FIRST CSIRT Framework

Computer Security Incident Response Team (CSIRT)
Services Framework

Version 1.1.1

CONTENTS

INTRODUCTION

This is the updated version of the Computer Security Incident Response Team 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 now been moved into the main document, as they are often the foundation for the other services provided by CSIRTs.

This document provides a comprehensive list of services that CSIRTs may provide. It's not necessary for a CSIRT to provide all services, but all teams will provide at least some of the services. This document does not cover activities of product security teams and this will be described in the PSIRT Service Framework.

This Framework will likely develop: CSIRTs will continue to develop to face the ever-changing challenges to keep their stakeholders secure against new threats emerging.

This document intended is to support CSIRTs choosing their service portfolio. The document makes no suggestions or recommendations about capability and capacity. These topics are dealt with elsewhere.

Finally: This document would never have been possible without the help of many volunteers spending many hours drafting, revising and giving feedback to this document. One person stands out particularly: Peter Allor has been driving the creation of the CSIRT Framework since its beginning. Without him we would not have this document.

CONTEXT AND SCOPE

The Framework addresses external services to stakeholders and essential internal services to operate. Add explanation on the overall structure of the document and why some sections has been eliminated.

PURPOSE

"The CSIRT Services Framework defines a set or list of suitable services and functions that CSIRTs implement, at least in part, to serve their stakeholder. Its purpose is to facilitate establishment of CSIRT operations, capability development, and education and training, through the use of a community-accepted terminology and approach to what a CSIRT may do."

HISTORY

The CERT/CC CSIRT Services List has been used since the late 1980s in many cases to serve as a consistent and comparable description of CSIRTs and their corresponding services. In recent assessments of various existing, informal CSIRT services lists, it was determined that although it was broadly used and adapted, the CERT/CC list was missing key components that represent the extended understanding regarding the mission of modern-day CSIRTs.

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 its excising and possibly

future members. Initially the document's purpose was to have a common basis to develop trainings. Meanwhile the document has acquired wider scope and helps other concerned with CSIRTs work defining their activities. Given the global span of the membership of FIRST, the community came together and created this document from the different perspectives the members have.

General Principles

Design Principles

- Common Framework Model. This model is the same one as used in the PSIRT Service Framework.
- Simplicity. The framework must be as simple as possible, removing any unnecessary complexity or redundancy. Simplicity facilitates acceptance and usage by the community.
- Comprehensiveness. The framework must address those services/functions a CSIRT could potentially provide/perform in the eyes of the community, that fit to the role of a CSIRT. CSIRTs rarely will perform all services and certainly not at a high maturity level.
- Consistency of Language. The framework must use well-defined language in a consistent fashion in order to facilitate understanding by non-native speakers and ensure interoperability. Furthermore, we use previously defined terminology used in international standards unless for other good reasons.

Use Standardized Or Widely-Accepted Definitions

The CSIRT Services Framework currently provides its own definitions for words that are already defined in standards or well-referenced documents.

Hierarchical Model

- A hierarchical model consisting of the following levels, as defined below:
    - Service Area
    - Service
    - Function
- Service Area – group services related to a common aspect. They help to organize the services along a top-level categorization in order to facilitate understanding. (This area will be further developed in Version 2.0.)
- Service – the set of recognizable, coherent actions towards a specific result on behalf of or for the stakeholder of an incident response team. The list of functions used to implement the service.
- Function – a means to fulfil the purpose or task of a specified service. The list of tasks that can be performed as part of the function

RECOMMENDED DEFINITIONS

In order to make use of the framework in the most effective way, it is necessary to use standard definitions which have been adopted and accepted by the community. It's depicted in Figure 1 below.

SERVICE AREAS – SERVICES – FUNCTIONS

SERVICE AREAS

Service Areas regroup services related to a common aspect. They help to organize the services along a top-level categorization to facilitate understanding. 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 means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. A service is a coherent, ready-to-use deliverable that is of value to the customer.

In the context of CSIRTs, customers are the CSIRT stakeholder; therefore, services are delivered on behalf or for the identified stakeholder.

A service is specified by the following template:

- A "Description" field describing the nature of the service.
- A "Value Proposition" field describing the value the service brings to subscribers (what they will achieve via the service, rather than what they get from the CSIRT).

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.

The list of tasks that can be performed as part of the function.

INTERNAL ACTIVITIES

Internal activities designate supporting functions, which are needed to provide services, but are not specific to a CSIRT. Not all internal activities are defined, only those whose specification in this framework can bring value to CSIRT.

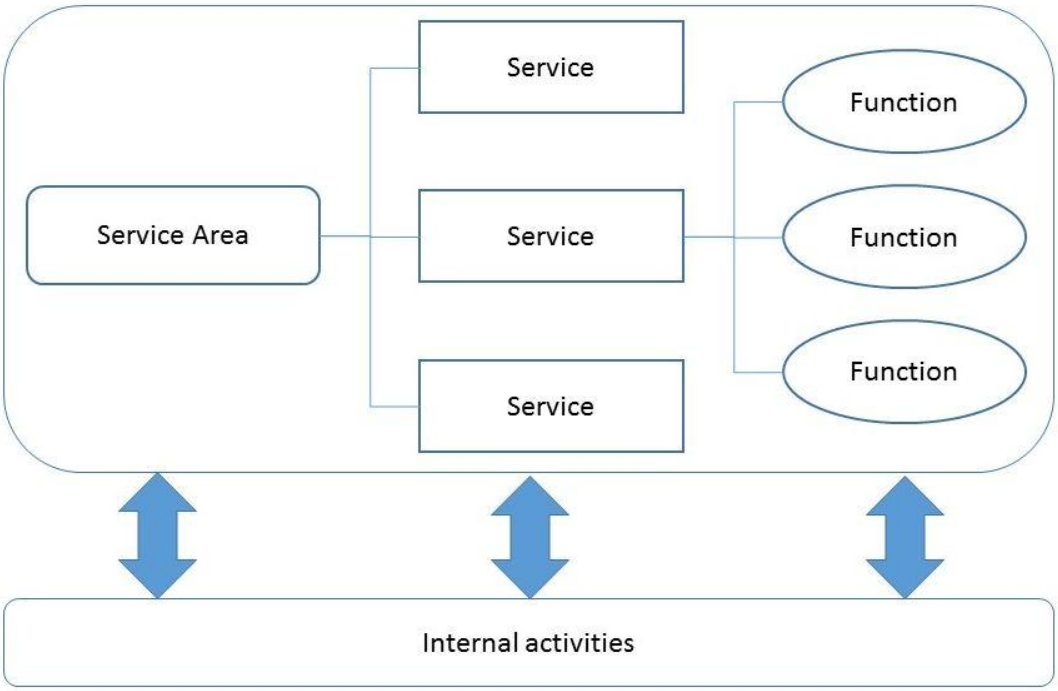

Figure 1: Framework Service Hierarchy

CAPACITY

Within the context of this framework, capacity is generally used to express the quantity of output(s) that can be delivered by a particular capability over a period of time, and in some cases with indication of the number of clients/requests that can be serviced concurrently, where relevant.

