November 2019

Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0

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

CSIRT Services Framework

1 Purpose

The 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 is 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).

The mission and purpose of the 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.

The Framework seeks to assist teams by identifying and defining core categories of services and their sub-components. This includes a title and description for each service, sub-service, function, and optionally sub-function – as appropriate. This document is a starting point to provide a consistent service framework that identifies a standard set of terms and definitions to be used across the community. Note that this document does not explain how to build or improve a CSIRT or corresponding team. This type of information is available in other documents, some of which are listed in Annex 1 as supporting resources.

This version of the CSIRT Services Framework replaces all previous versions. It makes no suggestions or recommendations about capability, capacity, maturity, or quality 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 framework document. Also, this framework does not look at implementation or propose a specific way to implement any particular service. It is important to understand that these services can be implemented in many different ways, while still ensuring that reasonable expectations of constituents and stakeholders are met.

2 Introduction and Background

A Computer Security Incident Response Team is an organizational unit (which may be virtual) or a capability that provides services and support to a defined constituency for preventing, detecting, handling, and responding to computer security incidents, in accordance with its mission.

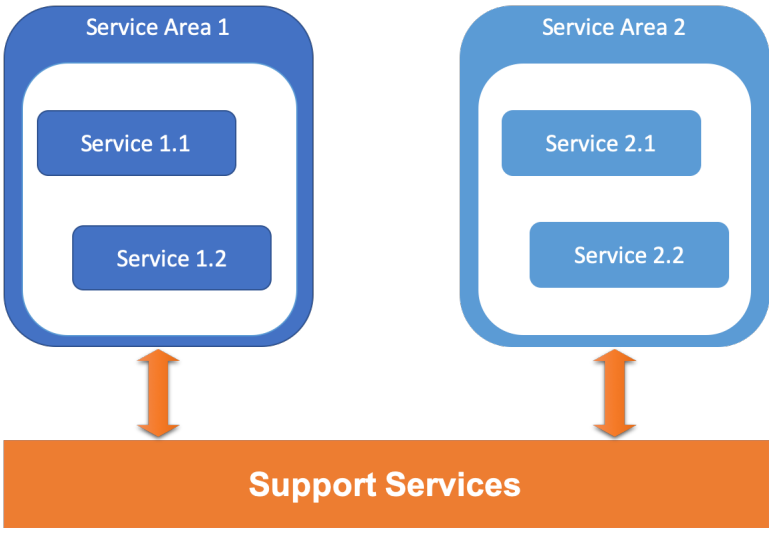
A properly deployed CSIRT has a clear mandate, a governance model, a tailored services framework, technologies, and processes to provide, measure, and continuously improve defined services.

Various entities in the CSIRT community have developed their own service lists or frameworks over the years. As technology, tools, and processes changed, the community felt that there were topics and activities missing from the existing lists. FIRST, interested in enabling the global development and maturation of CSIRTs, recognized that this was a key piece in developing a common language for all CSIRTs and other entities who collaborate with CSIRTs. Given the geographical and functional span of the membership of FIRST, it was determined that the community that it constitutes would be an appropriate source for definitive capture and representation of the services provided by CSIRTs. Based on this understanding, a community-driven approach to developing an improved CSIRT services framework was launched, and an initial version was published in 2017.

Since then, a similar approach has been taken to develop a Product Security Incident Response Teams (PSIRT) Services Framework in recognition of many operational aspects that require a different set of services and corresponding activities. All Services Frameworks can be found on the FIRST website.[1]

This is an improved version of the second version of the CSIRT Services Framework. Based on the feedback by several experts on the first version, this edition has been restructured and expanded where necessary. In particular, the internal activities have been removed as those do not constitute service offerings to constituents. Internal and external activities supporting the full life cycle of any service offering can be organized in services and functions just like services designated to be provided to constituents. Those services and functions are mostly known as Support Services. Some examples would be administrative activities like managing staff and hiring, travel reimbursements, or the organization of training events.[2]

Based on our knowledge there are many different ways to provide such Support Services, and most are depending on the organization hosting the CSIRT or related service offerings. For example, hiring and managing of staff is surely required in supporting the CSIRT, but is considered a typical organizational support task and not specific to CSIRTs.



[1] https://www.first.org/standards/frameworks/csirts/ for CSIRT related materials
[2] Check [Kossakowski 2001] for a discussion of internal support services and its relationship to other services

Although internal services and functions are providing the backbone to enable any team or organisational unit to fulfill its mission, such support services are considered out of scope and are not further detailed or discussed within FIRST Services Frameworks.

As CSIRTs will continue to face the ever-changing challenges to keep their constituents secure against new emerging threats, the services covered by this framework will be reviewed, vetted, and extended or amended as needed in future versions.[3]

3 The Difference Between a CSIRT and a PSIRT

The focus on constituents as well as the services offered are the key differentiators between the CSIRT of an organization and other security teams represented in the same organization, such as a PSIRT. Generally, the focus on products is the key differentiator between the PSIRT and any other security team, including but not limited to CSIRTs inside an organization.

Inside an organization, an Enterprise CSIRT is focused on the security of computer systems and networks that make up the infrastructure of an organization. If there are multiple security teams and CSIRTs inside a large organization, one of them might serve as coordinator and single point of contact to the external parties. Such teams are called Coordinating CSIRTs.

Such Coordinating CSIRTs are also established as independent entities serving a specific set of individuals and/or organizations known as a constituency. Organizations belonging to a specific constituency share some common characteristics (like being part of a national research network or belonging to a specific country). The Coordinating CSIRT acts as single point of contact for the whole group and is focused on the overall security aspects of these organizations.

Today, national CSIRTs have been established as a distinctive type of Coordinating CSIRT to facilitate and often coordinate the activities of CSIRTs located in a particular nation or offer limited services for all citizens, specific sectors of critical infrastructure entities, etc. of this nation.

While there are important differences between any CSIRT and PSIRT, it is important to recognize that there is also synergy between the two entities. The important point to take away is that both CSIRTs and PSIRTs do not operate independently of each other, as, for example, many CSIRTs warn constituents about security vulnerabilities. Such warnings are almost always based on information provided by vendor PSIRTs.

4 CSIRT Services Framework Structure

The framework for CSIRT services is based on the relationships of four key elements:

SERVICE AREAS → SERVICES → FUNCTIONS → SUB-FUNCTIONS

These elements are defined as:

[3] A FIRST Special Interest Group (SIG) has been established to steer the “CSIRT Framework Development”.

SERVICE AREAS

Service areas group services related to a common aspect. They help to organize the services along a top-level categorization to facilitate understanding and communication. The specification for each service area would include a “Description” field consisting of a general, high-level narrative text describing the service area and the list of services within the service area.

SERVICES

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

A service is specified by the following template:

- A “Description” field describing the nature of the service
- A “Purpose” field describing the intent of the service
- An “Outcome” field describing any measurable results of the service

FUNCTIONS

A function is an activity or set of activities aimed at fulfilling the purpose of a particular service. Any function might be shared and used in the context of several services.

A function is described by the following template:

- A “Description” field describing the function
- A “Purpose” field describing the intent of the function
- An “Outcome” field describing any measurable results of the function
- The list of sub-functions that might be performed as part of the function.

SUB-FUNCTIONS

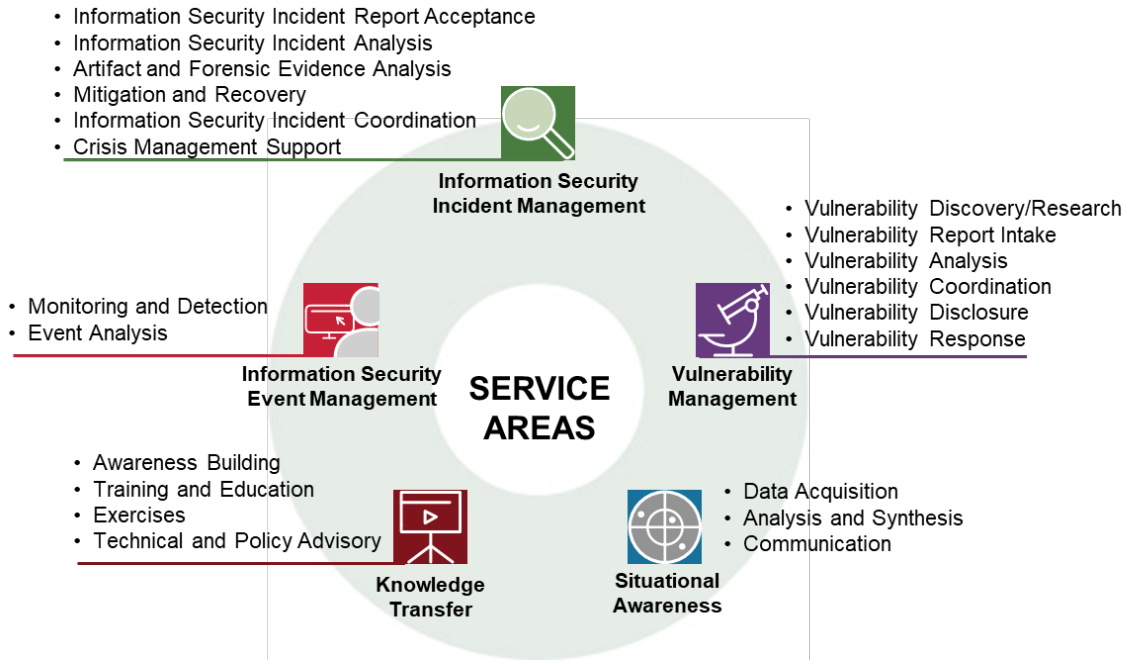
A sub-function is an activity or set of activities aimed at fulfilling the purpose of a particular function. Any sub-function might be shared and used in the context of several functions and/or services. Sub-functions might be optionally performed or required for any of those functions and/or services.

A sub-function is also described by the following template:

- A “Description” field describing the sub-function
- A “Purpose” field describing the intent of the sub-function
- An “Outcome” field describing any measurable results of the sub-function

For the purpose of the CSIRT Services Framework no sub-functions have been fully described. Only a short characterization is given for each one.

Below figure displays (next page) the CSIRT Services Framework Service Areas and Services. A full table of service areas, services and functions is available as Appendix 4.


• Information Security Incident Report Acceptance
• Information Security Incident Analysis
• Artifact and Forensic Evidence Analysis
• Mitigation and Recovery
• Information Security Incident Coordination
• Crisis Management Support
Information Security Incident Management
• Vulnerability Discovery/Research
• Vulnerability Report Intake
• Vulnerability Analysis
• Vulnerability Coordination
• Vulnerability Disclosure
• Vulnerability Response
Vulnerability Management
• Monitoring and Detection
• Event Analysis
Information Security Event Management
SERVICE AREAS
• Awareness Building
• Training and Education
• Exercises
• Technical and Policy Advisory
Knowledge Transfer
• Data Acquisition
• Analysis and Synthesis
• Communication
Situational Awareness

5 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.[4]

The following services are considered as offerings of this particular service area:

- Monitoring and detection
- Event analysis

5.1 Service: Monitoring and detection

Purpose: Implement automated, continuous processing of a wide variety of information security event sources and contextual data in order to identify potential information security incidents, such as attacks, intrusions, data breaches or security policy violations.

Description: Based on logs, NetFlow data, IDS alerts, sensor networks, external sources, or other available information security event data, apply a range of methods from simple logic or pattern matching rules to the application of statistical models or machine learning in order to identify potential information security incidents. This can involve a vast amount of data and typically, but not necessarily, requires specialized tools such as Security Information and Event Management (SIEM) or big data platforms to process. An important objective of continuous improvement is to minimize the number of false alarms that need to be analyzed as part of the Analyzing service.

Outcome: Potential information security incidents are identified for analysis as part of the Analyzing service.

The following functions are considered to be part of the implementation of this service:

- Log and sensor management
- Detection use case management
- Contextual data management

5.1.1 Function: Log and sensor management

Purpose: Manage log sources and sensors.

