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.

Product Security Incident Response Team (PSIRT) Services Framework
Version 1.0
# Table of Contents

## INTRODUCTION

OPERATIONAL FOUNDATIONS

### SERVICE AREA 1  STAKEHOLDER ECOSYSTEM MANAGEMENT

#### SERVICE 1.1 INTERNAL STAKEHOLDER MANAGEMENT

- Function 1.1.1 Engage Internal Stakeholders
- Function 1.1.2 Internal Secure Development Lifecycle
- Function 1.1.3 Incident Post-Mortem Process

#### SERVICE 1.2 FINDER COMMUNITY ENGAGEMENT

- Function 1.2.1 Engage Finders

#### SERVICE 1.3 COMMUNITY AND ORGANIZATIONAL ENGAGEMENT

- Function 1.3.1 Define & Engage with Upstream Communities & Partners
- Function 1.3.2 Engage with Peer PSIRTs
- Function 1.3.3 Engage with Coordinators (CERTs, CSIRTs, or other coordination center organizations)
- Function 1.3.4 Engage with Security Vendors
- Function 1.3.5 Engage with Bug-Bounty Vendors

#### SERVICE 1.4 DOWNSTREAM STAKEHOLDER MANAGEMENT

- Function 1.4.1 Engage with Downstream Stakeholders

#### SERVICE 1.5 INCIDENT COMMUNICATIONS COORDINATION WITHIN THE ORGANIZATION

- Function 1.5.1 Provide Communication Channels/Outlets
- Function 1.5.2 Secure Communications Management
- Function 1.5.3 Security Defect Tracking System Updates
- Function 1.5.4 Information Sharing and Publishing

#### SERVICE 1.6 REWARD FINDERS WITH RECOGNITION & ACKNOWLEDGEMENT

- Function 1.6.1 Provide Acknowledgements
- Function 1.6.2 Reward Finders

#### SERVICE 1.7 STAKEHOLDER METRICS

- Function 1.7.1 Understand Stakeholder Artifact Requirements
- Function 1.7.2 Collect Stakeholder Metrics
- Function 1.7.3 Analyze Stakeholder Metrics
- Function 1.7.4 Provide Stakeholder Metric Artifacts

## SERVICE AREA 2  VULNERABILITY DISCOVERY

### SERVICE 2.1 INTAKE OF VULNERABILITY REPORTING

- Function 2.1.1 Ensure Reachability
- Function 2.1.2 Handle Vulnerability Reports

### SERVICE 2.2 IDENTIFY UNREPORTED VULNERABILITIES

- Function 2.2.1 Monitor Exploit Databases
- Function 2.2.2 Monitor Conference Programs
- Function 2.2.3 Monitor Publications by Renown Finders
- Function 2.2.4 Monitor Mass Media

### SERVICE 2.3 MONITORING FOR PRODUCT COMPONENT VULNERABILITIES

- Function 2.3.1 Inventory of Product Components
- Function 2.3.2 Monitor Third-Party Advisories
- Function 2.3.3 Monitor Vulnerability Intelligence Sources
74 Function 2.3.4 Set-up Procedures for Intake of Vendor-Internal Supply Chain.................44
75 Function 2.3.5 Notification of Internal Development Teams........................................45
76 SERVICE 2.4 IDENTIFYING NEW VULNERABILITIES...........................................45
77 Function 2.4.1 Vulnerability Assessment.................................................................45
78 Function 2.4.2 Maintain Expertise for Security Testing Tools...................................46
79 SERVICE 2.5 VULNERABILITY DISCOVERY METRICS.........................................46
80 Function 2.5.1 Operational Reports.......................................................................46
81 Function 2.5.2 Business Reports..........................................................................47
82 SERVICE AREA 3 VULNERABILITY TRIAGE AND ANALYSIS..............................49
83 SERVICE 3.1 VULNERABILITY QUALIFICATION..................................................49
84 Function 3.1.1 Quality Gate and Bug Bars............................................................49
85 Function 3.1.2 Continuous Improvements............................................................50
86 SERVICE 3.2 ESTABLISHED FINDERS...............................................................50
87 Function 3.2.1 Finder Database.............................................................................50
88 Function 3.2.2 Accelerated Handling for Established Finders..................................51
89 Function 3.2.3 Finder Profile..............................................................................51
90 Function 3.2.4 Defining Finder Report Quality......................................................51
91 SERVICE 3.3 VULNERABILITY REPRODUCTION..................................................52
92 Function 3.3.1 Establish Service Level Agreement for a Vulnerability Reproduction........52
93 Function 3.3.2 Reproduction Test Environment....................................................52
94 Function 3.3.3 Reproduction Tools.......................................................................52
95 Function 3.3.4 Vulnerability Storage.....................................................................53
96 Function 3.3.5 Affected Products.........................................................................53
97 SERVICE AREA 4 REMEDIATION.................................................................54
98 SERVICE 4.1 SECURITY UPDATE RELEASE MANAGEMENT PLAN.....................55
99 Function 4.1.1 Product Lifecycle Management.......................................................55
100 Function 4.1.2 Method of Delivery.......................................................................55
101 Function 4.1.3 Delivery Cadence..........................................................................56
102 SERVICE 4.2 REMEDIATION..............................................................................56
103 Function 4.2.1 Analysis.........................................................................................56
104 Function 4.2.2 Remedy Resolution.......................................................................57
105 Function 4.2.3 Remedy Delivery..........................................................................58
106 Function 4.2.4 Risk Management.........................................................................58
107 SERVICE 4.3 INCIDENT HANDLING.................................................................59
108 Function 4.3.1 Establish Situation Room..............................................................59
109 Function 4.3.2 Incident Management....................................................................60
110 Function 4.3.3 Communication Plan.....................................................................60
111 SERVICE 4.4 VULNERABILITY RELEASE METRICS........................................61
112 Function 4.4.1 Operational Reports.....................................................................61
113 Function 4.4.2 Business Reports..........................................................................62
114 SERVICE AREA 5 VULNERABILITY DISCLOSURE.............................................63
115 SERVICE 5.1 NOTIFICATION.............................................................................64
116 Function 5.1.1 Intermediate Vendor (Downstream Vendor)....................................64
117 Function 5.1.2 Coordinators..................................................................................64
PSIRT Services Framework

Introduction

A Product Security Incident Response Team (PSIRT) is an entity within an organization which, at its core, focuses on the identification, assessment and disposition of the risks associated with security vulnerabilities within the products, including offerings, solutions, components and/or services, which an organization produces and/or sells.