CAPABILITY

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

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 maturity of an organization will be determined by the extent, quality of established policies and documentation, and the ability to execute a set process. The level of advancement in knowledge, skill and proficiency is measured against a defined reference model.

DETAILED DESCRIPTION OF THE SERVICES AND INTERNAL ACTIVITIES

Service Area 1 – INCIDENT MANAGEMENT

Incident Management is the raison d'etre of CSIRTs. The functions in this service area cover the full life cycle of an incident's response.

1.1 SERVICE - INCIDENT HANDLING

Services related to the management of a cyber-event, to include alerting constituents and coordinating activities associated with the response, mitigation, and recovery from an incident. Incident handling is dependent upon analysis activities, which are defined in the "Analysis" area.

1.1.1 Function - Incident Validation and Classification

Conclusively verifying that a reported incident in fact occurred and has had some impact on the involved systems and is relevant to the CSIRT's mandate.

Purpose: To provide technical proof that an event is a security incident, network or hardware error and identify the potential security impact and damage on the Confidentiality, Availability, and/or Integrity of information assets in an area the CSIRT carries a responsibility.

Outcome: Determine whether a reported event is indeed an incident that needs to be handled or whether the report can be registered in the relevant systems and closed without further action for the CSIRT or passed on to a relevant entity. Derive particulars of the events that have lead the constituent to believe that a security incident has indeed occurred and determine whether there is malicious intent or if there is a different reason – such as misconfiguration or hardware failure.

1.1.2 Function - Incident Tracking

Documenting information about actions taken to resolve an incident, including critical information collected, analysis performed, remediation and mitigation steps taken, closure and resolution.

1.1.3 Function - Information Collection

The intake, cataloguing, and storage of information related to events and incidents to include:

- **Incident Report Collection:** Collection of reports regarding malicious or suspicious events and incident reports from constituents and 3rd parties (such as other security teams or commercial intelligence feeds), whether manual, automated or machine readable forms.
- **Digital Data Collection:** Gathering and cataloguing of digital data that may be, but are not guaranteed to be, useful in understanding incident activity (e.g., disk images, files, network logs/flows).
- **Other data types (non-digital):** Gathering and cataloguing of non-digital data (physical sign-in sheets, architecture diagrams, business models, site assessment data, policies,

enterprise risk frameworks, etc.).

- **Artifact Collection:** The business and technical processes used to intake, catalogue, store, and track artifact s believed to be remnants of adversary activity.
- **Evidence Collection:** The business of collecting information and data for possible use in law enforcement activities, often including capturing metadata regarding the source, method of collection, and owner and custody information.

1.1.4 Function - Coordination and reporting

Information sharing and advisement activity both internal and external to the CSIRT. This primarily occurs when the CSIRT is reliant on expertise and resources outside of direct control of the CSIRT to effectuate the actions necessary to mitigate an incident. 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 on-going activities from adversaries.

1.1.5 Function - Communication with news media

Communicating with media to explain what happened in a given incident in a manner suitable for release to the public. This typically means simplifying the issues and leave out confidential information, but still give a clear picture of the situation. This can be on behalf of the constituent or on behalf of the CSIRT itself. It is important that the CSIRT has predefined processes with its stakeholder communication department.

1.2 Service - Incident Analysis

Services related to identifying and characterizing information about events or incidents such as scope, affected parties, involved systems, timeframes (discovery, occurrence, reporting), status (ongoing versus completed).

1.2.1 Function - Impact Analysis

Identifying and characterizing the impact to the business function supported by involved systems.

Purpose: To identify the size and scope of the incident to include affected parts of the infrastructure, services, data, and department or organization. A general approach to remediation can be made based on this analysis.

Outcome: Determine the (potential) damage that an incident has incurred or might incur. Identify not only technical aspects, but also any media coverage, loss of trust or credibility and any reputational damage.

1.2.2 Function - Mitigation Analysis

Find measures to stop an ongoing issue, e.g. close a security hole or stop a malicious process.

1.2.3 Function - Recovery Analysis

Define a plan to restore impacted services to full functionality without reopening the original security issue.

1.3 SERVICE - INCIDENT MITIGATION AND RECOVERY

Services related to reducing the impact of an incident and working to restore business functions within the stakeholder.

- Containment: 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.
- Mitigation: Preventing further damage through eradication, implementing a work-around, or implementing more in-depth and comprehensive containment strategies.
- Repair: Implementing changes in the affected domain, infrastructure or network necessary to fix and prevent this type of activity from reoccurring. This includes strengthening the organizational defensive posture and operational readiness by policy changes and additional training and education.
- Recovery: Restoring the integrity of affected systems and returning the affected data, systems and networks to a non-degraded operational state.

1.3.1 Function – Containment

Purpose: Stop an incident from spreading

Outcome: Implement measures that ensure an incident does not spread any further, i.e. remains confined to the currently affected domain.

1.3.2 Function - Restore confidentiality, integrity, availability

Purpose: Restore the all systems to full functionality.

Outcome: Measures to restore the services to full capacity as well as closing any detected vulnerabilities that lead to the original incident.

Service Area 2 - ANALYSIS

In the course of an incident CSIRTs must analyze artefacts they find. There are many different types of artefacts, which warrant a different treatment. Not every team will process every artefact type.

2.1 SERVICE - ARTIFACT ANALYSIS

Services related to the understanding of the capabilities and intent of artifact's (e.g., malware, exploits, spam, and configuration files) and their delivery, detection, and neutralization.

Purpose: As part of the incident handling process, digital artifact's may be found on affected systems or malware distribution sites. Artifact's may be the remnants of an intruder attack, such as scripts, files, images, configuration files, tools, tool outputs, logs, etc. Artifact analysis is done to find out how the artifact may have been used by an intruder, such as to get into an organization's systems and networks, or to identify what the intruder did once in the system. Artifact analysis strives to identify how the artifact operates on its own or in conjunction with another artifact's. This can be achieved through various types of activities including: surface analysis, reverse engineering, runtime analysis, and comparative analysis. Each activity provides more information about the artifact. Analysis methods include but are not limited to identification of type and characteristics of artifact, comparison to known artifact s, observation of artifact execution in a runtime environment, and disassembling and interpreting binary artifact s. By doing an analysis of the artifact (s), an analyst tries to reconstruct and determine what the intruder did, in order to assess damage, develop solutions to mitigate against the artifact, and provide information to constituents and other researchers.