Description: Sensors and log sources need operational management throughout their lifecycle. They must be deployed, onboarded, and decommissioned. Outages, data quality/scope, and configuration

[4] Although this 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.

issues must be identified and resolved. Sensors that have some form of configuration such as pattern definitions need their configuration maintained in order to remain effective. Sensors may also include external detection services or Open-Source Intelligence (OSINT) sources, if they form the basis for detection use cases.

Outcome: A reliable stream of relevant information security events is available as input for detection use cases.

5.1.2 Function: Detection use case management

Purpose: Manage the portfolio of detection use cases through their entire lifecycle.

Description: New detection approaches are developed, tested, and improved, and eventually onboarded into a detection use case in production. Instructions for analyst triage, qualification, and correlation need to be developed, for example in the form of playbooks and Standard Operating Procedures (SOPs). Use cases that do not perform well, i.e., that have an unfavorable benefit/effort ratio, need to be improved, redefined, or abandoned. The portfolio of detection use cases should be expanded in a risk-oriented way and in coordination with preventive controls.

Outcome: A portfolio of effective detection use cases that are relevant to the constituency is developed.

5.1.3 Function: Contextual data management

Purpose: Manage of contextual data sources for detection and enrichment.

Description: The various contextual data sources that are involved in detection and enrichment need to be managed throughout their lifecycle. These can be live APIs to or exports from other IT systems such as a Configuration Management Database (CMDB), Identity and Access Management (IAM), or Threat Intel systems, or entirely separate data sets that need to be managed manually. The latter would be the case for indicator lists, watchlists and whitelists to suppress false positives.

Outcome: Up to date contextual data is available for both detection and enrichment.

5.2 Service: Event analysis

Purpose: Triage detected potential information security incidents and their qualification as information security incidents for escalation to the Information Security Incident Management service area or as false alarms.

Description: The flow of detected potential information security incidents must be triaged and each one qualified as an information security incident (true positive) or as a false alarm (false positive) using manual and/or automated analysis. This may require manual or automated gathering of additional information, depending on the detection use case. Priority should be given to the analysis of potentially more critical information security incidents to ensure timely reaction to what is most important. Structured qualification of detected potential information security incidents enables effective continuous improvement in a directed way by identifying detection use cases, data sources, or processes with quality issues.

Outcome: Qualified and correlated information security incidents are available as input to the Information Security Incident Management service area and false positives are qualified for continuous improvement.

The following functions are considered to be part of the implementation of this service:

- Correlation
- Qualification

5.2.1 Function: Correlation

Purpose: Identify events directly related to other potential or ongoing security incidents.

Description: Potential information security incidents pertaining to the same assets (e.g., systems, services, customers) or identities (e.g., users), or which are otherwise directly related to other potential information security incidents are grouped together and escalated as a single information security incident in order to avoid duplicate efforts. New potential information security incidents directly related to ongoing information security incidents are assigned to that information security incident instead of opening a new, separate information security incident.

Outcome: Grouping of related potential information security incidents for combined qualification or updating to an existing information security incident already handled by the Information Security Incident Management service area is performed.

5.2.2 Function: Qualification

Purpose: Triage and qualify detected potential information security incidents in order to identify, categorize, and prioritize true positives.

Description: Potential information security incidents need to be triaged and each qualified as an information security incident (true positive) or as a false alarm (false positive). Because analysts have a limited number of potential information security incidents they can analyze, and in order to avoid alert fatigue, automation is key. Mature tooling facilitates effective triage by enriching with context information, assigning risk scores based on the criticality of affected assets and identities and/or automatically identifying related information security events. Recurring cases that can be automated should be identified and automated. Potential information security incidents with higher criticality should be analyzed before less critical ones. In addition to qualification as true or false positives, a more fine-grained qualification is an important input for continuous improvement of detection use cases as well as the management of log sources, sensors, and contextual data sources. More fine-grained qualification can also support the definition of higher-quality KPIs for measuring the success of this service area.

Outcome: Qualified potential information security incidents are available for handling as part of the Information Security Incident Management service area.

6 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 services are considered as potential offerings of this service area:

- Information security incident report acceptance
- Information security incidents analysis
- Artefact and forensic evidence analysis
- Mitigation and recovery
- Information security incident coordination
- Crisis management support

6.1 Service: Information security incident report acceptance

Purpose: Receive and process reports of potential information security incidents from constituents, from Information Security Event Management services or third parties.

Description: For a CSIRT, the most important task is the acceptance of reports about information security events and potential information security incidents affecting networks, devices, components, users, organizations, or infrastructure—referred to as the “target”—inside the constituency. The CSIRT should anticipate that potential information security incidents may be reported from various sources in various formats, both manually and automatically.

To enable constituents to report information security incidents more effectively, the CSIRT should provide one or more mechanisms as well as guidance or instructions on what and how to securely report information security incidents. Reporting mechanisms can include email, a website, a dedicated information security incident reporting form or portal, or other appropriate methods to enable reports to be submitted safely and securely. Reporting guidance, if not included as part of an information security incidents reporting form itself, should be provided in separate documentation or via a

webpage, and should list the specific information that is desirable for inclusion in the report.

Due to the potentially large number of automatically escalated potential information security incidents detected via an Information Security Event Management service, this must be planned for in advance of adopting such interfaces or authorizing constituents to use them.[5]

Outcome: The information security incident report is received with professional and consistent intake of each report as well as its initial validation and classification.

The following functions are considered to be part of the implementation of this service:

- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing

6.1.1 Function: Information security incident report receipt

Purpose: Accept or receive information about an information security incident, as reported from constituents or third parties.

Description: Effective intake of information security incident reports requires mechanisms and processes to receive the reports from constituents, stakeholders, and third parties (e.g., finders, researchers, ISACs, other CSIRTs). Information security incident reports may include affected devices/networks/users/organizations, conditions already identified like exploited vulnerabilities, impact both on technical and business level, and actions that have been taken to start remediation and/or mitigation steps and potentially resolution. Occasionally, information security incident information may be received jointly as part of the input to other services, most namely the Vulnerability Report Intake (e.g., if an information security incident is reported that has been identified while analyzing a vulnerability report). Automatically submitted reports might or might not be acknowledged pending further choices of the implemented interfaces and protocols.

Outcome: Information security incident reports are appropriately handled from constituents or third parties, including the initiation of documenting or tracking the reports

The following sub-functions are considered to be part of this function:

- Monitoring communications channels regularly and check whether the advertised means of contacting the CSIRT are operational and reports can be submitted
- Reporting initial acknowledgement to the submitter of the information security incident report, requesting additional information if needed, and setting expectations with the reporter

6.1.2 Function: Information security incident triage and processing

Purpose: Initially review, categorize, prioritize, and process a reported information security incident.

[5] As is to be expected for all services related to the intake of information and data, there are many similarities. It is therefore common to combine such services from several service areas offered into one service/function. As this is not mandatory and there is no set combination of service areas, we have chosen to keep such services separate within the CSIRT Services Framework, although each team is free to choose the best organizational model for its own setup.

Description: Information Security Incident Reports are reviewed and triaged to obtain an initial understanding of the information security incident in question. It is of particular importance whether it has a real information security impact on the target and can result (or has already resulted) in damage to the confidentiality, availability, integrity, and/or authenticity of information assets or other assets. Depending on the amount of detail and quality of the information provided in the initial report, it may or not be obvious whether a real information security incident has occurred or if there is a different reason—such as misconfiguration or hardware failure. The next step will be determined on the basis of the preliminary assessment (e.g., process the report for further analysis; seek additional information from the reporter or other sources; decide that the report needs no further action or is a false alarm).

It is possible that attacks may originate from within the constituency of a CSIRT, may target this constituency, or the constituency is affected by collateral effects only. If the CSIRT does not provide Information Security Management services for the identified targets, then the report should be forwarded securely to an external group for handling, such as the affected organization(s) or CSIRT(s).

Unless there is a reason to decline an information security incident report or the report has been forwarded to another entity responsible for its handling, the report should be passed on to the Vulnerability Analysis service for further review, analysis, and handling.

Outcome: It can be determined if a reported matter is indeed an information security incident that needs to be handled by the CSIRT or passed on to a relevant entity.

The following sub-functions are considered to be part of the implementation of this service:

- Processing 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
- Updating acknowledgement of reports by providing some feedback on further steps based on categorization or prioritization results available
- Merging new information about already handled information security incidents to the available data to allow a consistent analysis and processing

6.2 Service: Information security incident analysis

Purpose: Analyze and gain an understanding of a confirmed information security incident.

Description: This service consists of functions to gain an understanding of the information security incident and its actual and potential impact to identify the underlying issues or vulnerabilities or weaknesses (root causes) that allowed the successful attack, compromise, or exploit.

Detailed analysis is often complex and time-consuming. The objective is to identify and characterize the information security incident in as much detail as required or justified by the current understanding of its impact. Information security incidents can be characterized by scope, affected entities, tools, or attacks deployed, timelines, etc. This service may continue in parallel while the Information Security Incident Coordination service and functions are occurring, or mitigation/recovery actions are taken.

The CSIRT may use other information and its own analysis (see below for some options) or knowledge available from vendors and product security teams or security researchers to better understand what has happened and what steps to take to remedy losses or damage.

Outcome: Knowledge is increased of the key details of an information security incident (e.g., description, impact, scope, attacks/exploits, and remedies).

The following functions are considered to be part of the implementation of this service:

- Information security incident triage (prioritization and categorization)
- Information collection
- Detailed analysis coordination
- Information security incident root cause analysis
- Cross-incident correlation

6.2.1 Function: Information security incident triage (prioritization and categorization)

Purpose: Categorize, prioritize, and create an initial assessment of an information security incident.

Description: The Analyzing Information Security Incidents service begins with a review of the available information to categorize, prioritize, and assess the impact an information security incident has on the involved systems relevant to the CSIRT's mandate. Some of this may have been documented during the Information Security Incident Report Triage and Processing function (of the Information Security Incident Report Intake service) if the information security incident was reported to the CSIRT by a constituent or third party.

If prior triage has not already been completed, the information security incident may be assigned to a subject matter expert who can provide technical confirmation that it has some impact on the involved systems and is relevant to the CSIRT's mandate (i.e., a potential security impact on networks or systems that can result in damage to the confidentiality, availability, or integrity of information assets in an area the CSIRT according to its mandate).

Outcome: The information record of an information security incident is categorized, prioritized, and updated.

6.2.2 Function: Information collection

Purpose: 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.

Description: Enable the collection of all valuable information to obtain the best understanding of the context, so that the origin and the content of the information can be appropriately evaluated and tagged to be used for any further processing.

While collecting information, the agreed sharing policies and limitations of what data can be used in which context or for what form of processing must be accepted and adhered to. Also, the collection

mechanisms and procedures must ensure that proper labeling and attribution of sources is used in order to later validate the origins as well as the appropriateness or authenticity.

Outcome: Structured information about collected digital and non-digital data or metadata is available, with tracking information and points of control of the integrity of both handling and storage. Depending on whether the results will be used for future (informal) analysis or law enforcement activities, different requirements exist in regard to establishing a formal chain of custody that can be defended in court at some later stage.

The following sub-functions are considered to be part of the implementation of this function:

- Evaluation and validation of information sources providing data and information
- Collection of reports regarding malicious or suspicious events, information security events, escalated potential information security incidents, and/or information security incident reports from constituents and third parties (such as other security teams or commercial intelligence feeds), whether manual, automated, or machine-readable forms
- Gathering and cataloging of digital data that may be, but are not guaranteed to be, useful in understanding incident activity (e.g., disk and memory images, files with metadata or checksums, network architecture characteristics, logs); this includes but is not limited to artefacts believed to be remnants of adversary activity
- Gathering and cataloging of non-digital data (e.g., physical sign-in sheets, architecture diagrams, business models, site assessment data, policies, enterprise risk frameworks)
- Gathering and cataloging of metadata regarding the source, method of collection, persons having handled data or objects, owner, and custody information especially as it may be viewed as evidence for forensic analysis or law enforcement activities later on

6.2.3 Function: Detailed analysis coordination

Purpose: Initiate and track any other technical analysis in regard to an information security incident.

Description: As more detailed technical analysis may be required; such analysis may be executed by other experts (inside or outside the host organization or CSIRT) or other third parties (such as a service provider specialized in such analysis). This requires initiating and tracking such activities up to the successful delivery of the desired analysis.