A properly deployed PSIRT is not an independently operating group, disconnected from the development of the organization’s products. Instead it is part of the organization’s broader secure engineering initiative. This structure ensures that security assurance activities are integrated into the Secure Development Lifecycle (SDL).

Product security incident response is often associated with the maintenance phase of the SDL because most product security vulnerabilities are reported as quality escapes after the product has been released to the market. However, PSIRT can be impactful in the earlier requirements gathering of architecture, design, planning and risk modeling phases.

The difference between PSIRT and CSIRT

The focus on products is the key differentiator between the PSIRT of an organization and other incident response teams represented in the same organization, such as Computer Security Incidence Response Team (CSIRT). Generally, an Enterprise CSIRT is focused on the security of computer systems and/or networks that make up the infrastructure of an organization.

While there are important differences between an Enterprise CSIRT and PSIRT, it is important to recognize that there is also synergy between the two groups. The important point to take away is that PSIRT does not operate independently of other parts of an organization and throughout this framework we will highlight areas of collaboration and synergy that should be nurtured.

PSIRT Organizational Structure
PSIRTs can be as unique and varied as the products they help protect. Between organizations within the same sector or industry there will be variations in business characteristics, operating models, product portfolios, organizational structures, and product development strategies. As a result, there is no single one-size fits all product security incident response strategy or team template for all organizations to follow. However, three PSIRT models are used by most companies: Distributed, Centralized and Hybrid.

**Distributed Model**

The Distributed model utilizes a small core PSIRT that works with representatives from the product teams to address security vulnerabilities in products. In this model, the smaller PSIRT operations team has several core responsibilities:
- Creating policies, processes procedures and guidelines for the triage, analysis, remediation, and communication of fixes, mitigations or other advisory information to address security vulnerabilities.
- Establishing a matrix of (tiered) product security engineering representatives throughout the organization.
- Offering leadership and guidance regarding product security vulnerability response and potential risk to the business.
- Acting as the collection point for incoming security vulnerabilities where the economies of scale benefit from a central point of control.
- Notifying the security engineer representatives of new security vulnerabilities, and assist in the development of remediation plans, and draft/publish communication of a fix or mitigation, including incident management.

An organization with a large and diverse product portfolio can benefit from the Distributed model because the cost of the PSIRT mission is defrayed across the organization. This model also allows the PSIRT mission to scale by leveraging the skilled people in the product engineering teams.

The challenge with the Distributed PSIRT model is that the people responsible for performing the triage and delivering the fixes for security vulnerabilities are not directly controlled by or do not report to the PSIRT Operations team.

**Centralized Model**

The Centralized model has a larger PSIRT staff drawn from multiple departments that report into one or more senior executives responsible for the organization’s product security. This model might have a structure similar to the following:
● **PSIRT Program Management Department**: Creates policies, processes procedures and guidelines for the triage, analysis, remediation, and communication of fixes for security vulnerabilities. Manages the operations of the overall PSIRT initiative, ticketing system and represents PSIRT leadership to the organization.

● **PSIRT Security Intelligence and Triage**: Monitors various external sources for security vulnerabilities. Assesses the initial impact of security vulnerabilities to the organization’s product portfolio.

● **PSIRT Remediation and Communications**: Directly provides code fixes for security vulnerabilities to the product engineering teams.

This model works well with a smaller organization and/or an organization with a homogenous product portfolio. This model concentrates and cultivates a high level of security skill and expertise into one area of the organization. The challenge with this model is in the cost of maintaining a centrally specialized team that does not scale as well if the product portfolio grows and/or becomes more diverse.

**Hybrid Model**

The Hybrid model is a variation that includes characteristics of both the Distributed and Centralized model. An organization may choose to implement some characteristics and features of both models, creating a hybrid that takes into account the following factors:
Other Considerations

It is important for a PSIRT to have the autonomy to maintain an independent and objective position on the organization’s product security vulnerabilities. As such, in developing the organization’s PSIRT strategy and structure, the organization should consider how the team should best be integrated into the organization and its reporting structure. It is important that a PSIRT report to an executive of the company that confirms the authority of the PSIRT.

As a PSIRT continues to mature and scale, and the mission evolves, the composition or reporting structure of the team could change. The driving force of change and maturity of a PSIRT is its key stakeholders and, unfortunately, the impact of a severe vulnerability on a broad spectrum of the organization’s stakeholder base. Stakeholders are often defined by the model adopted by the organization as well as the size of the organization.

Stakeholders

Considering the stakeholders’ needs and requirements is a critical part of defining the strategy and structure of a PSIRT. The model that an organization adopts to form the PSIRT can dictate the identity of the stakeholders and the amount of influence they have. It is critical to continue to maintain positive relationships. Service Area 1: Stakeholder Ecosystem Management, contains more detail on the ecosystem of stakeholders and how to manage them.

One final consideration in the formation of the product incident response team and strategy is influencers. This is different than stakeholders, in that stakeholders are discretely named people or groups of people. In contrast, influencers are industry and government standards, legislation, regulations, and trends. These influencers may levy greater requirements on the formation, strategies, policies, and operational characteristics of a PSIRT than the stakeholders.
What does the PSIRT team do?