Outcome: Understand the nature of a recovered digital artifact along with its relationship to other artifacts, attacks, and exploited vulnerabilities. Identify solutions to mitigate against analyzed artifact(s) by understanding the tactics, techniques, and procedures used by intruders to compromise systems and networks and carry out malicious activities.

2.1.1 Function - Surface Analysis

Identifying and characterizing basic information and metadata about artifact's (e.g., file type, strings output, cryptographic hashes, file size, filename); along with reviewing any public or private source information about the artifact.

Purpose: As a first step in gathering basic information, surface analysis compares information gathered from the artifact with other public and private artifact s and/or signature repository. All known information (i.e., potential damage, functionality, and mitigation) is gathered and analyzed. Further analysis may be required depending on the objective of the analysis being conducted

Outcome: Identify characteristics and/or signature of digital artifact and any information already known about the artifact including maliciousness, impact, and mitigation. (Such information can be used to determine next steps.)

2.1.2 Function - Reverse Engineering

In-depth static analysis of an artifact to determine its complete functionality, regardless of the environment within which it may be executed.

Purpose: To provide a deeper analysis on malware artifact s 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. Uncovering all of the machine language exposes functions and actions the malware can perform. Reverse engineering is a deeper analysis that is done when surface and runtime analysis do not provide the full information needed.

Outcome: Derive complete functionality of a digital artifact to understand how it operates, how it is triggered, related system weaknesses that can be exploited, its full impact, and potential damage, therefore, developing solutions to mitigate against the artifact and, if appropriate, create a new signature for comparison with other samples.

2.1.3 Function - Run Time or Dynamic Analysis

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).

Purpose: To provide insight to the artifact ’s operation. Use of a simulated environment captures changes to the host, network traffic, and output from execution. The basic premise is to try to see artifact in operation in as close to a real-life situation as possible.

Outcome: Gain additional insight on digital artifact ’s operation by observing its behavior during execution to determine affected host system’s changes, other system interaction, and resulting network traffic in order to better understand system damage and impact, create new artifact signature(s), and determine mitigation steps. (Note: not all functionality is apparent from runtime analysis since not all artifact code sections may be triggered. Runtime only allows the analyst to see what the malware does in the test situation not what it is fully capable of doing.)

2.1.4 Function - Comparative Analysis

Analysis focused on identifying common functionality or intent, including family analysis of cataloged artifacts.

Purpose: To explore an artifact’s relationship to other artifact s. It may identify similarities in code or modus operandi, targets, intent, and authors. Such similarities can be used to derive the scope of an attack (i.e., is there a larger target, has similar code been used before, etc.). Comparative analysis techniques can include exact match comparisons or code similarity comparisons. Comparative analysis provides a broader view of how the artifact or similar versions of it were used and changed over time, helping to understand the evaluation of malware or other malicious types of artifact s.

Outcome: Derive any commonalities or relationships to other artifact s in order to identify trends or similarities that may provide additional insights or understanding of digital artifact ’s functionality, impact, and mitigation.

2.2 Service - Media Analysis

Services involving the analysis of relevant data from systems, networks, digital storage, and removable media in order to better understand how to prevent, detect, and/or mitigate similar or related incidents. These services may provide information for legal, forensic, compliance reviews or other historical reviews of information.

Purpose: To collect and analyze evidence from media such as hard drives, mobile devices, removable storage, cloud storage, or other formats including paper or video. If the findings of the analysis are to be presented in a legal or compliance setting, the information will need to be collected in a forensically sound manner, which preserves the integrity and chain of custody of the evidence. The evidence may include artifact s such as malware left behind; change of state of files, registries, and other system components; network traffic capture or other log files, information in memory. Note that media analysis is looking to find evidence of what happened and optionally attribute that activity; it is different from artifact analysis, which looks to understand one artifact and its relationships. However, artifact analysis techniques may be used as part of the media analysis techniques and methods. These services may also be invoked outside a cyber incident but as part of a human resources issue or other legal or organizational investigation.

Outcome: Present findings that 1) inventory information assets (i.e., intellectual property or other sensitive information found); 2) provide a timeline of events that may shows additions, alterations and deletions made to any media assets involved in the incident, along with who or what performed those activities, if possible, and how all the evidence ties together to explain the extent and impact of the incident.

2.3 Service - Vulnerability / Exploitation Analysis

Services provided to enable a deeper understanding of the vulnerabilities that have been a factor in a cyber-incident

2.3.1 Function - Exploitation Vulnerability / Path Analysis

Understanding the weakness/weaknesses leveraged to cause an incident and the adversarial tradecraft utilized to leverage that weakness.

Purpose: To inform the stakeholder of any known vulnerabilities (common entry points for attackers), thus systems can be kept up-to-date and monitored for exploits, minimizing any negative impact.

Outcome: Have a full grasp of a vulnerability and the way malicious actors will be able to use this vulnerability to execute their infiltration / exploitation of systems

2.3.2 Function - Root Cause Analysis

The understanding of the "design" or "implementation" flaw that allowed the attack.

Purpose: To identify the root cause and point of compromise, helping eradicate an issue completely.

Outcome: Have a firm grasp of the circumstances that allow a vulnerability to exist and in which circumstances an attacker can consequently exploit the vulnerability.

2.3.3 Function - Remediation Analysis

The understanding of the steps necessary to fix the underlying flaw that enabled the attack, and prevent this type of attack in the future.

Purpose: To identify the issue that enabled the compromise, patch the vulnerability, change a procedure or design, review remediation by a third party, and identify any new vulnerabilities introduced in the remediation steps

Outcome: Establish a plan to improve processes, infrastructures and designs to close the specific attack vector and to prevent this attack in the future.

2.3.4 Function - Mitigation Analysis

Analysis to determine the means to mitigate (prevent) the risks created because of an attack or vulnerability without necessarily remediating the underlying flaw that introduced it.

Service Area 3 - INFORMATION ASSURANCE

CSIRTs possess a wealth of experience from handling incidents, they understand what's going on in the wild. It thus makes sense to involve them in any risk management processes as knowledge centers. However CSIRTs typically do not own these processes, they are a component part of them. This service area describes services that help stakeholders to improve their risk management.

3.1 SERVICE - RISK ASSESSMENT

Services related to assessing risk or compliance assessment activities. This may include conduct of the actual assessment, to providing support to evaluate the results of an assessment. Typically done in support of a compliance requirement (e.g., ISO 27XXX, COBIT).

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

Outcome: Consistent process for information risk assessment and management applied to key assets and data; input to risk assessments; selection of relevant risk treatment options to include incident management and forensics where appropriate.