Outcome: A list of pending and—from the viewpoint of the incident handler coordinating the response to any given information security incident—outsourced analysis is available.

6.2.4 Function: Information security incident root cause analysis

Purpose: Identify the root cause of the information security incident, identifying the circumstances that allowed the exploited vulnerabilities to exist or that allowed the exploitation to succeed (including but not limited to user behavior).

Description: This function involves the process and actions required to understand the architecture, usage, or implementation flaw(s) that caused or exposed systems, networks, users, organizations, etc. to the kind of attack or exploit or compromise as exercised against the targets of an information

security incident. It is also concerned with the circumstances in which an attacker could compromise more systems based on the initial access to gain further access.

Depending on the nature of the information security incident, it may be difficult for a CSIRT to perform this function thoroughly. In many situations, this function may best be conducted by the affected target itself, as especially in the context of Coordinating CSIRTs no detailed technical knowledge is available about systems or networks that have been compromised.

Outcome: The information security incident and the way in which malicious actors initially gained access and used it further on is understood so that remediation or mitigation methods can be determined to minimize the risk of future exposure or exploitation by eliminating the root causes.

6.2.5 Function: Cross-incident correlation

Purpose: Enable the usage of all available information to get the best understanding of the context and detect interrelationships that otherwise would not have been recognized or acted upon.

Description: This function involves the correlation of available information about multiple information security incidents to determine interrelations, trends, or applicable mitigations from already closed information security incidents to improve the response to currently handled information security incidents.

Outcome: The bigger picture is understood in terms of situational awareness based on a detailed knowledge about similarities and confirmed or suspected interrelationships of otherwise independent information security incidents.

6.3 Service: Artifact and forensic evidence analysis

Purpose: Analyze and gain an understanding of artefacts related to a confirmed information security incident, taking into consideration the need to preserve forensic evidence.

Description: The services related to the understanding of the capabilities and intent of artefacts (e.g., malware, exploits, volatile memory dumps or disk copies, applications codes, logs, documents), their delivery mechanisms, their propagation, their detection, their mitigation, and their disarming or neutralization. This applies to any formats and sources: hardware, firmware, memory, software, etc. Any artefact or evidence must be preserved and collected without any modification and kept in isolation. As some artefacts and data may become evidence in the context of law enforcement activities, specific regulations or requirements may apply.

Even without preserving a chain-of-custody, this service usually involves complex and time-consuming tasks, and requires expertise, setting up dedicated and monitored analysis environments--with or without external accesses from standard wired or wireless networks (such as performing the forensics activities in a sealed or Faraday room), logging of activities, and compliance with procedures.

As part of the handling of information security incidents, 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 analysis is carried out in order to find out some or all of the information listed below, which is not considered to be a complete list:

- The context required of the artefact to run and to perform its intended tasks, whether malicious or not
- How the artefacts may have been utilized for the attack: uploaded, downloaded, copied, executed, or created within an organization's environments or components
- Which systems have been involved locally and remotely to support the distribution and actions
- What an intruder did once to access to the system, network, organization, or infrastructure was established: from passively collecting data, to actively scanning and transmitting data for exfiltration purposes, or collecting new action requests, updating itself or making a lateral movement inside a compromised (local) network
- What a user, user process, or user system did once the user account or user device was compromised
- What behavior characterizes the artefacts or compromised systems, either in standalone mode, in conjunction with artefacts or components, connected to a local network or the Internet, or in any combination
- How the artefacts or compromised systems establish connectivity with the target (e.g., intrusion path, initial target, or detection evasion techniques);
- What communication architecture (peer-to-peer, command-and-control, both) has been utilized
- What were the actions of the threat actors, what is their network and systems footprint
- How the intruders or artefacts evaded detection (even over long periods of time which may include reboot or reinitialization)

This can be achieved through various types of activities including

- media or surface analysis
- reverse engineering
- runtime or dynamic analysis
- comparative analysis

Each activity provides additional information about the artefacts. Analysis methods include but are not limited to identification of type and characteristics of artefacts, comparison with known artefacts, observation of artefact execution in a runtime or a live environment and disassembling and interpreting binary artefacts.

In carrying out an analysis of the artefacts, an analyst attempts to reconstruct and determine what the intruder did, in order to detect the exploited vulnerability, assess damages, develop solutions to mitigate against the artefacts, and provide information to constituents and other researchers.

Outcome: The nature of recovered digital artefacts and analyzed forensic evidence is understood along with the relationship to other artefacts, internal or external objects or components, attacks on frameworks, tools, and exploited vulnerabilities. Working assumptions or proof of what the threat actor did, and how the artefacts behaved. This knowledge is critical to assess losses, damages, business

impacts, etc. and to develop containment and mitigation or recovery strategies. The tactics, techniques, and procedures used by attackers or intruders to compromise systems, users, networks, organizations and/or infrastructures is understood. This includes those tactics, techniques, and procedures used to propagate, exfiltrate, update, modify, or fake its behavior, data, auto-delete traces of its own activities, or carry out additional malicious activities.

List of functions which are considered to be part of the implementation of this service:

- Media or surface analysis
- Reverse engineering
- Runtime or dynamic analysis
- Comparative analysis

6.3.1 Function: Media or surface analysis

Purpose: Compare information gathered from the artefact with other public and private artefacts and/or signature repositories.

Description: This function involves identification and characterization of basic information and metadata about artefacts, including but not limited to file types, string outputs, cryptographic hashes, certificates, file sizes, file/directory names. As all available information is gathered and analyzed further, this may be used to review any public/open or private/closed source information repositories to learn more about the artefact or its behavior, as such information can be used to determine the next steps.

Outcome: Identify Characteristics and/or the signature of digital artefact are identified, and any information already known about the artefact including maliciousness, impact, and mitigation.

6.3.2 Function: Reverse engineering

Purpose: Perform in-depth static analysis of an artefact to determine its complete functionality, regardless of the environment within which it may be executed.

Description: To provide a deeper analysis of malware artefacts to include identifying hidden actions and triggering commands. Reverse engineering allows the analyst to dig past any obfuscation and compilation (for binaries) and identify the program, script, or code that makes up the malware, either by uncovering any source code or by disassembling the binary into assembly language and interpreting it. The analyst uncovers all of the machine language exposed functions and actions the malware can perform. Reverse engineering is a deeper analysis that is carried out when surface and runtime analysis do not provide the full information needed.

Outcome: Complete functionality of a digital artefact is derived to understand how it operates, how it is triggered, related system weaknesses that can be exploited, its full impact, and potential damage, in order to develop solutions to mitigate against the artefact and, if appropriate, create a new signature for comparison with other samples.

The following sub-functions are considered to be part of the implementation of this function:

- Static analysis

- Code reverse engineering
- Potential behavior analysis and description
- Potential signature design

6.3.3 Function: Run time or dynamic analysis

Purpose: Provide insight into the artefact's operation.

Description: This function involves understanding of an artifact's capabilities via observation while running the sample in a real or emulated environment (e.g., sandbox, virtual environment, and hardware or software emulators).

Use of a simulated environment captures changes to the host, network traffic, and output from execution. The basic premise is to try to see artefact in operation in as close to a real-life situation as possible.

Outcome: Additional insight is gained into a digital artefact's operation by observing its behavior during execution to determine the changes to the affected host system, other system interaction, and resulting network traffic in order to better understand the system damage and impact, create new artefact signature(s), and determine mitigation steps.

Note: Not all functionality is apparent from runtime analysis, since not all code sections may be triggered. Runtime analysis only allows the analyst to see what the malware does in the test situation, not what it is fully capable of doing.

The following sub-functions are considered to be part of the implementation of this function:

- Preparing an analysis environment (live/restricted/closed, emulated/simulated)
- Preparing collectors, sensors and/or probes
- Collecting initial behavior data and metadata
- Probing the artefact at multiple times in various contexts
- Carry out a system and/or network behavior analysis, both short-term and long-term
- Drawing conclusions by evaluating all results and data gathered, comparing the various results, and researching available knowledge bases for existing technical results matching the findings

6.3.4 Function: Comparative analysis

Purpose: Perform an analysis focused on identifying common functionality or intent, including family analysis of catalogued artefacts.

Description: This function involves exploring an artefact's relationship to other artefacts. This may identify similarities in code or modus operandi, targets, intent, and authors. Such similarities can be used to derive the scope of an attack (e.g., is there a larger target, has similar code been used before).

Comparative analysis techniques can include exact match comparisons or code similarity comparisons. Comparative analysis provides a broader view of how the artefact or similar versions of it were used and changed over time, helping to understand the evaluation of malware or other malicious types of artefacts.

Outcome: Any commonalities or relationships to other artefacts are derived in order to identify trends or similarities that may provide additional insights or understanding of a digital artefact's functionality, impact, and mitigation.

The following sub-functions are considered to be part of the implementation of this function:

- Defining a baseline of characteristics and observed behaviors
- Searching for the same or similar characteristics in available repositories/knowledge bases
- Updating available repositories/knowledge bases regarding newly observed or previously unknown symptoms, behaviors, and/or signatures which can be used to further categorize the researched artefact.

6.4 Service: Mitigation and recovery

Purpose: 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.

Description: Once the analysis has confirmed a potential information security incident and a response strategy has been developed, this must be turned over into a response plan. Even before a response plan can be finalized, ad-hoc measures may be taken. This service also includes the initiating and tracking of all activities which are performed until the information security incident can be considered closed or new information becomes available that requires further analysis and henceforth may also change the response strategy and plan.

Outcome: The information security incident is mitigated, and the cyber security posture is improved. Integrity of systems impacted by the underlying attack or activities of the attacker is restored, as well as serviceability of the network and systems compromised. Data is restored in case of data loss, if possible.

The following functions are considered to be part of the implementation of this service:

- Response plan establishment
- Ad hoc measures and containment
- Systems restoration
- Other information security entities support

In the case of a coordinating CSIRT, not all functions will be provided. While "supporting other information security entities" is an activity such teams provide, they sometimes also help with "establishing a response plan."

6.4.1 Function: Response plan establishment

Purpose: Define and enforce a plan to restore the integrity of affected systems and return the affected data, systems, and networks to a non-degraded operational state, restoring the impacted services to full functionality without recreating the context of enabling the original security issue to be exploited again.

Description: Without fully understanding the business impact and requirements to mitigate and recover, no meaningful response will be provided. As there is a conflict of interest—tracking the attack to gain more intelligence vs. containing the attack to avoid further losses—it is necessary to take all interests into consideration and work out a response plan that is plausible to address the known facts and provide the desired outcome within the required timeframe.

As with all plans, it must be considered that whenever new analysis results become available, the new findings need to be reviewed. Indeed, the response plan will usually need to be changed to provide continuous orientation and guidance. But without such plan—unless the response is handled by one small organizational group with little requirement of external interfaces or other entities—the activities might not be carried out effectively or efficiently due to a lack of coordination.

Outcome: An agreed response plan that meets business requirements if aided by available resources and support, which will then be executed. Tracking and coordination by a CSIRT would be provided by the "Coordination" service.

The following sub-functions are considered to be part of the implementation of this function:

- Determine the business impact of the information security incident
- Determine the business requirements and timeframe for a successful recovery
- Define decision processes and criteria (if not already defined by policies)
- Identify the objects to be recovered: environments, systems, applications, systems, transversal functions, etc.
- Identify required support and actions by internal and external entities
- Determine a response plan that provides for a meaningful response within the desired business requirements and timeframe based on available resources and the technical scope of required actions

6.4.2 Function: Ad hoc measures and containment

Purpose: Implement measures that ensure an information security incident does not spread any further, i.e., remains confined to the currently affected system, users, and/or domains to ensure that no further losses (including leakage of documents, changes to databases or data, etc.) can occur.

Description: The immediate challenge in case of an information security incident is to stop it from spreading. While systems are compromised or malware is active on end user systems, further data losses and more compromises occur. It is usually the main objective of attacks to reach out to specific data and systems, including attacks (including but not limited to lateral movements) to other organizations both inside and outside the organization suffering from the information security incident. Stopping or at least limiting the extent of any malicious activities or further losses requires short-term actions such as blocking or filtering traffic and removing access to specific services or systems and can also result in the disconnection of critical systems.