The model used will define the scope and operational activities of a PSIRT, but not necessarily change the actions an organization needs to take with respect to addressing security vulnerabilities in their products. The model refines the scope of the capabilities, actions and responsibilities directly attributed to the PSIRT rather than those distributed throughout the organization.

Ongoing Process and Policy Development

PSIRTs establish the organization’s policies with respect to product security. The needs of the business drive and dictate the requirements of PSIRT and not the other way around. Before the PSIRT policies can be implemented, they must be reviewed and imbued with authority by the organization’s leadership. Approved policies must be followed with clear procedures that, when followed, ensure the organization’s compliance to these policies.

Educating Stakeholders

Along with PSIRT policies and procedures, the PSIRT team needs to build workflow and management systems that streamline the execution and completion of the actions required to address product security vulnerabilities. These implementations will make it easier for the organization to adopt product security as part of their normal day to day business activities.

The greatest mistake that can be made when deploying the PSIRT mission, policies and procedures is to have it viewed as a separate responsibility or requirement. Therefore, it is critical to educate all members of the organization on product security basics and the role they play. The entire organization must be included, enabled, and empowered to meet the PSIRT policy requirements.

The Importance of Metrics

It is critical to measure the success of the product security incident response mission. Metrics does not define the requirement, but supports the program, helps determine the required resources, and may help identify places that need process/tool improvements. Creation and tracking of metrics may also help in the maturing of a PSIRT by uncovering issues or bottlenecks with respect to the deployment and adoption of a PSIRT. Service 1.7 Stakeholder Metrics and Service 5.3 Vulnerability Metrics goes into more details on the types of metrics that would be valuable to track.
Definitions

In this document, we are defining the use of certain terms. Note that Service Areas, Services, and Functions identify what is being done at different levels of details, while Tasks and Actions identify how it is being done at different levels of details. Tasks and Actions are being published in an accompanying document and can / will be updated more frequently:

- **Advisory**:^1^ announcement or bulletin that serves to inform, advise, and warn about a vulnerability of a product.

- **Bug Bars**: categories of bugs that will be fixed during particular development phase. Usually includes severity.

- **Coordinator**:^2^ optional participant that can assist vendors and finders in handling and disclosing vulnerability information.

- **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**:^3^ individual or organization that identifies a potential vulnerability in a product or online service. Note, finders can be researchers, reporters, security companies, hackers, users, governments, or coordinators.

- **Function**: a means to fulfill the purpose or task of a specified service. The list of tasks that can be performed as part of the function.

- **Open Source**: works that are freely available to the public, that once shared are collaborated or commented on by numerous individuals. Open source projects are not owned by companies or individuals and often have large bodies of individuals contributing to improve upon the shared ideas.

- **Partners**: Original Equipment Manufacturers (OEM)s, suppliers, Original Design Manufacturers (ODM)s.

- **Product**:^4^ a system implemented or developed for sale or to be offered for free.

- **Quality Gate**: set of criteria that must be met before product moves to next phase of development or release.

---

^1^ ISO/IEC 29147:2014 Information technology—Security techniques — Vulnerability disclosure-Terms/Definitions 3.1

^2^ ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.1


- **Remediation (or Remedy)**: Patch, fix, upgrade, configuration, or documentation change to address a vulnerability.

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

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

- **Secure Development Lifecycle (SDL)**: Is a development process that helps developers build more secure products and address security compliance requirements while reducing development cost.

- **Service Area**: Group services related to a common aspect that help to organize the services along a top-level categorization to facilitate understanding.

- **Service**: The set of recognizable, coherent actions towards a specific result on behalf of or for the constituency of an incident response team. The list of functions used to implement the service.

- **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**: Is a person or party with an interest or concern in PSIRT operation or organization. They can affect or be affected by the PSIRTs actions, objectives and policies. PSIRT stakeholders are the "groups without whose support the organization would cease to exist."

- **Third-party**: Any upstream supplier or producer that provides components incorporated into a product or solution/service.

- **Vendor**: Person or organization that developed the product, or service, or is responsible for maintaining it.

- **Vulnerability**: Weakness of software, hardware, or online service that can be exploited.

---

5 ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.4
7 The Project Management Body of Knowledge (PMBOK) Guide and Standards
8 The Project Management Body of Knowledge (PMBOK) Guide and Standards
10 ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes-Terms/Definitions 3.8
This section identifies and describes the foundation of core components that an organization needs to plan, establish, and effectively operate a PSIRT.

**Purpose:** Enable an organization to plan and implement the foundational components for establishing and operating a PSIRT.

**Outcome:** The identification, planning, and implementation of the PSIRT operational foundation components help an organization establish its PSIRT which will prepare the PSIRT to carry out its mission and sustain the company’s ability to provide its products and services to its defined stakeholders.

---

### I. Executive sponsorship

Obtain sponsorship from the organization’s executives and key decision makers.

**Purpose:** Inform and obtain the support (buy-in) from the organization’s executives (e.g., C-level officers, board of directors) or other decision makers to enable the PSIRT to
operate effectively.

**Outcome:** On-going funding and support based off desired business metrics.

To obtain executive sponsorship, the organization should inform or educate the executives by providing them with a plan and other supporting information to help them understand the purpose, importance, potential risks of security vulnerabilities and benefits of operating a PSIRT. (See “PSIRT Charter” and “Budget’ below.)

See Service 1.1 Internal Stakeholder Management for related information.

II. Stakeholders

Identify stakeholders and the relationship your PSIRT will have with these groups.

**Purpose:** Understand who the PSIRT will serve and with whom the PSIRT will interact.

**Outcome:** Clearly defined list of interested parties.

This should include external stakeholders, such as the organization’s customers, external security researchers, CSIRTs, and other PSIRTs, as well as internal stakeholders, such as software developers, engineers, customer support, legal, and public/corporate/media relations.