3.1.1 Function – Inventory of Critical Asset/Data

Identify key assets and data that are critical to completing the organization's mission. These assets and data may not necessarily be owned by the organization (e.g., cloud provider or external data set). This includes identifying their location, their owner, their information sensitivity level, their mission function, and their current status / level.

Purpose: To identify on a regular basis those assets and data where incident management may be a requirement to enable the organization to complete its mission, in conjunction with the relevant lines-of-business.

Outcome: A regularly updated inventory, list or database of key assets and data for use by the organization in risk assessments.

3.1.2 Function - Standards Evaluation

Gaining Organizational Risk Policy / Policies and enumerated/identified Standards by Executives for evaluation of Security Level/Status. Suggesting criteria for assessment or benchmarking for Enterprise Risk Managers and CISO's to consider. Examples of standards may include, but are not limited to, Basel II, COBIT, ITIL, Certification and Accreditation.

Purpose: To assist in the selection of an approved information risk assessment methodology for use in the organization and provide input into wider, organizational-level risk assessment and management.

Outcome: A selected information risk assessment methodology for use across the organization; Executive-level support and buy-in for the selection made; organizational policies mandating the use of the selected risk assessment methodology where appropriate; agreed measures, templates and outputs; agreed process and procedures for information

risk assessment; agreed mechanisms to integrate information risk assessment results into organizational-level risk management and decision-making.

3.1.3 Function - Execute Assessment

Assist in conducting reviews and participating in assessments to ensure risk and security requirements are met / addressed.

Purpose: To complete the information risk assessment for a selected key asset or data, using the approved methodology, in as thorough a manner as possible.

Outcome: A completed information risk assessment for the selected key asset or data.

3.1.4 Function - Findings & Recommendations

Developing and providing findings, reports and/or recommendations (e.g., report writing, using the tasks in publication of information).

Purpose: To assist in the full documentation of the findings of a completed risk assessment and enumerate actions to be taken and recommendations to be considered as a result of the assessment.

Outcome: An authorized, signed off, report detailing the critical asset or data, the risk assessment process followed, data used in the risk assessment, results, recommendations, actions, plans and timescales for distribution.

3.1.5 Function - Tracking

Assist the CISO and/or Risk Manager in tracking both status of assessments and subsequent implementation of recommendations.

Purpose: To make sure that all plans, actions and recommendations are followed up and completed within the documented timescales.

Outcome: Regular review of plans and timescales; list of completed actions; revisions to timescales if actions are not completed on time; report of progress against plans and timescales.

3.1.6 Function - Testing

Active testing for compliance with risk levels. Can include penetration testing, vulnerability scanning and assessment, application testing, auditing and verification, etc.

Purpose: To test that the risk treatment(s) selected and implemented are fit for purpose, are implemented correctly, and provide the risk mitigation expected.

Outcome: A documented test plan with expected results; documented tests and results; comparison with expected results; actions and timescales to correct any deviations from expectations.

3.1.7 Function - Risk Assessment Advice

Provide advice on risk assessment standards/approaches/methodologies and how to perform risk assessments and manage results.

3.2 Service – Operating Policies Support

Services that develop, maintain, institutionalize, and enforce organizational concept of operations, and other policies.

Purpose: To act as a trusted advisor on operational policies for information security and incident management to a constituent or line-of-business by providing impartial, fact-based advice, considering the opportunity or problem under discussion, the environment in which the advice may be used and any resource constraints that apply.

Outcome: Business decisions that incorporate information security and incident management considerations; incident management seen as a trusted advisor; members of the incident management team involved in business decisions when and where appropriate.

3.3 Service – Business Continuity and Disaster Recovery Planning Support

Services provided to stakeholder related to organizational resilience activities based on risks identified. This could include a range of risk management activities, from conducting the actual assessment to providing analysis support in evaluating and mitigating the results of an assessment.

Purpose: To act as a trusted advisor on business continuity and disaster recovery to a constituent or line-of-business by providing impartial, fact-based advice, considering the opportunity or problem under discussion, the environment in which the advice may be used and any resource constraints that apply.

Outcome: Business decisions that incorporate business continuity and disaster recovery considerations; incident management seen as a trusted advisor; members of the incident management team involved in business decisions when and where appropriate.

3.4 Service – Technical Security Support

Services providing advice on the execution, integration and/or implementation of pertinent security techniques or technology.

Purpose: To act as a trusted advisor on the technical implications and selected technologies to a constituent or line-of-business by providing impartial, fact-based advice, considering the opportunity or problem under discussion, the environment in which the advice may be used and any resource constraints that apply.

Outcome: Business decisions that incorporate technical security considerations; incident management seen as a trusted advisor; members of the incident management team involved in business decisions when and where appropriate.

3.5 Service – Patch management

Services that assist stakeholder with the capabilities necessary to manage the identification of inventory, systems to patch, deployment and verification of patch installation.

Purpose: To assist in the identification, acquisition, installation and verification of patches for products and systems and to provide an assessment of the utility and impact of patches from an incident management perspective.

Outcome: Organizational awareness and understanding of the patches required; understanding of patches to be applied by service providers; understanding of the impact of patches on information risk; understanding of the impact on incident management.

Service Area 4 – SITUATIONAL AWARENESS

To focus its activities and contribute to the risk management a CSIRT needs to get an overview of the current threat landscape. Getting a good grasp of the threat landscape is no easy task and involves different functions, as described below.

Situational Awareness is a collection of activities that gives an organization an awareness of its operating environment. Situational awareness involves the identification of critical elements that may affect an organization's mission, the monitoring of those elements and using this knowledge to inform decision-making and other actions.

It provides the necessary awareness of events and activities in and around the organization that may affect the organization's ability to operate in a timely and secure manner.

4.1 SERVICE – METRIC OPERATIONS

Services that focus on the development, deployment, and operation of systems and analysis methodologies to identify activities for investigation.

Purpose: To create the information collection infrastructure and processes necessary to provide situational awareness to the organization.

Outcome: An operational information collection infrastructure (i.e. sensors) that provide information for situational awareness.

4.1.1 Function – Requirements Analysis

Understanding the needs of the stakeholder and securing the authorizations under which the CSIRT can operate.

Purpose: The requirements development process identifies the situational awareness needs of the organization and then maps those requirements to the types of information needed to meet those objectives.

Outcome: From an information perspective understand the level of awareness needed by the organization and its stakeholder. In addition, ensure the organization has all the necessary policy and legal approvals to collect the information.

4.1.2 Function – Data Source Identification

Determining the data necessary to fulfil requirements.

Purpose: Sensors come in a variety of forms from automated systems to humans. These sources of information (data) are used to build the situational awareness picture for an organization. The "Identification of Necessary Data" process maps situational awareness requirements to potential information sources (i.e., sensors).