Denying further access to potentially critical evidence data will allow a full analysis of such evidence. Denying further access to other systems and networks will also limit the exposure from liability as a result of damage done to other organizations.

Stopping immediate damage and limiting the extent of malicious activity through short-term tactical actions (for example, blocking or filtering traffic) can also involve regaining control of systems. As long as attackers or active malware have ready access to more systems or networks, no return to normal operation will be possible.

Outcome: Control of systems and networks involved is regained. Access is denied for attackers and malware to data, systems, and networks in order to avoid more attacks and/or compromised systems and data.

The following sub-functions might be part of the implementation of this function:

- Temporarily remove access for users/systems/services/networks
- Temporarily disconnect systems or networks from networks or backbones
- Temporarily disable services
- Require users to change their passwords or crypto credentials
- Monitor for signs of intrusions and indicators of compromise
- Verify that all users/systems/services/networks are unaffected

6.4.3 Function: System restoration

Purpose: Implement changes in the affected domain, infrastructure, or network necessary to fix and prevent this type of activity from reoccurring.

Description: Restore 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.

Outcome: Measures are applied to restore the systems and services to full functionality as well as capacity. Measures are applied to close any detected vulnerabilities or weakness that contributed to the original information security incident. Detection and reaction measures are improved as recommended by the analysis and response plan.

The following sub-functions are considered to be part of the implementation of this function:

- 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

6.4.4 Function: Other information security entities support

Purpose: Enable the constituents to perform the required management and technical activities in order to successfully mitigate an information security incident and recover from it.

Description: A CSIRT may provide direct (onsite) assistance to help the constituents to recover from losses and to remove vulnerabilities. This might be a direct extension of offering analysis services on-site (see above). On the other hand, a CSIRT might choose to support the staff of the constituents responding to the information security incident with more detailed explanations, recommendations, etc.

Outcome: Response of the constituents is improved, and recovery is faster. By adding to the available body of knowledge the future effectiveness and efficiency of related activities may be strengthened. In addition, it helps to support those entities inside the constituency that are lacking detailed technical knowledge to carry out the necessary action to respond.

6.5 Service: Information security incident coordination

Purpose: Ensure timely notifications and accurate information distribution; keep the information flow and track the status of activities of entities that are either tasked or requested to participate in responding to the information security incident; and make sure the response plan is carried out and deviations caused by both delays or new information are managed accordingly.

Description: Being notified and kept informed about the details and ongoing activities in relation to an information security incident is critical for all stakeholders and organizations involved. As some activities required for a successful mitigation and recovery might involve management approval, this requires suitable escalation and reporting functions established before any information security incident can be handled effectively and efficiently. As the CSIRT analyzes all information as it becomes available, coordination makes sure that notifications and information reach the right points of contact, track their responses, and make sure that all parties carrying out activities report back to provide for accurate situational awareness until the information security incident is considered closed and requiring no further coordination.

Stakeholders should have avenues to submit questions, check the status of information security incidents, and report issues to the CSIRT. To engage internal stakeholders, the CSIRT should provide communications channels to advertise the remediation status of information security incidents. To engage external stakeholders, the CSIRT should maintain communications channels to other CSIRTs and CSIRT communities that might provide recommendations or technical support.

Outcome: The response is successfully coordinated based on well-informed entities that contribute to the response to an information security incident.

The following functions are considered to be part of the implementation of this service:

- Communication
- Notification distribution
- Relevant information distribution

- Activities coordination
- Reporting
- Media communication

6.5.1 Function: Communication

Purpose: Engage effectively with stakeholders and establish appropriate multiple communication channels providing the required confidentiality.

Description: A CSIRT must account for the most accurate audience as communications are crafted and released. In return, a CSIRT must also be equipped to receive incoming feedback, reports, comments, and questions from a variety of sources based on its own communication.

The security policy and the information sharing policy may require information to be handled in a strict manner. The CSIRT must be able to share with stakeholders in a reliable, secure, and private manner, both externally and internally.

Non-disclosure agreements must be set up as far in advance as possible and communication resources set up accordingly. As an extension, the concept of "information under embargo" can also be used. Hence, a retention policy must also be established to ensure that both the data used to craft the information and the information itself are properly handled, shared, and kept based on constraints—such as time—until these constraints become void or the information is publicly disclosed.

Communication channels can take multiple forms based upon the needs of stakeholders and constituents. All information communicated must be tagged according to the information sharing policy. Traffic Light Protocol may be utilized.

Outcome: All communication channels are available according to the security requirements of all receiving and sending parties.

The following sub-functions are considered to be part of the implementation of this function:

- Provide internal communication channels
- Provide external communication channels

6.5.2 Function: Notification distribution

Purpose: Alert entities impacted by the information security incident or those that can contribute to the response to it and provide those entities with the required information to understand their role of involvement and any expectations that might exist regarding their cooperation and support.

Description: A security incident touches on many internal and potentially external entities and, possibly, systems, and networks. As CSIRTs are a central point for receiving reports of potential information security incidents, they also serve as a hub for notifying authorized points of contact about them. The notification usually will provide not only the appropriate technical details but also information about the expected response and a point of contact for any fellow-up.

Outcome: Information about an information security incident is available to entities required to either take part in the response or to be informed about it.

6.5.3 Function: Relevant information distribution

Purpose: Keep communicating with the identified entities and provide a suitable flow of available information in order to enable those entities to benefit from available insights and lessons learned, to apply improved responses or take new ad-hoc measures.

Description: As the response to an information security incident progresses, more analysis results and reports from potentially other security experts, CSIRTs, or victims become available.

It may be helpful to pass some of the information and lessons learned on to the Knowledge Transfer Service Area (if supported) to improve training and technical documents as well as to help create appropriate awareness, especially if new attacks or incident trends are identified.

Outcome: Available information is distributed to those either responsible for taking part in the response or requiring to be kept informed about the progress and current status.

6.5.4 Function: Activities coordination

Purpose: Track the status of all communication and activities.

Description: As many entities are potentially involved in responding to an information security incident, it is necessary to track the status of all communication and activities. This involves the actions requested by a CSIRT or requests for sharing of further information as well as requests for technical analysis of artefacts s or the sharing of indicators of compromise, information about other victims, etc. This primarily occurs when the CSIRT is reliant on expertise and resources outside of the direct control of the CSIRT to effectuate the actions necessary to mitigate an incident. But it also occurs inside larger organizations for which an internal CSIRT coordinates the mitigation and recovery activities.

By offering bilateral or multilateral coordination, the CSIRT participates in the exchange of information to enable those resources with the ability to take action to do so or to assist others in the detection, protection, or remediation of ongoing activities from attackers and help to close the information security incident.

Outcome: Situational awareness is developed of the current status of all activities and status of the entities that take part in the response.

6.5.5 Function: Reporting

Purpose: Ensure that all involved entities within a business have information about the status of current activities so that further decisions about the next steps to be taken are based on the best situational awareness available.

Description: Delivering concise and factual information about the current status of activities requested or carried out in response to an information security incident. Instead of waiting to be pulled for such information as part of an ongoing coordinated action as required for any successful response, timely reports are critical to enable effective coordination.

Outcome: Internal stakeholders are apprised of the scope of current activities, actions already completed, and pending ones. The assessed impact of delays, recommendations and requested actions is also communicated, making it possible to understand the overall impact in regard to the selected response strategy and developed plan.

6.5.6 Function: Media communication

Purpose: Engage with the (public) media to be able to provide accurate and easy-to-understand factual information about ongoing events to avoid the spread of rumors and misleading information.

Description: Communicating with the media is unavailable 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 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.

Outcome: Factual information providing a clear summary of the ongoing information security incident is developed including steps to be taken by potential victims or outlining the chosen response strategy to recover from the information security incident.

6.6 Service: Crisis management support

Purpose: Provide expertise and contacts to other security experts, CSIRTs, and CSIRT communities in order to help mitigate the crisis.

Description: While today's information security incidents rarely constitute an organizational or national crisis, they have the potential to do so. But the response to a crisis is usually associated with an emergency that threatens the well-being of humans and society at large, or at least the existence of an organization. As it is established in crisis management, a high-ranking role will take over the responsibility of a crisis, thereby changing the usual line of command for the duration of the emergency.

As the systems and networks might contribute to emergencies or are required to be available to respond to a crisis situation, a CSIRT will usually be a critical resource for managing such situations and provide valuable experience but also the established services and networks of points of contacts.

Outcome: The crisis management team can use the CSIRT's resources to address the cyber security aspects of the current crisis. At the same time, the CSIRT's communication resources can be utilized to reach out to constituents and external parties to ask for specific support actions or help. It can also be used to communicate in a trusted way towards constituents, using established communication means and trusted networks.

The following functions are considered to be part of the implementation of this service:

- Information distribution to constituents
- Information security status reporting
- Strategic decisions communication

6.6.1 Function: Information distribution to constituents

Purpose: Provide established communication resources to help respond to the crisis.

Description: 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.

Outcome: Available information is distributed to constituents, benefiting from established trust relationships that help to reassure recipients of the accurateness of the information disseminated.

6.6.2 Function: Information security status reporting

Purpose: Ensure that the crisis management team has a complete overview of current information security incidents and known vulnerabilities to consider this as part of its overall priorities and strategies.

Description: The function involves delivering concise and factual information about the current status of cyber security inside the constituency. As a crisis might be used to start other attacks or as occurring attacks might be part of the overall activities leading this crisis, it is very important for the crisis management team to establish complete situational awareness.

The CSIRT can provide such situational awareness for its services and constituents. This may either be requested or is expected by standard policies in a time of crisis. In any case, as crisis management is only successful based on the established information flow as it depends on coordinate resources to address the most critical aspects of the crisis, reporting must be timely and accurate.

As ongoing information security incidents will require resources to handle them, a decision must be taken to either discontinue the response for the duration of the incident (and allocate the now available resources to other areas) or to carry on. Reasonable decisions can only be taken based on the best situational awareness available.

Outcome: The crisis management team will be apprised of the scope of current activities, actions already completed, and pending ones. The assessed impact of delays, recommendations and requested actions are also communicated, allowing to understand the overall impact in regard to the selected strategy to address the current crisis.

6.6.3 Function: Strategic decisions communication

Purpose: Inform other entities in a timely manner about the impact caused by the crisis on currently open information security incidents.

Description: 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 stop their support or interaction with the CSIRT as they might believe that the crisis is taking over.

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

Outcome: Information of the crisis impact on the CSIRT operation is distributed to constituents and other entities involved with responding to open information security incidents. The expectations of the CSIRT towards such entities are clearly described and ensure that the information needs of the CSIRT are clearly communicated.

7 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 this 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.

The following services are considered offerings of this service area:

- Vulnerability discovery / research
- Vulnerability report intake
- Vulnerability analysis
- Vulnerability coordination
- Vulnerability disclosure
- Vulnerability response

Few CSIRTs will provide all of these services, but instead will provide only those services in their realm of responsibility. For example, a CSIRT may limit its services to learning of a new vulnerability from public sources (Vulnerability Discovery/Research) or from third parties (Vulnerability Report Intake) and then issue a security advisory to its constituents (Vulnerability Disclosure) when needed, without necessarily participating in any coordination efforts with product vendors or others who develop a solution (Vulnerability Coordination) or being involved in directly deploying a fix (Vulnerability Response).

7.1 Service: Vulnerability discovery / research

Purpose: Find, learn of, or search for new (previously unknown) vulnerabilities; vulnerabilities can be discovered by members of the vulnerability management service area or through other related CSIRT activities

Description: Discovery of a new vulnerability is a necessary first step that starts the overall vulnerability management lifecycle. This service includes those functions and activities that a CSIRT may actively perform through its own research or other services to discover a new vulnerability. Functions and activities related to the passive receipt of new vulnerability information from someone else are described later in the Vulnerability Report Intake service. Occasionally a new vulnerability may be discovered by a CSIRT during other activities, such as while analyzing or investigating an incident report. Another means of learning of a new vulnerability is through reading public sources (e.g.,

websites, mailing lists[6]), other external sources (e.g., premium services, subscriptions), or by actively looking for vulnerabilities through deliberate research (e.g., through fuzz testing, reverse engineering). Such discoveries should be documented and fed into the organization's vulnerability handling processes, regardless of how the CSIRT discovered or learned of the vulnerability.