See Service Area 1 Stakeholder Ecosystem Management for (Service 1.1 Internal Stakeholder Management, Service 1.2 Research Community Engagement, Service 1.3 Community and Organizational Engagement, and Service 1.4 Downstream (Consumer) Stakeholder Management) for related information.

III. PSIRT Charter

Develop a charter or other document (e.g., strategic plan, implementation plan, or concept of operations document).

**Purpose:** Identify, describe, and document the basic program elements under which the PSIRT will operate.

**Outcome:** A document that describes why the PSIRT was created/funded and desired outcomes from the PSIRT.

The PSIRT charter (or plan) should define the following:

- PSIRT mission (should support and align with the organization’s mission).
- Purpose, roles and responsibilities.
- Products and services (e.g., receive vulnerability reports, develop fixes or patches, distribute patch announcements).

IV. Organizational model

Determine and document the organizational structure and model that the PSIRT will use.
**Purpose:** Identify, describe, and document the organizational model under which the PSIRT will operate.

**Outcome:** Establish a well-defined team structure with documented roles and responsibilities.

The documented organizational model should describe the PSIRT's internal reporting structure and identify the authority under which the PSIRT operates. See “PSIRT Organizational Structure” in the Introduction for descriptions of some common organizational models (e.g., distributed model, centralized model, hybrid model). See Service 1.5 Incident Communications (e.g., the PSIRT reports directly to the Chief Information Security Officer [CISO]).

**V. Management and Stakeholder Support**

Obtain support “buy-in” from organizational management and internal stakeholders.

**Purpose:** Inform and obtain the support buy-in from other internal management and stakeholders to enable the PSIRT to operate effectively.

**Outcome:** Stakeholders are apprised of key business metrics to ensure ongoing support.

See Service 1.1 Internal Stakeholder Management for related information.

**VI. Budget**

Identify the costs of resources required to operate the PSIRT, and obtain the appropriate funding to finance these resources.

**Purpose:** Identify, describe, and document the organizational model under which the PSIRT will operate and be funded.

**Outcome:** Documented PSIRT operational costs, expenses, and funding model.

The budget should include expenses for staffing the PSIRT (salaries, benefits, plus other encumbered costs), equipment and other capital expenses (e.g., information technology systems/devices, software licenses), and training budget (including travel expenses).

**VII. Staff**

Identify the staffing resources needed to provide your PSIRT services, and obtain a skilled staff.

**Purpose:** Identify, describe, and document the organizational model under which the PSIRT will be staffed.

**Outcome:** PSIRT staffing resource needs will be documented.

This includes identifying the various staff position or roles and responsibilities for individual members of the PSIRT, as well as the competencies (knowledge, skills, abilities [KSAs]) and any other requirements (e.g., education, experience, certifications).
expected of those roles. Full time employee, vendors, contractors, or a combination of these may fill these positions or roles.

As part of the staffing plan (or as identified in a separate document), training requirements should be identified and planned, including general training for all PSIRT staff and role-based training for individuals (e.g., initial onboarding/mentoring; ongoing training, education, and awareness; specific training for professional development).

See Service 6.1 PSIRT for related information.

VIII. **Resources and Tools**

Identify and acquire other necessary resources and tools.

*Purpose*: Identify and acquire the resources, equipment, and tools needed for the PSIRT to operate.

*Outcome*: The tooling and resource needs for the PSIRT will be documented and understood.

These resources and tools include the following:

- Infrastructure, such as facilities (office space).
- Tools/Technology/Equipment (hardware, software) (e.g., see Service 3.3 Reproduction).
- Vulnerability Reporting System/Methods (e.g., website, email, phone) (see Service 2.1 Intake of Vulnerability Reporting).
- Secure Communications (e.g., PGP/encryption) (see Function 1.5.2 Secure Communications Management).
- Vulnerability Database/Tracking system (e.g., see Function 1.5.3 Security Defect Tracking System Updates and Function 3.2.1 Finder Database).

XI. **Policies and Procedures**

Document the policies, processes, and procedures relevant to conducting PSIRT operations.

*Purpose*: Identify, describe, and document the policies and procedures under which the PSIRT will operate.

*Outcome*: The PSIRT will have formal policies that describe PSIRT authority and the governance/operations they will wield. The PSIRT will also have formally documented procedures/guidelines that describe how to perform duties.

Documenting the policies and procedures will ensure common understanding among all PSIRT staff, enable consistency and repeatability of the products and services provided by the PSIRT, and serve as a training resource for new PSIRT staff.
X. Evaluation and Improvements

Identify metrics for evaluating performance and/or effectiveness to identify improvements.

*Purpose:* Assess or evaluate how well a PSIRT is operating, and to identify potential areas for improvement.

*Outcome:* The PSIRT will be able to measure its performance and understand areas where improvement is desired.

The PSIRT should continuously and/or periodically assess or evaluate how it is performing (providing its products and services) and identifying any potential areas for improvement.

Evaluation metrics and methods can be informal (e.g., collecting feedback from stakeholders) or formal, and can occur as needed (e.g., documenting lessons learned [see Function 1.1.3 Incident Post-Mortem Process]) or on a designated schedule.

The information provided in this PSIRT Framework document can be one source of the criteria or capabilities used to evaluate a PSIRTs operations.
This service area describes the services and functions a PSIRT can fulfill to appropriately engage with both internal and external stakeholders. Execution of services under this umbrella are in effect throughout the lifecycle of an incident or the maturity lifecycle of the PSIRT team. This service area is dedicated to ensuring all stakeholders of the PSIRT are appropriately informed and engaged in the incident response process.