Outcome: The identification of data needed to support the situational awareness requirements of the organization. Some of the data sources may already exist while others may need to be engineered and/or acquired.

4.1.3 Function – Data Acquisition

Determining the methods, tools, techniques, and technologies used to gather necessary data.

Purpose: This process identifies methods for collecting, processing and storing the information (data) that is collected.

Outcome: Determine the specific details as to how the information will be collected, stored, processed and sanitized.

4.1.4 Function - Results Management

Triage and dissemination of information and metrics derived from sensors. Usually, provided via a dashboard for view by various levels within an organization.

Purpose: Make results available to stakeholders.

Outcome: The results may be presented, depending on the targeted audience in the form of dashboards, reports, weekly summary emails etc.

4.2 Service - Fusion and Correlation

Services that conduct analysis and inclusion of multiple data sources. Take feeds of information, regardless of the source, and integrate them into an overall view of the situation (Situational Awareness).

Purpose: Identify new relationships between incidents, indicators and actors that allow improved mitigation or response to a security incident.

Outcome: Enable a consistent process for the organization to leverage new threat information, and integrate it with existing information available within the organization's knowledge repository. The final outcome of this process will be an improved set of information that enables the CSIRT to make decisions in a more efficient and accurate manner.

4.2.1 Function - Determine Fusion Algorithms

Determine the methods and techniques (algorithms) or technologies used to analyze (fuse) the information.

Purpose: As part of incident handling, it is important that the CSIRT maintains a good operational view on information received from various sources. Fusion allows information to be managed in such a way that allows the CSIRT to rapidly consider new information as it is received, and fully contextualize this information and make it usable during the incident handling process.

Outcome: Develop an internal process that allows the intake of new information, its assessment in the context of existing information, and the successful exploitation of the resulting information available to the CSIRT, in the context of an incident.

4.2.2 Function - Fusion Analysis

Analysis (fusing) of the data resources using the data in the knowledge management system to identify commonalities and relationships amongst the data.

Purpose: As part of incident handling, the CSIRT will need to continuously maintain an understanding of the threat a particular incident poses to the organization. In order to do so, it will need an up-to-date awareness of the incident itself and the evolution in the tactics, techniques and procedures leveraged by the adversary. It will need to continuously gather information, and assess it against existing information. This function will leverage the fusion algorithms selected in Function 4.2.1 to perform analysis of threat information obtained from external sources.

Outcome: Understand the impact of new threat information gathered against existing incidents, and well prepare the organization for any changes in TTP's by an adversary, or enable it to continuously update its mitigation and response techniques to better deal with related incidents.

4.3 Service - Development and Curation of Security Intelligence

Services provided to internal or external constituents in the interest of developing and curating third party sources of security intelligence. Security intelligence can be defined as security and threat information that provides either operational intelligence or threat intelligence. Services may include, but are not limited to, analysis, development, distribution, and management of security intelligence, including threat indicators, threat detection logic such as antimalware rules and signatures, and adversary tactics, techniques, and procedures. These services are dependent upon information exchange activities, which are defined in service area 5, "Outreach/Communications".

Purpose: Information from external entities is crucial for obtaining a sufficient level of situational awareness. A CSIRT needs a large amount of high-quality information relevant to its operation, but the cost and workload required to obtain it means that the efforts have to be focused on selected set of sources.

Outcome: Multiple, high-quality data feeds covering all relevant areas of a CSIRT's operation are ingested - primarily through entirely automated processes - by the data management system. Another outcome is also processes to detect anomalies and changes in trends in the information streams obtained from the external sources

4.3.1 Function - Source Identification and Inventory

Continual identification, maintenance, and integration of information sources into knowledge management and analysis processes.

Purpose: Obtain relevant, high-quality information from external sources to perform effective incident response and to proactively increase the situational awareness (and the security posture of the organization, in general). External sources complement data collected internally: incident reports, vulnerability reports and output from sensors operated by the CSIRT.

Outcome: The acquisition of high-quality, relevant security information from internal, external, open source and/or commercial sources. All collected information is stored in the data management system.

4.3.2 Function - Source Content Collection and Cataloguing

The acquisition of threat information source materials. These sources may be both internal, external, open source and/or fee for service.

Purpose: Rate the quality of collected information. Observe changes in characteristics (including quantity) of data obtained from external sources to detect anomalies and/or new trends.

Outcome: Documentation containing quality ratings of sources. Automated or semi-automated process to major changes in the overall characteristics of the information obtained from external sources.

4.3.3 Function – Information sharing

Capturing, developing, sharing, and effectively using organizational knowledge to include data mark-up (e.g., STIX, TAXII, IODEF, TLP), indicator databases, and malware / vulnerability catalogues.

Purpose: Constituents require cybersecurity data and knowledge at a level of quality and timeliness appropriate for their needs. Cybersecurity data consists of information intended to be processed by systems in order to support security automation. Cybersecurity knowledge consists of information intended for human cybersecurity analysts/operators. Additionally, other CSIRT services and functions require cybersecurity data and knowledge as inputs. Such information is best managed as an overall CSIRT resource given that most information is re-used across several services and functions.

Outcome: Cybersecurity data and knowledge of the required quality is provided to constituents in a timely fashion. Other CSIRT services and functions can easily obtain the data and knowledge they require from a single source within the CSIRT.

Service Area 5 - OUTREACH/COMMUNICATIONS

5.1 SERVICE - SECURITY AWARENESS RAISING

Services that work within the stakeholder to raise the collective understanding of threats that they face and actions that can be taken to reduce the risk posed by these threats

5.2 SERVICE - CYBERSECURITY POLICY ADVISEMENT

5.2.1 Function - Policy Consultancy

Cyber security policies are often written in a formal language, devising overall goals independent of the concrete tasks CSIRT performs. Yet they ultimately shape the services performed by a CSIRT.

Purpose: Creation of Cyber Security policies and their interpretation needs a translation from the policy framework into the services portfolio down to the individual functions performed by a CSIRT.

Outcome: CSIRTs understand policies and can actively contribute to their creation.

5.2.2 Function - Legal Consultancy

Advising the stakeholder about the legal aspects of incident response

Purpose: Incident response often deals with legally delicate issues. E.g. CSIRT staff is often faced with privacy sensitive information or even material that is illegal to possess in certain jurisdictions. CSIRTs and its constituents need to ensure that they operate in a legal manner. In many cases this function will be provided by an external legal expert with sufficient knowledge of CSIRTs.

Outcome: Legal advice and assessment of a given action or process.

5.2.3 Service – Information Sharing and Publications

Services that focus on broad communication, including notifications made by the organization to their constituency in support of operations. Examples include notations of training, events, organizational policies and procedures.

5.2.4 Function - Public Service Announcements

Dissemination of security related information to improve awareness and implementation of organizational, constituent, sector or public security practices.