Outcome: This service results in an increased discovery of potential vulnerabilities that were not reported directly to the CSIRT.

The following functions are considered to be part of the implementation of this service:

- Incident response vulnerability discovery
- Public source vulnerability discovery
- Vulnerability research

These functions may be services (or functions) performed by others (e.g., researchers, vendors, PSIRTs, or third-party specialists) instead of the CSIRT.

7.1.1 Function: Incident response vulnerability discovery

Purpose: Identify a vulnerability that was exploited as part of a security incident.

Description: During the course of analyzing a security incident, information may be discovered that indicates that a vulnerability was exploited by the attacker. An incident may have been enabled through exploitation of a known vulnerability that was previously unpatched or unmitigated; or it may be due to a new (zero-day) vulnerability.

Some of this vulnerability information might be received as an output from one of the services of the Information Security Incident Management service area if a vulnerability was exploited as part of an incident. The information can then be passed on to the Vulnerability Triage function or the Vulnerability Analysis service, as appropriate.

Outcome: Information about a vulnerability that is suspected to have been exploited as part of a security incident is passed on to the Vulnerability Management service area.

7.1.2 Function: Public source vulnerability discovery

Purpose: Learn about a new vulnerability from reading public sources or other third-party sources.

Description: A CSIRT may initially learn about a new vulnerability from various public sources that announce such information. The sources can include vendor announcements, security websites, mailing lists, vulnerability databases, security conferences, social media, etc. This function may also learn of new vulnerabilities through other third-party sources that may not be completely open to the public, such as through paid subscriptions or premium services where information is shared with only a limited group. Staff may be assigned the responsibility to perform this function and collect information to organize it for further review and sharing. Similar vulnerability information might also be received

[6] New vulnerability information received by email may be considered to be an activity of either the Vulnerability Discovery service, Public Source Vulnerability Discovery function, Vulnerability Report Intake service, or of the Vulnerability Report Receipt function, depending on the CSIRT's internal processes or on how broadly the vulnerability information was distributed.

from the services of the Situational Awareness service area.

Outcome: New vulnerabilities are identified that have been disclosed through public or other external sources.

7.1.3 Function: Vulnerability research

Purpose: Discover or search for new vulnerabilities as a result of deliberate activities or research.

Description: This function includes the discovery of new vulnerabilities as a result of specific CSIRT activities, such as the testing of systems or software using fuzz testing (fuzzing), or through the reverse engineering of malware.

This function may also receive input from the service(s) of the Information Security Incident Management service area or the Situational Awareness service area that would initiate this function to look for suspected vulnerabilities.

The discovery of a new vulnerability as a result of this vulnerability research function may become input to the Vulnerability Response service, Vulnerability Detection function (see sub-functions for Vulnerability Scanning and Vulnerability Penetration Testing).

Outcome: New vulnerabilities are identified through research.

7.2 Service: Vulnerability report intake

Purpose: Receive and process vulnerability information reported from constituents or third parties.

Description: One of the primary sources of vulnerability information may be reports or questions sent from a CSIRT's constituents or other third parties. The CSIRT should anticipate that vulnerabilities may be reported from these various sources, and provide a mechanism, a process, and guidance for vulnerability reporting. Reporting infrastructures may include email or a web-based vulnerability reporting form. Not all vulnerabilities are reported directly to a CSIRT by constituents or third parties through the established channels. Supporting guidance should include reporting guidelines, contact information, and any disclosure policies.

To enable constituents to report vulnerabilities more effectively, the CSIRT should provide one or more mechanisms as well as guidance or instructions on what and how to securely report vulnerabilities. Reporting mechanisms can include email, a website, a dedicated vulnerability reporting form or portal, or other appropriate methods to enable reports to be submitted safely and securely. Reporting guidance, if not included as part of a vulnerability reporting form itself, should be provided in separate documentation or via a web page, and should list the specific information that is desirable to be included in the report.

Outcome: The vulnerability report is received with professional and consistent intake of each report as well as its initial validation and classification.

The following functions are considered to be part of the implementation of this service:

- Vulnerability report receipt
- Vulnerability report triage and processing

7.2.1 Function: Vulnerability report receipt

Purpose: Accept or receive information about a vulnerability, as reported from constituents or third parties.

Description: Effective intake of vulnerability reports requires mechanisms and processes to receive the reports from constituents, stakeholders, and third parties (finders, researchers, vendors, PSIRTs, other CSIRTs or vulnerability coordinators, etc.). Vulnerability information may include affected devices, conditions necessary to exploit the vulnerability, impact (e.g., privilege escalation, data access, etc.), as well as actions taken to resolve the vulnerability, remediation and/or mitigation steps, and resolution. Occasionally, vulnerability information may be received jointly as part of the input to other services, most notably the Information Security Incident Report Intake (e.g., if a vulnerability is reported to be exploited as part of an incident report).

Outcome: Vulnerability reports from constituents or third parties are appropriately handled, including the initiation of documenting or tracking the reports.

The following sub-functions are considered to be part of this function:

- 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.

7.2.2 Function: Vulnerability report triage and processing

Purpose: Initially review, categorize, prioritize, and process a vulnerability report.

Description: Vulnerability Reports are reviewed and triaged 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). Depending on the amount of detail and quality of the information provided in the vulnerability report, it may or not be obvious whether a new vulnerability exists.

Unless there is a reason to decline a vulnerability report, the report should be passed on to the Vulnerability Analysis service for further review, analysis, and handling. If the CSIRT does not provide a Vulnerability Analysis service, then the report should be securely forwarded to an external group for handling, such as the affected vendor(s), PSIRT(s), or a vulnerability coordinator.

Outcome: Available information is identified to determine what to do next.

The following sub-functions are considered to be part of the implementation of this service:

- 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.

7.3 Service: Vulnerability analysis

Purpose: Analyze and gain understanding of a confirmed vulnerability.

Description: The Vulnerability Analysis service consists of functions aimed at gaining an understanding of the vulnerability and its potential impact, identifying the underlying issue or flaw (root cause) that allows the vulnerability to be exploited, and identifying one or more remediation or mitigation strategies to prevent or minimize the exploitation of the vulnerability.

The Vulnerability Analysis service and functions can continue in parallel while the Vulnerability Coordination service and functions occur with other participants in a coordinated vulnerability disclosure (CVD)[7] process.

Outcome: Knowledge of the key details of a vulnerability (e.g., description, impact, resolution) is increased.

The following functions are considered to be part of the implementation of this service:

- Vulnerability triage (validation and categorization)
- Vulnerability root cause analysis
- Vulnerability remediation development

7.3.1 Function: Vulnerability triage (validation and categorization)

Purpose: Categorize, prioritize, and perform an initial assessment of a vulnerability.

Description: The Vulnerability Analysis service begins with a review of the available information to categorize, prioritize, and assess whether a vulnerability has some impact on the involved systems and is relevant to the CSIRT's mandate. Some of this may have been documented during the Vulnerability Report Triage and Processing function (of the Vulnerability Report Intake service) if the vulnerability was reported to the CSIRT by a constituent or third party.

If prior triage has not already been completed, the vulnerability may be assigned to a subject matter expert who can provide technical confirmation that it has some impact on the involved systems and is relevant to the CSIRT's mandate (i.e., the potential security impact on networks or systems that can result in damage to the confidentiality, availability, or integrity of information assets in an area of the CSIRT according to its mandate).

Outcome: The information record of a vulnerability is categorized, prioritized, and updated.

7.3.2 Function: Vulnerability root cause analysis

Purpose: Understand the design or implementation flaw that causes or exposes the vulnerability to exist.

Description: The goal of this analysis is to identify the root cause of the vulnerability, identifying the circumstances that allow a vulnerability to exist, and in which circumstances an attacker can consequently exploit the vulnerability. This analysis may also attempt to understand the weakness(es)

[7] See the Vulnerability Coordination and Vulnerability Disclosure service areas for related information on coordinated vulnerability disclosure (CVD).

leveraged to instigate an incident and the adversarial tradecraft utilized to leverage that weakness. Depending on the nature of the vulnerability, it may be difficult for a CSIRT to perform this function thoroughly. In some cases, this function may have already been performed by the finder or reporter of the vulnerability. In many situations, this function may best be conducted by the product vendor or developer of the affected software or system or their respective PSIRT. It is also possible that a vulnerability is present in more than one product, in which case multiple analyses may be needed of the affected software or systems, requiring coordination with multiple vendors, PSIRTs, or stakeholders.

Outcome: Understanding of the vulnerability and the way in which malicious actors will be able to use this vulnerability is used to determine remediation or mitigation methods to minimize the risk of exposure or exploitation.

7.3.3 Function: Vulnerability remediation development

Purpose: Develop the steps necessary to fix (remediate) the underlying vulnerability or mitigate (reduce) the effects of the vulnerability from being exploited.

Description: This function will ideally identify a remediation or a fix for a vulnerability. If a vendor patch or fix is not available in a timely manner, a temporary solution or workaround, called a mitigation, may be recommended, such as disabling the affected software or making configuration changes, to minimize the potential negative effects of the vulnerability. Note that the actual application or deployment of a remediation (patch) or mitigation (workaround) is a function of a separate service, called Vulnerability Response in this framework.

As part of the Vulnerability Analysis service and Remediation Development, this function may optionally include other sub-functions or activities, such as validating the changing of a procedure or design, reviewing remediation by a third party, or identifying any new vulnerabilities introduced in the remediation steps. Vulnerabilities that are not remediated or mitigated should be documented as acceptable risks.

This function will often receive information or input from the affected product's vendor(s), sometimes as part of the initial report or announcement handled by other services or functions.

Outcome: A plan is established to change (patch) the software code, implement a workaround, or to improve processes, infrastructures, and/or designs to close the specific attack vector and to prevent the vulnerability from being exploited.

The following sub-functions are considered to be part of this function:

- Vulnerability remediation/patch development
- Vulnerability mitigation development

This function is typically performed by other entities (e.g., product vendors, PSIRTs).

7.4 Service: Vulnerability coordination

Purpose: Exchange information and coordinate the activities with participants involved in a coordinated vulnerability disclosure (CVD) process.

Description: The handling of most vulnerabilities involves notifying, working with, and coordinating the

exchange of relevant information with multiple parties including vulnerability finders/reporters, affected vendors, developers, PSRITs, or other trusted experts (e.g., researchers, CSIRTs, vulnerability coordinators) who can work together to analyze and fix the vulnerability.

Outcome: Information sharing with CVD participants who can assist in providing information to remediate/mitigate the vulnerability is effective and timely.

The following functions are considered to be part of the implementation of this service:

- Vulnerability notification/reporting
- Vulnerability stakeholder coordination

7.4.1 Function: Vulnerability notification/reporting

Purpose: Initial share or report new vulnerability information with others who are to be involved in the CVD process.

Description: The handling of most vulnerabilities involves notifying, working with, and coordinating the exchange of relevant information with multiple parties including the affected vendors, developers, PSIRTs, or other trusted experts (e.g., researchers, CSIRTs, vulnerability coordinators) who can work together to analyze and fix the vulnerability.

Outcome: Vendors (or other CVD participants) are informed about a vulnerability and can act to develop a remediation or mitigation solution.

7.4.2 Function: Vulnerability stakeholder coordination

Purpose: Conduct follow-on coordination and sharing of information among the various stakeholders and participants involved in coordinated vulnerability disclosure (CVD) efforts.

Description: Coordinate the exchange of information among the finders/researchers, vendors, PSIRTS, and any other participants in the coordinate vulnerability disclosure (CVD) efforts to analyze and fix the vulnerability and prepare for the disclosure of the vulnerability. This coordination should also include agreement by participants on the timing and synchronization of the disclosure.

Outcome: Vulnerability information is more effectively, timely, and responsibly shared among participants who can develop or announce a remediation/mitigation solution.

The following sub-functions are considered to be part of this function:

- Vulnerability publication development

7.5 Service: Vulnerability disclosure

Purpose: Disseminate information about known vulnerabilities to constituents so that they can act upon that information to prevent, detect, and remediate/mitigate known vulnerabilities.

