others (C052)	Strategic Planning (C047)	Leadership	
r	R	R	R	R	G	R			R	R	R	G				G	R	G		Awareness Coordinator
			മ	æ	മ	മ			æ	R	R	മ					മ			Communication Liaison
മ					മ		G		ര		G		ര	ര						Data Manager
	മ	മ			മ															IT Administrator
Г	മ				ര		æ						മ							IT Security Administrator
		R	R	æ	æ				ര		G		ര	G						Incident Analyst
æ		æ	æ	æ	æ	മ	æ		മ	മ	മ		മ	ര						Incident Responder
മ	æ	R	R	æ	R	R	G		ര			<u>ه</u>	ര	മ		ര	മ	G		Incident Triage Coordinator
Г		R	æ	æ	æ				ര				മ	മ						Malware / Forensic Analyst
æ	æ		R	æ	ര	G			æ	æ	R		ര			æ	മ	æ		Policy Advisor
æ	æ	æ	æ	æ	æ	മ	æ		æ	æ	₽	മ	മ	മ			മ	G		Risk Analyst including Risk & Continuity Advisor
		R	R	æ	æ				മ	മ	മ		മ							Situational Awareness Data Analyst
æ	æ	R	æ	æ	æ	R			മ	മ	G	G	മ			æ	æ	G		Situational Awareness Manager
		æ			æ				മ	മ	G	G	മ	G		æ	æ	G		Staff Developer
ഒ		G	G	ര	ര		G						ര	G						System and Sensor Administrator
ഒ	æ		G		æ	G	æ		ര	മ	G	G	ര							Technical Policy Advisor
æ		æ	മ	æ	æ		۵		മ	മ	G		മ							Threat Warning Analyst
		R		æ		R			æ	R	R		ര				æ	G		Training Developer
		G		മ	മ				æ	æ	æ	G	മ				æ			Training Instructor
ഒ	മ	G		മ	മ		G		ര	മ	G		മ	G						Use Case Manager
æ				æ	æ		G		ഒ	G	G		മ							Vulnerability Analyst
æ				æ	æ		۵		മ	മ	മ		മ							Vulnerability Assessment Analyst
æ	æ	G	æ	æ	æ	R			മ	മ	G	മ	മ	മ		മ	മ	G		Vulnerability Coordinator
æ	æ	G	R	æ	R	R			ര	G	G	മ	G	G		G	മ	G		Vulnerability Disclosure Coordinator
æ				æ	æ		۵		മ	മ	G		മ							Vulnerability Researcher
æ	æ	ഹ	∞	æ	æ	æ			ഹ	മ	ഹ	മ	ഹ			ഹ	മ	G		Vulnerability Triage Coordinator



G = generic competency R = role-specific competency

Vulnerabilities Assessment (C057)	Threat Analysis (C055)	Technology Awareness (C053)	Systems Testing and Evaluation (C050)	Systems Integration (C049)	System Administration (C048)	Software Testing and Evaluation (C046)	Requirements Analysis (C043)	Problem Solving (C040)	Operations Support (C035)	Operating Systems (C034)	Network Management (C033)	Knowledge Management (C029)	Intelligence Analysis (C027)	Information Technology Assessment (C025)	Information Systems and Network Security (C024)	Information Assurance (C022)	Incident Management (C021)	Data Management (C013)	Data Analysis (C012)	Computer Network Defense (C007)	Computer Forensics (C005)	Asset and Inventory Management (C001)	Technical	
	R	R					₽	G				æ												Awareness Coordinator
												æ												Communication Liaison
æ	æ	R						G			æ	æ			æ	æ		æ		æ				Data Manager
		R	æ	æ	æ	æ		G	R	R	æ				R							æ		IT Administrator
		R	æ	æ	æ	æ		G	æ	R	æ				æ	æ				æ		æ		IT Security Administrator
æ	R	R						G				æ	ᅍ	R	æ		R	æ	æ	æ	æ			Incident Analyst
æ	R	æ						G				æ	æ	R	æ		R		æ	æ	R			Incident Responder
æ	R	R					R	G				R	æ	R	R		R		æ	æ	R			Incident Triage Coordinator
₽	R	R						G				æ	æ	æ	æ		R	æ	æ	æ	æ			Malware / Forensic Analyst
ᅍ	R	R					R	G				æ				æ								Policy Advisor
₽	R	R					æ	G				æ	æ	R	æ	æ	R			æ				Risk Analyst including Risk & Continuity Advisor
	R	R						G				æ	æ	æ	R	æ	R	æ	æ	æ				Situational Awareness Data Analyst
	R	₽					₽	മ	₽			æ	₽	₽	æ	æ	R	æ	æ	æ		∞		Situational Awareness Manager
								G				æ						æ						Staff Developer
		R	æ	æ	æ	æ		G	æ	R	æ				æ	æ		æ		æ		₽		System and Sensor Administrator
							æ	G				æ		R	R	æ	R							Technical Policy Advisor
	R	R					æ	G	æ			æ	æ	R	R	æ	R	æ	æ	æ				Threat Warning Analyst
		R					R					æ		R	R		R							Training Developer
																								Training Instructor
₽	R	R					æ	G		æ	æ	æ	æ		R	æ		æ		æ		R		Use Case Manager
æ	R	R						G				æ	æ			æ		æ	æ	æ	R	æ		Vulnerability Analyst
R	R	R						G				æ	æ			æ		æ	æ			70		Vulnerability Assessment Analyst
æ	R	R					æ	G				æ	æ			æ			æ					Vulnerability Coordinator
							R	G				æ	R						æ					Vulnerability Disclosure Coordinator
æ	R	R						G				æ	æ			æ			æ	æ	æ			Vulnerability Researcher
R	æ	æ					æ	G				æ	æ			æ			æ					Vulnerability Triage Coordinator
																								•