5.2.5 Function - Publication of Information

- Requirements Gathering: Identifying what information is required to be disseminated, to whom, and in what manner and timeframe (scoping).
- Note: publication may be to a limited audience or more in-depth publication for partner audiences.
- Development: Defining the format and purpose of information products to fulfill

requirements.

- Authoring: Accurately capturing information so that it is readily understood by the intended audience(s) (e.g., presenting the results of forensic, incident, vulnerability, and malware management activities).
- Review: Reviewing publication for clarity, accuracy, grammar, spelling, sensitivity, and adherence to information disclosure rules, and obtaining final approval.
- Distribution: Delivery of information to intended audience via necessary and appropriate channels

Service Area 6 - CAPABILITY DEVELOPMENT

6.1 SERVICE - ORGANIZATIONAL METRICS

Services that focus on identification, establishment, collection, and analysis of achievement of organizational performance goals, along with measuring organizational effectiveness.

Purpose: A key struggle for computer security incident response teams (CSIRT) and incident management organizations today is determining how successfully they meet their mission of managing cybersecurity incidents. This function is focused on identifying what questions (information) need answering for management, CSIRT teams, and stakeholders among others to evaluate their operations and show value; establishing mechanisms for collecting the measurements to provide needed metrics, and then collecting, analyzing, and presenting results.

Outcome: Provide the necessary awareness and empirical evidence to demonstrate how well an incident management organization is meeting and executing their mission; while identifying gaps for improvement. Use this information to facilitate decision making and improve performance and accountability.

6.2 SERVICE - TRAINING AND EDUCATION

Capability is the core building block for CSIRT Services and provides training and education to a CSIRT stakeholder on topics related to cybersecurity, information assurance and incident response. Capacity infers some level of capability at some level of maturity.

Purpose: A training and education program is usually the first step towards defining and putting into motion a capability building entity. This can be done through various types of activities including training and education, documented requisite knowledge, skills and abilities required, developed educational and training materials content delivery, mentoring, professional and skill development, and delivery of exercises and labs. Each of these activities will collectively contribute to the organization's and Team's capability.

Outcome: Understand the landscape of the training and education program as well as its relationship in supporting the CSIRT Team's Capability building. Be in a position to understand and document the types of Team and Organization results, as well as the KPIs to be able to understand progress achieved.

6.1.1 Function - Knowledge, Skill, and Ability Requirements Gathering

Knowledge, Skill, and Ability (KSA) requirements gathering: Collecting knowledge, skill, and ability needs and the competence of a stakeholder in regard to determining what training and education should be provided.

Purpose: To properly assess, identify, and document what the CSIRT Team requisite KSA's, to enable ready and strong Team members.

Outcome: Identify needed characteristics of KSA's and a process by which the CSIRT Team can meet business needs. This will determine what level the Team is operating at, as well as if and where it has opportunities for improvement.

6.2.1 Function - Development of Educational and Training Materials

Development of Educational and Training Materials: Building or acquiring content of educational and training materials such as presentations, lectures, demonstrations, simulations, etc.

Purpose: Educational and training material development is used by a CSIRT Team to help maintain user awareness, keep the Team fresh with rapidly changing landscape and threats, and facilitate communications between the CSIRT and its constituencies.

Outcome: CSIRT training and education materials that are of adequate quality; deliver to the needs of the rapidly changing CSIRT environment and utilize varied and effective presentation techniques and platforms.

6.2.2 Function - Delivery of Content

Transfer of knowledge and content to "students". This can occur via various methods, such as computer-based training/online, instructor-led, virtual, conferences, presentations, lab, etc.

Purpose: A formal process for content delivery will help the Team identify a transparent approach to how CSIRT members are best able to receive their training.

Outcome: A content delivery framework, which utilizes all available methods, presenting, learning of technical, soft skills and processes, using all alternative approaches, including hands-on labs, remote CBT and in person training, etc.

6.2.3 Function – Mentoring

Learning from experienced staff, through an established relationship, using on-site visits, rotation (exchange), shadowing, and discussion rationale for specific decisions and actions.

Purpose: 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.

Outcome: A CSIRT Team that has increased retention, loyalty, confidence and overall ability to make sound decisions.

6.2.4 Function - Professional Development

Helping staff members successfully and appropriately plan and develop their careers. Can include attending conferences, advanced training, cross-training activities, etc.

Purpose: Professional development promotes a continuous process of securing new knowledge, skills and abilities that relate to the overall Team environment.

Outcome: Derive characteristics of professional development so the Team not only has confidence, but also has the requisite knowledge, skills and abilities that they directly transfer to practice, and are up to date based on the job roles and needs.

6.2.5 Function - Skill Development

Providing training for organization staff on tools, processes, and procedures for daily operations functions.

Purpose: After the appropriate skills have been identified, a CSIRT Team needs to commit to a series of actions that will determine their ability for readiness.

Outcome: Developed and trained staff with the needed technical, soft skills and process understanding. CSIRT members who are ready to address the daily operational challenges, supporting both the Team and its customers.

6.3 Service - Conducting Exercises

Services 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 as a whole. These types of exercises can be used to:

- Test policies & procedures: Team assesses whether there are sufficient policies and procedures in place to meet the event. This is, generally, a paper/table top exercise.
- Test operational readiness: Team assesses whether the right people are in place to respond to the event and whether procedures are executed correctly. This, typically, involves exercising procedures.

Purpose: Exercises are conducted to improve the effectiveness and efficiency of cybersecurity services and functions. This function and associated sub-functions address both the needs of the organization as well as 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 for which they have already received training. 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.
- Certify: 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 will be directly improved, and lessons for further improvements will be identified. Depending on the specific objective(s) of an exercise, cybersecurity may also be demonstrated to stakeholders, staff can be trained, and the efficiency and effectiveness of services and functions can be assessed and/or certified. Lessons for improving future exercises can also be identified

6.3.1 Function - Requirements Analysis

Define the specific service/capability that the exercise should focus on.

Purpose: Ensure an effective effect and outcome of the exercise by focusing on specific issues.

Outcome: The purpose of the exercise.

6.3.2 Function - Format and Environment Development

Define the format and the extent of the exercise.

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

Outcome: The type of the exercise as well as the resources needed to conduct it.

6.3.3 Function - Scenario Development

Development of exercise scenarios in support of stakeholder objectives.

Purpose: The purpose of organizing exercises is to provide an opportunity for the target audience to improve the efficiency and effectiveness of their services and functions through the handling of simulated cybersecurity events/incidents.

Outcome: A specific target audience has improved the efficiency and effectiveness of its services and functions and has identified lessons for its further improvements. Lessons for improving future exercises have also been identified.