Prior to formally providing these services, the PSIRT must first identify the unique stakeholders that are relevant for their businesses. Stakeholders include such parties as executive or business leadership, internal development teams, external component providers or developers, or even the organization’s customer-base. It can be extremely useful to compile a matrix of stakeholders-to-products/versions to streamline the communication process. Prior to communicating with these stakeholders, it also would be beneficial to understand the viewpoints or artifacts or methods by which they desire to be engaged by (web portal, personalized email, internet chat, ticketing system, etc.). For the purposes of this document, stakeholders are divided into several groups (your specific business circumstance may identify others): finders, peers/partners, internal teams, and stakeholders of your products.

**Purpose:** Highlight the processes and mechanisms to share information with the assorted stakeholders a PSIRT can and should interact with.

**Outcome:** Successful engagement with the PSIRTs stakeholder ecosystem will ensure timely reports of discovered vulnerabilities as well as satisfied stakeholders/partners when security vulnerabilities must be communicated to the organization’s stakeholders.
Service 1.1 Internal Stakeholder Management

Define processes related to engaging with internal stakeholders to ensure both awareness as well as assistance during incidents. Successful internal stakeholder engagement will improve communication and response efforts by clearly communicating the PSIRTs role within the organization and making internal connections between product teams and security analysts.

**Purpose:** Establish the PSIRTs authority and expertise to internal stakeholders to facilitate the smooth coordination of vulnerability remediation and product security.

**Outcome:** Flaws discovered by internal employees relieve the pressure of external embargoes or media scrutiny, and as such are some of the most impactful ways to improve an offering’s security profile.

**Function 1.1.1 Engage Internal Stakeholders**

Maintaining active dialog with internal teams involved around the development, testing, packaging, and maintenance of the organization’s offerings. Internal stakeholders not only are engineering resources, but also could be testing/quality assurance, release-engineering, stakeholder-facing support teams, sales and marketing, or other technical subject matter experts in the field.

**Purpose:** Build presence on internal messaging/information platforms to notify internal associates about the PSIRTs existence, processes, and functions.

**Outcome:** The PSIRT will have a formally documented list of internal stakeholders and an
understanding of their roles and responsibilities.

Sub-Function 1.1.1.1  Engage with Corporate/Business Leaders and Executives

For a PSIRT to be effective, it must understand and be able to react to the current organizational environment. Working with business leaders and executives helps the PSIRT on several levels. It helps legitimize the PSIRTs work within the organization by virtue of executive sponsorship. It allows the PSIRT to share information with leaders to help inform business decisions. It also allows leadership to express changes in policy and organizational direction that might alter the PSIRTs mission.

Sub-function 1.1.1.2  Engage with Public Relations/Corporate Communications, Legal Departments, and Government Affairs

Engaging with the array of internal Communications and Legal teams will ensure that the PSIRT is compliant with current branding and messaging standards as well as the regulatory/legal environment the organization must be compliant with (e.g., privacy, federal space). Each of these stakeholders offer unique paths to critical stakeholders of the PSIRT, and lines of communication should be established before times of critical events or incidents to ensure all parties can effectively work together.

Purpose: Ensure the PSIRT and any security vulnerability messaging is compliant with brand and legal policies. Working with the specialized communications or governmental/legal groups within the organization helps ensure the PSIRT is delivering brand-approved, or legally/contractually-approved messaging.

Outcome: Any communications coming from the PSIRT will be compliant with relevant corporate standards and policies. Ideally working with PR, Communications, Legal, and other internal groups will help the organization avoid loss of brand reputation, criminal or civil legal issues, or loss of corporate good-will from its stakeholders, regulators, and peers.

Sub-Function 1.1.1.3  Engage with Internal Business Units/Lines of Business

Engaging with development stakeholders ensures issues get appropriately documented, prioritized and addressed. For example, engineers from the PSIRT team or authorized delegates need to coordinate vulnerability remediation with the software engineering groups responsible for the faulty code. In times of incidents, these partnerships also assist in the speedy transmission of information and effective, quick remediation of the issue. Stakeholders here include Program or Product Managers, SDL oversight groups, Project Managers, Product Owners, and others with similar business-related responsibilities.
**Purpose:** PSIRTs should engage with the business to exchange information about the PSIRTs role in the product release process, any governance functions it fulfills, product flaws and vulnerabilities to ensure all parties understand their roles and responsibilities. Making these connections with business personnel will help ensure appropriate prioritization of flaws and adherence to corporate security guidelines. On-going conversations with the business, providing metrics around vulnerabilities and remediation will help them appropriately fund and address issues as they arise.

**Outcome:** The PSIRT will understand how the Lines of Business function, what their goals and objectives are, and how the PSIRT impacts them.

**Sub-Function 1.1.1.4** Engage with Internal Development/ Engineering

Engineers from the PSIRT team need to coordinate vulnerability remediation with the software engineering groups responsible for the faulty code. Engaging with development stakeholders ensures issues get appropriately documented, prioritized, and addressed. In times of Incidents, these partnerships also assist in the speedy transmission of information and effective, quick remediation of the issue.

**Sub-Function 1.1.1.5** Engage with stakeholder-facing support teams

Engineers from the PSIRT team need to provide explanation and artifacts to stakeholder support teams so that as issues develop and become public the support organization can respond to stakeholder inquiries and support requests. “Support” could include front-line (a.k.a. “Help Desk) personnel, premium support resources (e.g., Technical Account Management, Stakeholder Success Managers, etc.), or internal/external Sales teams, In-field resources (consulting, sales engineering, etc.).

**Purpose:** The PSIRT must supply timely information for the organization’s assorted stakeholder-facing support teams can respond to stakeholder demand for support/information/solutions. Failure to appropriately support the teams providing direct stakeholder support could negatively impact the brand, lose stakeholder faith and risk future revenue. These “front-line” associates must also be able to feed data and questions from/on-behalf of the organization’s stakeholders and partners.

**Outcome:** The PSIRT will be able to collect information around customer satisfaction of vulnerability remediations as well as respond to customer requests as needed.