Description: Inform the constituents of any known vulnerabilities (potential entry points for attackers), so that their systems can be kept up to date and monitored for exploits. Disclosure methods may include publication of information through multiple communication channels (e.g., website, email, social media), a vulnerability database, or other media. This service often, but not always, occurs following Vulnerability Coordination.

Outcome: Informed constituents can avoid the potential exploitation of known vulnerabilities prior to exploitation and can detect and mitigate vulnerabilities that already exist.

The following functions are considered to be part of the implementation of this service:

- Vulnerability disclosure policy and infrastructure maintenance
- Vulnerability announcement/communication/dissemination
- Post-vulnerability disclosure feedback

7.5.1 Function: Vulnerability disclosure policy and infrastructure maintenance

Purpose: Develop 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.

Description: CSIRTs that handle vulnerability reports should 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 policy will provide transparency to stakeholders and help to promote appropriate disclosure policies. Policies can range from no disclosure, where no vulnerability information is disclosed, to limited disclosure, where only some information is made available, to full disclosure, where all information is disclosed, which may include proof-of-concept exploits. The disclosure policy should include factors such as the scope of the policy, references to any reporting mechanisms and guidelines, and expected timeframes and mechanisms for the disclosure of the vulnerability.

Outcome: Trust, collaboration, and control of the disclosure is increased and relationships and coordination with CVD participants is improved.

7.5.2 Function: Vulnerability announcement/communication/dissemination

Purpose: Provide information to constituents (or the public) about a new vulnerability, so that they can detect, remediate or mitigate, and prevent future exploitation of the vulnerability.

Description: 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 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. Content to be included in the disclosure should follow a defined format, which typically can include information such as an overview or description, a unique vulnerability identifier, impact, severity, or CVSS score, resolution (remediation or mitigation), and supporting references or materials.

Outcome: The vulnerability is prevented, detected, and remediated/mitigated by providing timely, high-quality, effective information to constituents (or public).

7.5.3 Function: Post-vulnerability disclosure feedback

Purpose: Receive and respond to questions or reports from constituents about a vulnerability disclosure or document.

Description: Following the disclosure of a new vulnerability, CSIRTs can expect to receive follow-on

communications in the form of questions from some constituents about a vulnerability document. The questions may indicate a need for clarification, revision, or amendment of the vulnerability disclosure mechanism, if warranted. 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. If the vulnerability was determined to have been already exploited, constituents may be reporting newly discovered incidents as a result of the vulnerability disclosure. Such reports should feed into the functions of the CSIRT's Incident Reporting service.

Outcome: Any questions or requests for assistance are responded to in a timely manner following a vulnerability disclosure.

7.6 Service: Vulnerability response[8]

Purpose: Actively take information about known vulnerabilities and act upon that information to prevent, detect, and remediate/mitigate those vulnerabilities.

Description: The functions under this service are intended to determine whether a disclosed vulnerability exists on a constituent's systems, often through the intentional act of looking for the presence of such vulnerabilities. The service can also include the follow-on actions to remediate or mitigate the vulnerability through the deployment of patches or workaround strategies.

Outcome: Information was acted upon in order to detect the presence of a vulnerability, remediate/mitigate a disclosed vulnerability, and prevent the vulnerability from being exploited.

The following functions are considered to be part of the implementation of this service:

- Vulnerability detection / scanning
- Vulnerability remediation

This Vulnerability Response service and its related functions are usually performed by other specialized groups within an organization, typically not the CSIRT. This service is also unlikely to be provided by a Coordinating CSIRT.

7.6.1 Function: Vulnerability detection / scanning

Purpose: Actively engage in searching for the presence of known vulnerabilities in deployed systems.

Description: The goal of this function is to detect any previously unpatched or unmitigated vulnerabilities before they are exploited or impact the network or devices. This function may be initiated in response to an announcement about a new vulnerability, or it may be achieved as part of a periodically scheduled scan for known vulnerabilities. In order to provide vulnerability detection effectively, it is useful to have a systems inventory. Having such an inventory that can be queried for software version information can enable an organization to quickly assess the likely prevalence of a newly reported vulnerability in its infrastructure.

[8] Although the function and sub-functions for detecting vulnerabilities are sometimes referred to as "vulnerability management," this CSIRT Services Framework instead refers to these as part of this Vulnerability Response service, which is part of the larger service area named Vulnerability Management in this framework.

This function may receive input or be triggered from other services and functions.

Outcome: Vulnerabilities are detected through formal processes or tools designed to identify.

The following sub-functions are considered to be part of this function:

- Vulnerability scanning/hunting
- Vulnerability security assessments/penetration testing

This function is typically performed by other entities (e.g., IT service, SOC, third-party specialists, system owners).

7.6.2 Function: Vulnerability remediation

Purpose: Remediate or mitigate vulnerabilities to prevent them from being exploited, typically through the timely application of vendor-provided patches or other solutions.

Description: Vulnerability remediation is intended to resolve or eliminate a vulnerability. For software vulnerabilities, this typically occurs through the deployment and installation of vendor-provided solutions in the form of software updates or patches. When approved patches are unavailable or cannot be deployed, an alternative mitigation or workaround may be applied as a countermeasure to prevent exploitation of the vulnerability. This function often follows a positive identification of a vulnerability as the result of the Vulnerability Detection/Scanning/Hunting function.

Outcome: Exposure to the threat of a vulnerability being exploited is prevented or reduced.

The following sub-functions are considered to be part of this function:

- Vulnerability remediation (patch management)
- Vulnerability mitigation

This function is typically performed by others (e.g., IT, SOC, system owners), not the CSIRT.

8 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 services are offerings of this service area:

- Data acquisition
- Analysis and synthesis
- Communication

8.1 Service: Data acquisition

Purpose: Collect data that will help increase visibility as to what internal and external activities are occurring that may affect the constituency's security posture.

Description: Solicit, collect, determine, and satisfy the constituencies' information requirements to achieve awareness of important internal and external relevant activities. This service includes the logistics of collecting relevant information including news of current events, scheduling future events, reports and feeds, filtering the collected information, organizing information for use in incident analysis, prevent, detection, or other activities (such as planning or trending), storing it for later use, improving its "searchability", and more. Collected data will be used to determine the preventative measures needed and to help make informed decisions regarding incident management and information assurance activities. Without a basic perception of important environmental elements, the risk of other services forming an incorrect picture increases. CSIRTs will need to establish policy and procedures, and may employ technology to collect and vet information.

Outcome:

The following artefacts result from this service:

- a set of data collection requirements that identifies situational awareness needs, and then maps those requirements to the types of information to be collected in order to meet those objectives
- information about the current and expected future status of constituency assets and activities
- information about external events or trends that provides insight into the constituency's surroundings and current environment, including new technologies, methods, practices, risks, and threats
- properly formatted information readied for analysis and detection activities

The following functions are considered to be part of the implementation of this service:

- Policy aggregation, distillation, and guidance
- Asset mappings to functions, roles, actions, and key risks
- Collection
- Data processing and preparation

8.1.1 Function: Policy aggregation, distillation, and guidance

Purpose: Establish the context with which the constituency and its assets should comply to know what should be occurring on the infrastructure.

Description: The collection, aggregation, and distillation of policy establishes the basis of acceptable normal activity. The end result is a context that establishes how the constituency, and its infrastructure is supposed to be operating under acceptable conditions. For organizational CSIRTs, context includes understanding the organizations acceptable policies, plans, normal operating conditions, accepted risks, and tradeoffs. Understanding and context establish the basis against which observations can be evaluated.

Outcome: The acceptable observations that are taking place in the constituency are understood. This understanding is focused upon changes or impacts to infrastructure and assets.

8.1.2 Function: Asset mapping to functions, roles, actions, and key risks

Purpose: Provide knowledge of existing assets, ownership, baselines and expected activity supports analysis functions that identify abnormal situational observations.

Description: CSIRT teams need to understand the current cyber security state of a constituency and have a good understanding of what is acceptable security. They may need to know:

- 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 helps establish prioritization of assets that are potentially at risk, which can provide context for incident management activities. The more precise the information available to CSIRT team, the easier it will be to infer security issues and do something about them. Precise information may

mean the CSIRT having access to established security policies, current access controls, up-to-date hardware and software inventories, and detailed network diagrams.

Outcome:

The following lists result from this function:

- A list of key functions and the assets that support them; some assets may support multiple functions
- A list of the roles which perform each function and their equivalent digital role on the asset
- A list of generally permissible actions by each role
- A list of the key risks facing the assets and the functions.

These lists will evolve based upon situational changes.

8.1.3 Function: Collection

Purpose: Collect of information to support the Analysis and Interpretation service and/or other CSIRT services.

Description: Information and data collection activities extend beyond feeds providing automated information. Collection includes identifying useful sources such as information-relevant external activities including news from other constituencies, media sources, and other CSIRTs or security organizations, internal activities (e.g., organizational changes), technology developments, external events, political events, attack trends, defensive trends, conferences, available training, and more.

The data collection function supports other services such as Security Event Management, Incident Management, and Knowledge Transfer. It also supports functions and activities within these services such as analysis, prediction, response, and risk mitigation. Newly collected information may reveal that an attack on a constituent is more likely than before. External events may expose information that identifies new risks to assets for a period of time or require heightened detection activities. Overall the information helps provide actionable information to aid in decision making and incident handling.

Outcome: Data and datasets are collected and produced to provide an operational or environmental context that can be used by other services and functions, including analysis, to create a situational picture for the constituency, identify alerts, or plan for mitigating increased areas of risk to assets and supporting infrastructures.

8.1.4 Function: Data processing and preparation

Purpose: Establish a reliable, consistent, and current set of data that can support CSIRT activities and the requirements of the analysis service.

Description: Data processing and preparation includes transformation, processing, normalization, and validation of a set of data. Sources of cybersecurity data need to be validated for accuracy often due to a high number of false positives. The relevant data also typically comes in different formats, and new data needs to be combined with historical data before a complete analysis can be performed. Some types of data (such as news articles) may need to be analyzed or processed as part of the preparation

process. One example would be extracting relevant security information from a news article (e.g., names, dates, places, technical information, weaknesses, system names) and comparing it with internal data for potential impacts.

Some analysis methods require data to be stored in the same format, or for files to have the same number of records. There are multiple processing steps that may be involved to prepare the data. Data augmentation (also called enrichment) is performed by including other available information related to a given piece of data from other internal and external sources. For example, teams may collect information related to internet protocol addresses (IP addresses) such as autonomous system identifiers, country codes, or geo-location data. For internal asset information, teams may enrich their asset inventory data with the name of the asset owner, their role, their permissions on other assets, their physical working location over time, and more.

Outcome: Data is available and ready to be used by other services or functions.

8.2 Service: Analysis and synthesis

Purpose: Assess when the situation does not match with expectations (e.g., when specific assets may be about to experience a harmful event).

Description: The process of using current data, history, and analysis techniques to determine what is occurring that may impact the constituency assets and security posture, often done by determining an answer to a question or testing an intuition. Analysis may reveal when events do not match typical expected behavior, or may reveal information about the circumstance, nature, or origin of events or behaviors. Analysis may reveal implications to current and future situations. For example: a system may log that a user ID successfully logged into the system, but the system does not indicate whether the event was performed by a legitimate user. New sources (such as interviews with the user) will need to be incorporated into the analysis to provide the team with a more accurate picture to determine the legitimacy of the event. A variety of techniques may be used to analyze and interpret the collected data and its effect upon the constituency.

Outcome: A set of conclusions about the probable historical, current, and/or likely future events within a constituency is produced. It may also include recommendations about certain decisions that a constituency is facing. Analysis should be supported by evidence such as observation data collected from sensors and other sources and the interpretation of that evidence by analysts through a variety of methods. The analysis may also include constituents that need to be told about the results, and what they need to be told.

The following functions are considered to be part of the implementation of this service:

- Projection and inference
- Event detection (through alerting and/or hunting)
- Information security incident management decision support
- Situational impact

8.2.1 Function: Projection and inference

Purpose: Analyze the information collected during data acquisition with the intent of identifying current or predicting future situational pictures.