6.3.4 Function – Executing Exercises

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 virtual environments, simulations, field tests, table-tops, mock scenarios, or a combination.

Purpose: By conducting drills/exercises a CSIRT Team will increase its confidence in the validity of an organization's CSIR plan and its ability for execution.

Outcome: A Team that is as ready as possible, ensuring the KSAs key processes and execution of all work successfully together. This will also help determine the level the Team is operating at as well as if and where it has room for improvement.

6.3.5 Function - Exercise Outcome Review

Develop an after-action report which includes lessons learned or findings / best practices from the exercise.

6.4 Service - Technical Advice

Services that focus on recommendation, development, provision, and acquisition of cybersecurity related infrastructures, tools and services for a stakeholder. All of these systems and tools are related to CSIRT/security and not to general Information Technology; these systems could include messaging / alerting portals. Note that a CSIRT may well provide certain tools as a service to its stakeholder.

Purpose: Within the process of building and enhancing the capabilities of CSIRT stakeholder, a special focus is given to provide assistance on designing, acquiring, managing, operating and maintaining their infrastructure, systems and tools as well as to assist in building capability, capacity, and maturity of CSIRT services to stakeholders. This is a maturation of service levels.

Outcome: Develop a systematic approach for needs assessment, requirements definition, layout design, acquisition, compliance verification, maintenance and upgrades, operational training, internal and external audits of cybersecurity related infrastructures and tools

6.4.1 Function - Infrastructure Design and Engineering

Assisting in the design and engineering of the infrastructure to support stakeholder requirements.

Purpose: Provides broad understanding of the design methodology, knowledge of relevant standards and norms, and highlights best practices in designing and engineering the infrastructure, based on comprehensive needs assessment and analysis of the stakeholder requirements.

Outcome: Practical experience in developing and comparing infrastructure design approaches and alternatives, based on international best practices and incorporating the relevant standards and norms.

6.4.2 Function - Infrastructure Procurement

Assisting in the procurement of infrastructure, whether assisting in developing risk framework maturity or minimum-security requirements and standards for contract language (e.g., requiring compliance with a particular standard such as a product certification).

Purpose: Gain insight on developing the terms of reference for infrastructure procurement, in view of institutional, technical, and operational requirements.

Outcome: Understanding the process of infrastructure procurement, while observing relevant standards and norms, and taking into consideration various technical measures and contracting procedures that need to be followed.

6.4.3 Function – Tools Evaluation

Evaluation of tools on behalf of the stakeholder.

Purpose: Provide support in assessing the functionality and compliance of various tools, including hardware equipment, software, and custom applications.

Outcome: Analysis of the performance of tools as well as their compliance with standards, norms, and the preset terms of reference.

6.4.4 Function - Infrastructure Resourcing

Assisting in acquiring needed infrastructure resources. (i.e., hardware vendors, service providers, etc.)

Purpose: Highlight the key factors for achieving successful infrastructure resourcing, and develop mechanisms for establishing sustainable and effective relationships with solution providers and vendors based on clear responsibility and accountability.

Outcome: Derive key performance indicators (KPIs) for infrastructure resourcing, with appropriate service level agreements (SLAs) that may provide for efficient and effective infrastructure resourcing.

6.5 SERVICE - LESSON LEARNED

Incident response always has a reactive component to it. Often time is short and the initial situation is unclear. Many incidents happen because of an underlying root cause, that my need to be remediated at a later stage. This service aims at preventing similar incidents and at improving response to a similar or more general situation.

Purpose: Identify root causes of an incident and recommend actions to the stakeholder.

Outcome: Recommendations to adjust process, procedures and remediate underlying root causes for the stakeholder.

Service Area 7 - Research And Development

Keeping up with the ever evolving threats surface requires CSIRTs to constantly adapt. THis requires continuous research and development of new and existing tools.

7.1 Service - Development of Vulnerability Discovery/Analysis/Remediation/Root Cause Analysis Methodologies

Services that help define, identify new capabilities and improve methodologies for performing vulnerability related services or coordinating other organizations or commercial practices that can demonstrate the same.

Purpose: Some organizations will operate by only obtaining vulnerability information from external sources, but there are organizations that will have a need/desire to have organic capabilities to discover and analyze vulnerabilities. This function is intended to outline how an organization might architect these vulnerability research functions.

Outcome: When necessary determine the methodologies an organization may use to better understand vulnerabilities.

7.2 Service - Development of Technologies and Processes for Gathering/Fusing/Correlating Security Intelligence

Services that define, identify new capabilities, and improve methodologies for performing information analysis and sharing related services as it relates to operational and threat intelligences.

Purpose: In order to be successful, any security intelligence function must be able to collect information, as well as share relevant information with third parties. This collection is often dependent on human relationships between the sharing parties that effectuate a level of trust sufficient to enable sharing of sensitive information. An analyst must be able to develop these relationships, identify the appropriate sets of information that need to be shared, identify the protocols most suited for automated exchange, relationship management and joint investigations, and evaluate the effectiveness of an information source.

Outcome: The organization has processes and procedures in place to collect, analyze, synthesize and assess the relevance of information from external sources that describe threats on information security assets. The organization has the organic ability to develop new sources and sharing partners.

7.3 Service - Development of Tools

Services that develop, identify new capabilities, and share approaches to new tools and to automate the execution of CSIRT related processes.

Purpose: Develop tools the satisfy specific needs of a CSIRT.

Outcome: Tools developed by CSIRTS to aid in automation of CSIRT related tasks are scalable, reliable, produce deterministic results, and do not degrade the security posture of the CSIRT using them. Frees analyst resources for non-routine tasks.

Internal Activity 1 - DATA AND KNOWLEDGE MANAGEMENT

CSIRTs deal with a lot of information, both structured and technical as well as unstructured into the form of processes and the knowledge of "How a certain task is performed". Many times, the later information is not well documented. This may lead to a loss of capability if staff leaves. Structured information on the other hand can come in huge quantities and needs to stored and processed accordingly.

1.1 STANDARDS/SPECIFICATIONS MANAGEMENT

Data and information must be stored in a manner that allows efficient processing. This is typically done by adapting standards. These standards need to be flexible enough to accommodate new types of data yet specific enough to be of use.

1.1.1 DATA STANDARDS

Purpose: Ensure that available information, from past and present, can be processed

Outcome: Standards and possibly tools to process a given data type

1.1.2 KNOWLEDGE SPECIFICATIONS MANAGEMENT

Purpose: Specify how knowledge, which is accumulated over time is to be handled

Outcome: Standards and processes to handle information

1.2 DATA STORAGE MANAGEMENT

CSIRTs often handle information which needs with special requirements on Confidentiality, Integrity and Availability.

Purpose: Specify how data is to be stored

Outcome: Data storage specifications for the different types of data.