**Sub-Function 1.1.1.6** Internal working group participation

In more mature organizations, engineers from the PSIRT team can build and strengthen relationships with internal stakeholders by participating in various internal initiatives or working groups. This helps to reaffirm/establish the technical expertise of the PSIRT, and build networking/communication channels for future efforts.
**Purpose:** PSIRT members should be seen as active participants within the organization. Sitting in on working groups or other internal initiatives establishes the role and expertise of the PSIRT and raises awareness of how to engage the team.

**Outcome:** Participating in these efforts establishes credibility of the PSIRT and builds internal communication channels that can be leveraged during incidents.

**Function 1.1.2 Internal Secure Development Lifecycle**

Maintaining and enforcing a Secure Development Lifecycle is a cornerstone of establishing stakeholder confidence and trust in an organization's products. Without being able to demonstrate repeatable application of security standards through a product’s lifecycle, stakeholders may lose faith in the organization’s products, harsher requirements on the organization may be imposed (burden of proof, right to audit, etc.), and ultimately could lead to loss of revenue and stakeholder confidence.

**Purpose:** Organizations that follow good Secure Development Lifecycle practices will spend less on remediating security flaws in their product set by catching these flaws earlier in the development or augmentation of products. All participants in this lifecycle will clearly know expectations around security features, functionality, and requirements of offerings, and will understand their roles and responsibilities within the lifecycle.

**Outcome:** The PSIRT will have clear product release information and be able to provide metrics and data around delivery performance. In mature organizations, the PSIRT can provide data around common weaknesses of historic products to avoid making similar errors with future efforts.

**Sub-Function 1.1.2.1** Participate in SDL creation and maintenance

SDL is a critical governance process that helps an organization produce stable, repeatable offerings that adhere to common standards. The PSIRTs participation in the creation and maintenance of the organizational SDL helps ensure that appropriate security practices and checks are followed.

**Sub-Function 1.1.2.2** Participate in SDL governance/enforcement

SDL is a critical governance process that helps an organization produce stable, repeatable offerings that adhere to common standards. The PSIRTs participation in the governance and enforcement of the organizational SDL helps ensure that appropriate security practices and checks are followed, and that exceptions are documented and appropriately reviewed.

**Function 1.1.3 Incident Post-mortem process**

As vulnerabilities are discovered within the organization’s offerings, the PSIRT requires a mechanism to review these issues (be they code-related, process-related, or personnel-related) and to provide that feedback to participating stakeholders and organizational
leaders. Some severe or very public security vulnerabilities may require more in-depth analysis about how the company reacted to the issues and corrected it. A post-mortem is a meeting involving all internal stakeholders involved in remediation and communication efforts, and seek to document what went well, what could have been done better, and what changes will be made for future events.

**Purpose:** Provide a clear, factual account of events that occur during vulnerability response, including security incidents to perspectives from all involved parties/teams. In times of critical issues, the PSIRT can assist or lead the organization’s response to remediating these publicly-known, high-impact issues.

**Outcome:** The PSIRT will provide data around the organization performance reacting to software vulnerabilities. This data will be incorporated into the “lessons learned” for future improvement in events.

**Sub-Function 1.1.3.1** Establish a process to review failings in the development process that can lead to security vulnerabilities

Establishing a consistent process to review post-mortem issues helps ensure that products are continuously improved with lessons learned.

**Sub-Function 1.1.3.2** Track process failings and coordinate lessons-learned for routine vulnerability response and periodically review those issues with key stakeholders

The PSIRT needs to document, report on, and ensure that findings from review meetings are appropriately followed-up on. If left unattended or unresolved, chronic issues could lead to a decrease in product quality, increases in future security issues, and an overall decrease in stakeholder confidence.

**Sub-Function 1.1.3.3** Review timing of processes and release of updates

Track areas of strength and weakness.

**Sub-Function 1.1.3.4** Coordinate organization lessons-learned response review for high-profile incidents and provide reporting data to the business and other stakeholders as required.

**Sub-Function 1.1.3.5** Assist in coordination of revisal of internal processes identified in post-mortem process and track remediation progress.
Services related to engaging the research community as a stakeholder. Finders can take the form of academics, development professionals, professional security finders, or hobbyists. Finders have many varied roles and unique perspectives. Some can be academics, researching theoretical attacks or flaws in the hopes of publication and academic achievement, while others are professional security finders that are motivated by financial or corporate means. Still others may be hobbyists or enthusiasts participating in their spare time, perhaps to gain respect and accolades from their communities. Finder community engagement is a proactive approach to Product Security Incident Response.

**Purpose:** Position an organization’s PSIRT as an active contributor to the research community, and to build situational awareness of threats that may affect an organization’s product security. Negative or antagonistic relations with finders could lead to loss of early notification of research that could put the organization at a disadvantage in reacting to security vulnerabilities, and thereby impact stakeholder-sentiment towards the organization.

**Outcome:** Successful community engagement will strengthen an organization’s reputation and market position in championing product security. Additionally, positive engagement with finders can lead to early access to research and/or security vulnerability disclosures to help the organization prepare their reaction for eventual public release.
Function 1.2.1 Engage Finders

Activities designed to maintain active dialogue with finders that have expertise in the security of a company’s products and access to different channels.

Purpose: Build presence on social media sites such as Twitter. Monitor Twitter and other common sites/forums for indicators that finders or stakeholders may have found an issue. Consider regular attendance at security conferences where face to face meetings with finders can occur.

Outcome: The PSIRT will receive better quality reports with more advanced warning with highly-engaged finders.

Sub-Function 1.2.1.1 Invite qualified finders to private contracts

Some organizations find value in deepening the relationship with particular security finders. If it is valuable to your organization, qualified finders can be engaged in private contracts.

Sub-Function 1.2.1.2 Engage with security finders at conferences and other events

Some organizations find value by engaging face to face with particular security finders. It helps to build trust between your organization and the finders.