Description: The process of inferring the current state of a situation and making predictions about the possible likely near-term pictures based on the status and dynamics of the collected data. Sometimes the data may quickly show a security issue.

Outcome: The situational picture is updated along with knowledge about when a situational picture will change and how it might change.

8.2.2 Function: Event detection (through alerting and/or hunting)

Purpose: Determine and confirm the details of the current situational picture for the constituency.

Description: The systematic and often directed searching for anomaly activity inside and outside of network boundaries based upon external and internal information and trends. To assist the constituency with analyzing its data from sensors and other sources to draw conclusions about its environment and situation. For example, if an anti-virus sensor sends an alert of a suspicious file, the team may analyze the system configuration, the sensor configuration, the file that was alerted, the user activity at the time, and more, to draw a conclusion about the severity of the observation. This function may receive significant input from the Security Event Management service area. The observations from sensors that are used to detect events may be shared among multiple services.

CSIRT teams also need to determine the current situational picture based upon specific pieces of information about threats. This activity may sometimes be called “threat hunting.” Typically, threat hunting involves either preparing the environment to detect specific threat activity or searching for specific threat activity that may already be present.

Outcome: A situational picture is updated based upon the detection of events in the constituency.

8.2.3 Function: Information security incident management decision support

Purpose: Identify new insights during incidents that may help limit damage, mitigate future risk, or identify a newly created weakness.

Description: Performing analysis of specific evidence assists in identifying insights to support incident resolution. Sometimes, CSIRTs may focus their situational analysis to support a specific desired outcome such as incident resolution. Certain responses to an incident may affect a situational picture differently, and responders may ask for analysis (e.g., impact, cost, risk of failure) of choices. The decision-making needs of the constituency may change as their situational picture evolves, and the CSIRT team may initiate new analysis processes to assist them. This activity is related to the Incident Management Service Area. Incident Management functions are supported by Situational Awareness and the situational picture may change based upon Incident Management activities.

Outcome: Situational awareness is enhanced for incident management functions based upon new observations. Updated situational picture based upon incident management activities.

8.2.4 Function: Situational impact

Purpose: Determine the expected potential impact of a given observation or possible observation to a situational picture.

Description: This function identifies the impact a projection or inference may have upon a current or near-term future situation. An impact may include raising or lowering certain risks such as data loss, system downtime, or effects on data confidentiality/availability/integrity.

Outcome: An analysis is produced of the likely possible impact that an inference or projection may have upon a situation.

8.3 Service: Communication

Purpose: Notify constituents or others in the security community about changes in risks to the situational picture.

Description: The knowledge obtained from situational awareness must be communicated to the constituency. This will allow it to react to observations and to take actions that will improve defensive situations, e.g., reducing third-party risk by improving the security environment at certain high-risk suppliers.

Outcome: Accurate, actionable, and timely situational information is delivered to constituency so they can better understand their past and improve their current and future situational picture.

The following functions are considered to be part of the implementation of this service:

- Internal and external communication
- Reporting and recommendations
- Implementation
- Dissemination / integration / information sharing
- Management of information sharing
- Feedback

8.3.1 Function: Internal and external communication

Purpose: Inform constituents (and others) of the current situational picture and how it may be changing.

Description: Once the results of Analyze and Interpret are complete, they can be used to improve decision-making via both internal and external communication processes. Specific pieces of information are distributed based upon who needs to know them. Communication includes the method of delivery and the content that is being delivered. A CSIRT team might communicate new information and how it will change the situational picture. An example of this would be reporting the expected change a new malicious technique it has observed during an incident would have upon a constituent member. It may also include trend information such as the most useful sources of enrichment data and steps in which constituents can use it to improve their own situational awareness.

Outcome: Constituents are better informed and are prepared to take actions or make decisions that will improve their security or situation.

8.3.2 Function: Reporting and recommendations

Purpose: Create results, artefacts, or findings that communicate critical information discovered or created during analysis to audiences in a manner and format that they will understand.

Description: Reports and recommendations should clearly indicate the choices and actions faced by constituents, and include analysis of the expected consequences of each choice or action. Communication of findings should include a list of evidence supporting the analysis and the recommendation (if a recommendation is made). The methods used to create the findings should be clearly explained to the audience so they can also judge the claims presented. The CSIRT team may create reports on a single event, a series of events, trends, patterns, possible events, or more to support the needs for their constituency to understand a situational picture.

Outcome: The capability to provide accurate, timely, and complete reports on the situational picture, the evidence that supports the conclusions, and/or recommendations on possible courses of action and their potential effects to the constituency is improved.

8.3.3 Function: Implementation

Purpose: Adapt the constituent environment based on communications to be more prepared for or react to changes in the situational picture.

Description: In some instances, a CSIRT team may also perform the recommended adjustments to parts of the security infrastructure, for example changing the firewall rules on a particular honey pot based upon situational analysis.

Outcome: A course of action is performed or a change to the infrastructure is implemented by constituents based upon received communications containing analysis, projections, and/or recommendations.

8.3.4 Function: Dissemination / integration / information sharing

Purpose: Assemble, normalize, and prepare information and then share it with constituents and others outside the constituency.

Description:

This function may include the following sub-functions:

- using the results of the analysis service in internal and external planning and decision-making processes
- identifying the right targets to receive the information
- making the analysis results available
- ensuring the delivery is successful
- tracking and reporting on the sharing of information

- sending relevant information to the Knowledge Transfer service for further use and dissemination

Outcome: Situational Awareness Analysis outputs are used as inputs (both internally and among constituents) into in key decision processes e.g., threat hunting, incident analysis, resolution. Outputs are disseminated as part of handling or detecting incidents. Information and data coming from Situational Awareness can also become Best Practices, Reports, Training and Awareness Material through the Knowledge Transfer service area.

8.3.5 Function: Management of information sharing

Purpose: Ensure transfer of information is successful and useable.

Description:

This function may include the following sub-functions:

- providing information to other groups.
- formatting information for transfer.
- tracking transfer process and its outcome.

Outcome: Assurance is provided that the right information is being shared, and that once shared, it is received by partners, constituents, and other community members. Reports are provided on sharing activity.

8.3.6 Function: Feedback

Purpose: Improve the quality, timeliness, accuracy, and relevance of the data being received from internal and external sources.

Description: This function involves providing and receiving feedback on information provided, received, and used by the constituency, other service providers or other stakeholders. Was the information received accurate, applicable, timely, strategic, new/novel, etc.? Was it helpful in resolving an investigation? Did it lead to a new insight? This may mean providing information also to other CSIRT (as an external source) on the usefulness of or changes to signatures, honeypot findings, IOCs, warnings, threat information, mitigations, etc. This activity may also be performed by the Knowledge Transfer service area. If so, the results should be communicated back to the Situational Awareness service area.

Outcome: Observations and feedback is provided to internal and external sources in order to improve the accuracy, timeliness, quality, and usefulness of information received.

9 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 services are considered as offerings of this particular service area:

- Awareness building
- Training and education
- Exercises
- Technical and policy advisory

9.1 Service: Awareness building

Purpose: Increase the overall security posture of the constituency and help its members to detect, prevent, and recover from incidents; ensure that constituents are better prepared and educated.

Description: This service includes working 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.

Outcome: The constituency is provided with the necessary awareness of:

- events, activities, and trends that may affect its ability to operate in a timely and secure manner
- steps to take to detect, prevent and mitigate threats and malicious activity
- security and operational best practices

The following functions are considered to be part of the implementation of this service:

- Research and information aggregation
- Report and awareness materials development
- Information dissemination
- Outreach

9.1.1 Function: Research and information aggregation

Purpose: Aggregate, collate, and prioritize information that can be disseminated to the constituency for the improvement of the security posture and prevention and mitigation of risks.

Description: This function involves researching and aggregating 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.

Outcome: Information about relevant trends, ongoing incidents, and best practices, is aggregated and can be used to develop reports and awareness materials for varied audiences.

9.1.2 Function: Reports and awareness materials development

Purpose: Use the information aggregated and researched as being relevant to produce materials in different media with the goal of reaching different audiences or delivering specific content in the best way possible.

Description: This function involves developing 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 annual reports.

Outcome: CSIRT reports and awareness materials of adequate quality are developed to meet the needs of the constituency utilizing varied and effective delivery techniques and platforms.

9.1.3 Function: Information dissemination

Purpose: Disseminate security-related information to improve awareness and implementation of security practices.

Description: The function involves implementing a process of information dissemination that can help the CSIRT to best deliver its reports and awareness materials to its constituency based on the characteristics of different audiences and content.

Outcome: Information dissemination framework is implemented to enables the CSIRT's constituency to have access to timely and relevant information through different methods, including podcasts, blog posts, social media posts and videos, press releases, advertisements, campaigns, public reports, etc.

9.1.4 Function: Outreach

Purpose: Develop and maintain relationships with experts or organizations that may help or be part of the execution of the mission of the CSIRT.

Description: This function involves building partnerships, promoting cooperation, and engaging key stakeholders, internal or external to the constituency, with the goal of: disseminating awareness and best practices; helping the constituency and external stakeholders understand the services and benefits a CSIRT can provide; helping the CSIRT to better understand constituents' needs; and enabling the realization of CSIRT's mission. This may involve ensuring interoperability or fostering collaboration between or across organizations.

Outcome: Active and consistent outreach activities are performed that may include, but are not limited to, meeting with key stakeholders, participating in sector meetings, presenting at conferences, and organizing conferences.

9.2 Service: Training and education

Purpose: Provide training and education to a CSIRT constituency (which may include organizational and CSIRT staff) on topics related to cybersecurity, information assurance and incident management.

Description: A training and education program can help the CSIRT to establish relationships and to improve the overall cybersecurity posture of its constituency, including the ability to prevent future incidents from happening. Such a program can

- help maintain user awareness
- help the constituency understand the changing landscape and threats
- facilitate information exchange between the CSIRT and its constituency
- train the constituency on tools, processes and procedures related to security and incident management.

This can be done through various types of activities including documenting the knowledge, skills, and abilities (KSAs) required, developing educational and training materials, delivering content, mentoring, and professional and skill development. Each of these activities will collectively contribute to the constituency's and the team's capabilities.

Outcome: A consistent training and education program is provided that enables the CSIRTs' constituency to appropriately acquire

- methods to detect, prevent or respond to threats
- tools and practices to help protect critical assets
- understanding about incident management processes and how to get assistance

The following functions are considered to be part of the implementation of this service:

- Knowledge, skill, and ability requirements gathering
- Educational and training materials development
- Content delivery
- Mentoring
- CSIRT staff professional development

9.2.1 Function: Knowledge, skill, and ability requirements gathering

Purpose: Properly assess, identify, and document what the constituency needs are in terms of requisite KSAs, to develop appropriate training and education materials and improve its skill level.

Description: The function involves collecting knowledge, skill, and ability (KSA) needs and the competence of a constituency in regard to determining what training and education should be provided.

Outcome: Constituency KSA needs are characterized and documented to be used as basis for developing relevant education and training materials.

9.2.2 Function: Educational and training materials development

Purpose: Develop, using the constituency's KSA needs as a basis, educational, instructional, and training material that is appropriate to the delivery methods identified as the best to reach different audiences or deliver specific content.

Description: This function involves building or acquiring content of educational and training materials such as presentations, lectures, demonstrations, simulations, videos, books, booklets, etc.

Outcome: CSIRT training and education materials utilizing varied and effective presentation techniques and platforms are developed that are of appropriate quality and that meet the needs of the constituency.

9.2.3 Function: Content delivery

Purpose: Develop a formal process for content delivery that can help the CSIRT to best deliver the content to its constituency, based on the characteristics of different audiences and content.

Description: This function involves the transfer of knowledge and content to "students." This can occur via various methods, such as computer-based/online training (CBT/WBT), instructor-led, virtual, conferences, presentations, labs, capture the flag (CTF) competitions, books, online videos, etc.

Outcome: A content delivery framework has been designed to help the constituency learn technical and soft skills and processes, using all alternative approaches, including books, booklets, online videos, presentations, hands-on labs, CTFs, CBT/WBT, in-person training, etc. This results in constituency members who understand the content delivered.