1.3 DATA PROCESSING MANAGEMENT

CSIRTs often need to process large amounts of data, either for analysis or to forward to other teams or the stakeholder. For efficient use this data must be processed in an efficient manner.

Purpose: Define the workflow and tools used to efficiently process available data

Outcome: Tools and workflow specifications

1.4 DATA ACCESS MANAGEMENT

Purpose: Ensure that data is only accessible to authorized entities.

Outcome: Access management specification

1.5 Automation Support

Purpose: Data, especially large quantities, must be processed as automatically as possible to scale.

Outcome: Tools and processes for automation

Internal Activity 2 - Relationship Management

2.1 POC and Communications Management

Maintaining lists of points of contact and organizing mailing lists, topic taxonomies and mapping these to communications channels.

Management of lists used to distribute announcements, alerts, warnings, data feeds and other publications or information sharing.

Management of secure communication mechanisms used for email, web, instant messaging, or voice communications.

2.2 Peer Relationship Management

Development and maintenance of relationships with organizations that may be able to enable the execution of the mission of the CSIRT. This may involve ensuring interoperability or fostering collaboration between or across organizations.

2.3 Stakeholder Relationship Management

Development and implementation of practices, strategies and technologies used to identify, distinguish, understand, manage, track, and evaluate stakeholders.

2.4 Conferences / Workshops

Providing opportunities for the CSIRT and its stakeholder to spend time together discussing threats and challenges that they are facing, strengthen trust relationships, exchange contacts, and share best practices or lessons learned.

2.5 Stakeholder Engagement/Relations

Includes coordination with sector / vertical organizations, and maintaining formal points of contact with both internal and external stakeholders. Engagement with executive levels within the organization to educate on the mission of the organization and ensure security awareness understanding.

Internal Activity 3 - Branding/Marketing

Activities that ensure that stakeholders are aware of the CSIRT and the capabilities provided by the CSIRT, as well as how they should interact with the CSIRT to convey their needs.

Internal Activity 4 - PARTICIPATING IN EXERCISES

A CSIRT can have various levels of participation in an exercise due to its maturity level.

- Evaluation: Evaluate the outcomes of an exercise, solicit feedback, and identify lessons based on observation of the exercise.
- Observation: Observe a third-party exercise.
- Coordination: Coordinate an exercise.
- Participation: Participate in a cyber-exercise. Participant gets to choose the level of participation and gains from the outcome of the exercise (e.g., have a third-party evaluate their participation).

Purpose: The purpose of participating in exercises is to improve the effectiveness and efficiency of cybersecurity services and functions. The form of participation can be one of the following:

- Observer: Staff observe the conduct of an exercise but are not part of the target audience and are not challenged by the exercise events nor assessed for their performance. Observing without direct participation can help improve the effectiveness and efficiency of CSIRT services and functions to some extent. It can also help organize future exercises.
- Exercise Audience: Staff participate in an exercise as the target audience and are challenged by the exercise events, and may be assessed as well.

Depending on the modalities of the exercise, staff may travel to the exercise's location or participate remotely from their regular office or another suitable location. As well, the exercise may provide a specific environment or the participants may participate from their own exercise environment or their usual work environment.

Outcome: An improvement in the effectiveness and efficiency of cybersecurity services and functions, as well as the identification of lessons for further improvements. Depending on the specific objective(s) of an exercise, cybersecurity may also be demonstrated to stakeholders, staff can be trained, and the efficiency and effectiveness of services and functions can be assessed and/or certified. Lessons for improving future exercises can also be identified.

Internal Activity 5 - LESSONS LEARNED REVIEW

Similar to service 6.5 but with a focus on the CSIRT itself.

Purpose: Improve the capabilities of a CSIRT by analyzing the performance after an incident has been closed

Outcome: Recommendations for changes in procedures, processes, setup or infrastructure.

ANNEX 1 - SUPPORTING RESOURCES

FIRST - https://www.first.org

CERT/CC - http://www.cert.org

Trusted Introducer – https://www.trusted-introducer.org

TLP - https://www.first.org/tlp

IETF - https://www.ietf.org

ISO/IEC 27035 - http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379

ANNEX 2 - GLOSSARY

- Application Testing – An investigation conducted to provide stakeholders with information about the quality of the product or service under test.
- Basel II – The second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision.
- CERT/CC – Computer Emergency Response Team Coordination Centre.
- CISO – Chief Information Security Officer.
- Cloud – A distributed computing environment that allows application software to be operated using internet-enabled devices.
- COBIT – Control Objectives for Information and Related Technology.
- Cryptographic Hash – A hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone.
- CSIRT – Computer (or Cyber) Security Incident Response Team.
- External Data Set – A third-party collection of data.
- FIRST – Forum of Incident Response and Security Teams.
- Function – A means to fulfil the purpose or task of a specified service.
- Fuzz Testing – A software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program.
- Hardware / Software Emulator – Hardware or software that enables one computer system (called the host) to behave like another computer system (called the guest). Typically, utilized to enable the host system to run software or use peripheral devices designed for the guest system.
- IDMEF – xxx
- IEC – International Electrotechnical Commission.
- IETF – Internet Engineering Task Force.
- IODEF – Incident Object Description Exchange Format, which is a data representation that provides a framework for sharing information commonly exchanged by Computer Security Incident Response Teams (CSIRTs) about computer security incidents.
- ISO – International Organization for Standardization.
- ISO/IEC 27000-Series (ISO27k) – Information security standards that provide best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).
- ITIL – Information Technology Infrastructure Library, which is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.
- Open Source – A development model that promotes universal access via a free license to a product's design or blueprint, and universal redistribution of that design or blueprint,

including subsequent improvements to it by anyone.

- Penetration Testing – An attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality, and data.
- Reverse Engineering – The process of extracting knowledge or design information from anything man-made and re-producing it or reproducing anything based on the extracted information.
- RID – Real-time Inter-network Defense, which is an inter-network communication method to facilitate sharing incident handling data while integrating existing detection, tracing, source identification, and mitigation mechanisms for a complete incident handling solution.
- Sandbox – A security mechanism for separating running programs.
- Service – The action of helping or doing work on behalf of or for the stakeholder.
- STIX – Structured Threat Information eXpression, which is a collaborative community-driven effort to define and develop a standardized language to represent structured cyber threat information.
- Strings Output – A resulting sequence of characters, either as a literal constant or as some kind of variable.
- TAXII – Trusted Automated Exchange of Indicator Information, which is a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries.
- TLP – Traffic Light Protocol. Used to ensure that sensitive information is shared with the correct audience.
- Virtual Environment – An emulation of a particular computer system.
- Vulnerability Scanning and Assessment – A security technique used to identify security weaknesses in a computer system