Purpose: Finder attend security conferences and other events to discuss their findings, learn and network with others. Meeting them face to face gives opportunity to build mutual trust.

Outcome: A positive engagement with finders may establish/improve relationships with the finders. Finders may be more likely to report issues when they find them as a result of this engagement.

Sub-Function 1.2.1.3 Sponsor academic research in security flaws and topics

Some organizations find value by sponsoring academic research. If it is valuable to your organization, research which academic conferences pertain to your product or services.

Purpose: Academic conferences provide organizations with the opportunity to identify new areas of research and potential vulnerabilities. By sponsoring, organizations may be given early access to research papers and then can address the issue before the issue is presented to the public.

Outcome: Supporting academic research provides another avenue of finder submissions. It may allow the organization to direct/suggest areas for research. It
may also provide a pipeline of potential employees down the road.

Service 1.3 Community and Organizational Engagement

Sometimes referred to as “upstream” and “downstream”, community participation is essential to nurture joint remediation efforts or assist in mutual-aid with others within the organization’s peer groups. “Upstream” is a term used for groups or individuals from which you source components or projects for your organization’s products. “Downstream” refers to individuals, groups, or organizations that source your output as parts of their offerings. Downstream engagement is covered in Service 1.4 below.

A vibrant upstream community can help feed innovation into product streams as well as assist with the burden of complex vulnerability remediations, oftentimes filling in for the lack of crucial subject matter expertise that may be deficient within the organization. Likewise, cultivating professional relationships with individuals and teams from other organization can help virtually expand the capabilities of the PSIRT by allowing access to external perspectives, expertise, and historical knowledge. This can be achieved through proactively engaging the security community as a stakeholder, establishing relationships with partners and peer PSIRTs.

**Purpose:** The PSIRT needs to build and maintain an active ecosystem of partners and peers. These community associations can assist in a “many eyes” approach to finding and remediating flaws, as well as sharing good practices between different groups to improve the overall experience in vulnerability remediation.

**Outcome:** Good relationships and an active ecosystem of partners and peers will facilitate information sharing on threat intelligence and best-practices. A PSIRT with good reputation in the security community may help to draw resources and collaboration to address critical situations.

Function 1.3.1 Define & Engage with Upstream Communities & Partners

Oftentimes products will include code or components that were not created by the organization. The originators of these materials are sometimes called third-parties, suppliers, or upstream vendors, OEMs or simply partners. It is helpful to identify these partners within your ecosystem and determine how the organization would contact and engage them when vulnerabilities are discovered in the third-party’s code.

**Purpose:** Establish cordial working relationships with those individuals or groups from which you receive components or those groups that receive components from your organization. Understand who and how to contact these groups will keep the PSIRT informed of looming issues, as well as having an understanding of whom the PSIRT needs to inform as they discover affected components others derive from them.

**Outcome:** The PSIRT will better understand by who and from where components are sourced from. This should provide faster access to information and fixes when those components are discovered to have flaws.

Sub-Function 1.3.1.1 Document and define upstream communities and partners
Upstream communities and partners provide code, and/or, knowledge and expertise that is incorporated into the organization’s offerings. It is critical to know and engage with these suppliers to ensure speedy and effective interactions as security vulnerabilities are reported to and worked on with the PSIRT. Ideally these relationships are documented in contracts, covered by non-disclosure agreements and other protections for the organization.

Sub-Function 1.3.1.2 Find channels to engage these communities and partners in active dialogue

Each upstream community or partner may have different methods or tools they use to develop and communicate about their software/offers. The PSIRT should understand how to engage with these external groups, and ensure that the PSIRT has appropriate contacts/methods to collaborate on security issues involving those external parties.

Sub-Function 1.3.1.3 Actively provide expertise to these communities through project participation, making resources available to these projects, and acting as mentors to upstream developers and groups

Participation with upstream communities and partners helps build valuable trust between the groups, as well as helping augment the capabilities of that external team with expertise the organization may have.

Sub-Function 1.3.1.4 Participate in community events, such as conferences, to directly work with participants

Conferences and professional organizational meetings are excellent places for PSIRTs to interact with stakeholders and partners, getting direct feedback for the organization as well as building goodwill and a positive reputation amongst the external community that can be leveraged for future coordination/collaboration.

Sub-Function 1.3.1.5 Engage with community security teams and/or security leads on projects

It is critical that the PSIRT understands who and how to contact upstream software/hardware/service providers’ security teams (PSIRT, CSIRT, security engineers). Establishing lines of communication and rapport between the PSIRT and these groups helps ensure smooth interactions during times of crisis or vulnerability remediation.

Function 1.3.2 Engage with Peer PSIRTs

Nurturing relationships between peer PSIRT teams can help in information-sharing and potential mutual-assistance and/or coordination for incidents. Working with these peer
organizations can help fill in vital data to remediate vulnerabilities and virtually includes peer’s expertise to the organization as the two groups consult on issues.

**Purpose:** Provide communication channels between your organization and other PSIRT teams to share vulnerability information, threat intelligence, and best practices.

**Outcome:** A community of peer PSIRT is valuable to respond to vulnerabilities related to the software supply-chain. A faster response rate can be expected.

**Sub-Function 1.3.2.1** Document and define Peer PSIRTS

Collect contact information and engagement processes for future use. The PSIRT should engage and interact with the larger PSIRT community to share best practices and insights around lessons learned. As vulnerabilities arise, they are often solved in a collaborative, multi-group manner, and allows the PSIRT to extend its internal capabilities by leveraging these external peers for information and/or assistance.

**Sub-Function 1.3.2.2** Define Responsible Disclosure parameters between organizations

PSIRTS should carefully document vulnerability information sharing parameters and agreements. The PSIRT should honor embargo parameters set out by the vulnerability finder and/or reporting organization (and expect to have theirs honored).