9.2.4 Function: Mentoring

Purpose: Develop a program for CSIRT staff, constituency members, or external trusted partners to learn from experienced staff through an established relationship.

Description: A Mentoring program can help provide a formal as well as informal mechanism for the mentor to share with the mentee about education and skill development, insights, and life and career experiences outside of the official reporting relationship and structure of the team. This can involve on-site visits, rotation (exchange), shadowing, and discussing rationale for specific decisions and actions.

Outcome: Retention, loyalty, confidence, and overall ability to make sound decisions has been increased in the CSIRT team. Constituents have improved skill levels and a better relationship with its CSIRT. Improved capacity and capability of the constituency and the CSIRT team members, including the development of trusted relationships.

9.2.5 Function: CSIRT staff professional development

Purpose: Help staff members successfully and appropriately plan and develop their careers.

Description: Once the appropriate skills have been identified, professional development is used by a CSIRT to promote a continuous process of securing new knowledge, skills, and abilities that relate to the security profession, unique job responsibilities, and the overall Team environment. This can include attending conferences, advanced training, and cross-training activities, among others.

Outcome: Developed and trained staff are available with the requisite technical and soft skills and process understanding, and who are up to date based on the job roles and needs. CSIRT members are ready to address the daily operational challenges, supporting both the team and its customers.

9.3 Service: Exercises

Purpose: Conduct exercises to assess and improve the effectiveness and efficiency of cybersecurity services and functions.

Description: Services are offered by the organization to constituents that support the design, execution, and evaluation of cyber exercises intended to train and/or evaluate the capabilities of individual constituents and the stakeholder community as a whole, including communications capabilities. These types of exercises can be used to

- test policies and procedures: assess whether there are sufficient policies and procedures in place to effectively detect, respond and mitigate incidents. This is, generally, a paper/table-top exercise.
- test operational readiness: assess whether the organization has an incident management capability that is able to detect, respond to and mitigate incidents in a timely and successful manner, as well as to test whether the right people are in place, directories are up-to-date, and if procedures are executed correctly.

This service addresses both the needs of the organization and the needs of its constituents. More specifically, through the simulation of cybersecurity events/incidents, exercises can be used for one or several objectives:

- Demonstrate: Illustrate cybersecurity services and functions, as well as vulnerabilities, threats, and risks, in order to raise awareness.
- Train: Instruct staff on new tools, techniques, and procedures:
    - Exercise: Provide an opportunity for staff to use tools, techniques, and procedures they are expected to be knowledgeable about. Exercising is necessary for perishable skills and helps improve and maintain efficiency.
    - Assess: Analyze and understand the level of effectiveness and efficiency of cybersecurity services and functions, as well as the level of staff preparedness.
    - Verify: Determine whether a specified level of effectiveness and/or efficiency can be achieved for cybersecurity services and functions.

Outcome: The effectiveness and efficiency of cybersecurity services and functions is improved and opportunities for further improvements are identified.

Depending on the specific objective(s) of an exercise, cybersecurity may also be demonstrated to internal or external stakeholders, staff can be trained, and the efficiency and effectiveness of tools, services, and functions can be assessed and/or verified. Lessons for improving future exercises can also be identified and a report delivered to management or other key stakeholders.

The following functions are considered to be part of the implementation of this service:

- Requirements analysis

- Format and environment development
- Scenario development
- Exercise execution
- Exercise outcome review

9.3.1 Function: Requirements analysis

Purpose: Ensure an effective outcome of the exercise by concentrating on specific issues for the given scope and focus of the exercise.

Description: Determine the learning objectives and scope of the exercise. Define the specific services, capabilities, and topics to be covered by the exercise. Ensure exercise includes activities and topics that relate to required or desired skills needed by the participants, as well as the processes that should be tested.

Outcome: A description of the purpose of the exercise is determined, along with an outline of the learning objectives to be met.

9.3.2 Function: Format and environment development

Purpose: Specify and determine the internal and external resources and infrastructure needed to conduct the exercise.

Description: Define the format and platform needed to meet the objectives and deliver the expected outcomes of the exercise.

Outcome: The type of exercise (table top, hands-on, simulation, etc.) is identified, as well as the internal and external resources needed to conduct the exercise.

9.3.3 Function: Scenario development

Purpose: Provide an opportunity for the target audience to improve the efficiency and effectiveness of its services and functions, and its skills, knowledge, and abilities, through the handling of simulated cybersecurity events/incidents, including communications aspects.

Description: Development of exercise scenarios in support of stakeholder objectives. Deliverables also include instructions and guidance to the participants and exercise managers; these instructions include recommended actions for the participants detailing some/all scenario steps.

Outcome: A main scenario with variants and various types of formalized injects is developed, along with tasks and role allocation to the exercise management team.

9.3.4 Function: Exercise execution

Purpose: Conduct drills/exercises allowing a CSIRT team to increase its confidence in the validity of an organization's CSIRT plan and its ability for execution.

Description: The function involves performing readiness testing of constituent "students" to test their ability to apply training and perform job or task functions. Can be in the form of real or virtual environments, simulations, field tests, table tops, mock scenarios, or a combination, with injects being

provided in a structured manner. This will also help determine the level at which the team is operating, as well as if and where it has room for improvement.

Outcome: A CSIRT has assessed its preparedness and readiness, ensuring the KSAs, key processes, and execution all work successfully together, or must be adapted/improved.

9.3.5 Function: Exercise outcome review

Purpose: Perform a formal and objective analysis of the exercise, based on factual observations.

Description: Develop an after-action report which includes lessons learned or findings/best practices from the exercise, and provide an assessment to the stakeholders/management.

Outcome: Deliverables are created highlighting the success of the exercise, areas for improvement, general findings, and recommended actions to take in order to improve: the organization incident management capabilities, the CSIRT's team processes, and the capabilities of individual constituents and of the stakeholder community as a whole, including communications capabilities and procedures.

9.4 Service: Technical and policy advisory

Purpose: Ensure the constituency's policies and procedures include appropriate incident management considerations and, ultimately, enable the constituency to better manage risks and threats, as well as enabling the CSIRT to be more effective.

Description: Support the CSIRT constituency and key stakeholders, internal or external to the constituency, in activities related to risk management and business continuity, providing technical advice as needed and contributing to the creation and implementation of the constituency's policies, as well as influencing them to enable the CSIRT to be more effective. Policies are also important in legitimizing the services of a CSIRT.

Outcome: A constituency is enabled to make organizational decisions based on operational security best practices that incorporate business continuity and disaster recovery best practices, while also understanding the need of including incident management teams, as trusted advisors, in business decisions where appropriate.

The following functions are considered to be part of the implementation of this service:

- Risk management support
- Business continuity and disaster recovery planning support
- Policy support
- Technical advice

9.4.1 Function: Risk management support

Purpose: Improve the identification of opportunities and threats, improve controls, improve loss prevention and incident management in conjunction with information security and other relevant functions.

Description: Support to activities related to assessing risk or compliance. This may include conducting an actual assessment or providing support to evaluate the results of an assessment.

Outcome: The constituency is able to identify risks and threats and select relevant risk management options, including appropriate and effective incident management strategies, security controls, or threat mitigations.

9.4.2 Function: Business continuity and disaster recovery planning support

Purpose: Act as a trusted advisor on business continuity and disaster recovery by providing impartial, fact-based advice, considering the environment in which the advice may be used and any resource constraints that apply.

Description: Support the constituency in the activities related to organizational resilience, based on risks identified.

Outcome: The constituency is able to appropriately implement business continuity and disaster recovery plans that include and align with the incident management strategies.

9.4.3 Function: Policy support

Purpose: Act as a trusted advisor on the development and implementation of policies by providing impartial, fact-based advice, considering the environment in which the advice may be used and any resource constraints that apply.

Description: This function supports the constituency in the development, maintenance, institutionalization, and enforcement of policies, while ensuring they enable and support incident management activities. For internal CSIRTs, this typically includes support for information security and other operating policies. For coordinating and National CSIRTs, this might include support for public policies and new legislation.

Outcome: The constituency is able to develop effective policies, institutionalize policies, and enable effective incident management strategies.

9.4.4 Function: Technical advice

Purpose: Provide technical advice that can help the constituency to better manage risks and threats and implement current operational and security best practices, while enabling effective incident handling activities.

Description: This function provides support and recommendations for the improvement of cybersecurity related infrastructures, tools, and services for its constituency, with the goal of improving the security posture and incident management overall.

This might include advice on

- security considerations for acquisition, compliance verification, maintenance, and upgrades
- internal and external audits of cybersecurity related infrastructures and tools
- secure software development requirements and secure coding

Outcome: Support is provided to design, acquire, manage, operate and maintain the constituency's infrastructure and systems and tools, as well as assist in building the capability, capacity, and maturity of incident management activities.

ANNEX 1: Acknowledgments

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

- Vilius Benetis, NRD CIRT (LT)
- Olivier Caleff (Service Area Coordinator), openCSIRT Foundation (FR)
- Cristine Hoepers (Service Area Coordinator), CERT.br (BR)
- Angela Horneman, CERT/CC, SEI, CMU (US)
- Allen Householder, CERT/CC, SEI, CMU (US)
- Klaus-Peter Kossakowski (Editor), Hamburg University of Applied Sciences (DE)
- Art Manion, CERT/CC, SEI, CMU (US)
- Amanda Mullens (Co-Service Area Coordinator), CISCO (US)
- Samuel Perl (Service Area Coordinator), CERT/CC, SEI, CMU (US)
- Daniel Roethlisberger (Service Area Coordinator), Swisscom (CH)
- Sigitas Rokas, NRD CIRT (LT)
- Mary Rossell, Intel (US)
- Robin M. Ruefle (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)
- Désirée Sacher, Finanz Informatik (DE)
- Krassimir T. Tzvetanov, Fastly (US)
- Mark Zajicek (Co-Service Area Coordinator), CERT/CC, SEI, CMU (US)

ANNEX 2: Terms and Definitions

This section defines certain terms used in the CSIRT Services Framework.

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

Advisory[9] - 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 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)[10] - 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)[11] - A numerical score that reflects a vulnerability's severity.

Common Weakness Enumeration (CWE)[12] - 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 - A term used to denote a disclosure process that includes coordination. Source: ISO/IEC 29147:2018, Terms and definitions.

Coordinator[13] - An optional participant who can assist vendors and finders in handling and disclosing vulnerability information.

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.

[9] ISO/IEC 29147:2014 Information technology—Security techniques — Vulnerability disclosure- Terms/Definitions 3.1
[10] https://cve.mitre.org/
[11] https://www.first.org/cvss/
[12] https://cwe.mitre.org/about/index.html
[13] ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.1

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.

Finder[14] - 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 actions[15]; to perform a specified action or activity, work, operate.[16]

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 Incident[17] - 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)[18] - 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.

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

[14] ISO/IEC 29147:2014 Information technology—Security techniques — Vulnerability disclosure- Terms/Definitions 3.3
[15] Source: https://www.merriam-webster.com/dictionary/function
[16] Source: https://www.dictionary.com/browse/function
[17] Based on RFC2350 by considering „information security“ instead of „IT security“, https://tools.ietf.org/html/rfc2350.
[18] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator

source software is often maintained by a community of individuals and entities who collaboratively create and maintain it.

Product[19] - A system implemented or developed for sale or to be offered for free.

Remediation (or Remedy)[20] - 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."

Risk[21] - 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 Acceptance[22] - A risk response strategy whereby the project team decides to acknowledge the risk and not take any action unless the risk occurs.

Risk Register[23] - 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.

Stakeholders[24] - 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.

Vendor[25] - A person or organization that developed the product or service or is responsible for maintaining it.

Vulnerability[26] - A weakness in software, hardware, or an online service that can be exploited.

[19] ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability disclosure-Terms/Definitions 3.5
[20] ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability disclosure-Terms/Definitions 3.6
[21] ISO 31000:2009/ ISO Guide 73:2002 Risk management — Principles and guidelines- Terms/Definitions 2.1
[22] The Project Management Body of Knowledge (PMBOK) Guide and Standards
[23] The Project Management Body of Knowledge (PMBOK) Guide and Standards
[24] Architecture Content Framework
[25] ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.7
[26] 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.
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: Overview of all CSIRT Services and related Functions