**Sub-Function 1.3.2.3** Establish secure information-sharing channels to facilitate data-sharing around security vulnerabilities

The PSIRT should establish methods to securely share vulnerability and other confidential information with parties involved in the responsible disclosure arrangement. This could be such options as out-of-band, non-electronic communication, encrypted email/portals or private mailing lists.

**Sub-Function 1.3.2.4** Participate in Industry SIGs and/or functions

Working with peers on topics of interest for the industry supports and nurtures contacts as well as further the professionalization of the profession by collaboratively solving problems.

**Purpose:** Participation in the PSIRT community helps open lines of communication, allows for future collaboration on issues, and provides a sounding board to gauge services and processes. Participation in Industry SIGs also help further professionalize and mature the discipline.

**Outcome:** The PSIRT will have contacts within the PSIRT community and share good practices for the betterment of the Industry.
Function 1.3.3 Engage with Coordinators (CERTs, CSIRTs, or other coordination center organizations)

Working with government CERTs and CSIRT helps build trust to share information, and helps the PSIRT earn the trust and respect of valued peers. Other organizations with relevant interests or communities include FIRST, MITRE, Advancing Open Standards for the Information Society (OASIS), the Industry Consortium for Advancement of Security on the Internet (ICASI), ISO, amongst others. Groups that participate could be viewed based off of national, enterprise, regional or industrial sectors.

**Purpose:** Organizations are frequent targets for threat actors who often use previously unknown vulnerabilities to penetrate networks. Building relationships with CERTs and CSIRTs enables the trust and contacts needed to get potential vulnerability reports at early stages.

**Outcome:** Good relationships with CERTs, CSIRTs, and other coordination center organizations are valuable to become aware of vulnerabilities early-on. A faster response rate can be expected.

**Sub-Function 1.3.3.1** Find channels to engage these communities and partners in active dialogue

The PSIRT should research where the desired external groups engage in dialog and make efforts to participate in those forums.

Function 1.3.4 Engage with security vendors

Large commercial security vendors work with stakeholders during breaches and oftentimes will have forensic data that the PSIRT may not normally have access to. Developing relationships with these vendors helps build trust and mutual respect and ideally can help the PSIRT gain access to critical threat data that may otherwise not be available to them.

**Purpose:** Build a formalized partner program with security vendors who discover vulnerabilities being used (or could be used) in active attacks. At a minimum, a non-disclosure agreement between partners should be signed while a more thorough legal agreement is recommended.

**Outcome:** Security vendors will help monitor vulnerabilities or exploits that could otherwise go undetected underground. Security vendors can present a good opportunity to collaborate and improve product security.

**Sub-Function 1.3.4.1** Document and define Bug-Bounty Vendors in scope for the offerings the organization provides

Knowing and properly engaging with security vendors can speed communications
and efforts around vulnerability reporting/remediation as they report issues to the PSIRT. It is important to understand what these vendors will have access to and keep. The organization’s relationship to the bug bounty vendor should be thoroughly documented and vetted prior to entering into a relationship so all parties understand how they act, what they access, and how data is shared and with whom.

**Sub-Function 1.3.4.2** Find channels to engage these Security Vendors in dialogue

The PSIRT should research where the desired external groups engage in dialog and make efforts to participate in those forums.

**Function 1.3.5** Engage with Bug-Bounty Vendors

Building a relationship with Bug Bounty vendors to help further communication and data-sharing efforts around vulnerability management.

*Purpose:* If your organization receives frequent vulnerability reports from vendors/brokers who pay finders for bugs, consider maintaining a direct relationship with those organizations who often establish SLAs for vulnerabilities to be addressed.

*Outcome:* A direct relationship with bug-bounty vendors can help to start a constructive dialog to explain the process to releasing a product security patch. Alongside with establishing agreeable SLAs, such relationship will help to reduce the risk of zero-day vulnerabilities to the mutual benefit of all stakeholders.

**Sub-Function 1.3.5.1** Document and define bug-bounty vendors applicable to the offerings the organization provides.

**Sub-Function 1.3.5.2** Identify channels to engage these bug-bounty vendors in active dialogue.

**Service 1.4 Downstream Stakeholder Management**

Services related to engaging your stakeholder-base as a stakeholder. Establishing processes and methods to interact with the stakeholder community around product security response.

Stakeholders of the organization’s products are some of the most important to keep happy, as they represent current and future revenue opportunities for the organization. Stakeholders put the products and services of the organization to daily use, and oftentimes will find routine bugs and security flaws through normal usage. Reacting to these findings helps establish and reinforce the credibility of the organization and can help generate good-will towards the brand.

*Purpose:* PSIRT needs to build and maintain channels with the organization’s stakeholder base to convey information about product security vulnerabilities or during Incident
**Outcome:** Good relationships with your constituency will not only confirm (or in some cases increase) revenue, but will also provide stakeholders with a voice into your product, encouraging a sense of involvement and participation in the solution.

**Function 1.4.1 Engage with Downstream Stakeholders**

Stakeholders of your products and services should have avenues to share information, opinions, and get support around how the organization handles security vulnerabilities. Proactively working with the organization's stakeholders helps provide a positive brand-experience and sustain/improve stakeholder-loyalty.

**Purpose:** Provide methods for the organization's downstream stakeholders to communicate with the PSIRT, and receive support for security issues. Not reacting appropriately to stakeholder inquiries or demands could negatively impact the brand through negative public comments, loss of renewals or loss of new business.

**Outcome:** Downstream stakeholders should receive quick and clear guidance around security flaws. This will build levels of trust for the product and helps increase brand-loyalty. Create a positive-overall experience with the help of PSIRT and establish PSIRT expertise with stakeholders. Generally, improve the stakeholder’s view of the whole brand.

**Sub-Function 1.4.1.1 Provide clear lifecycle and support policies**

The organization should clearly and publicly describe what the stakeholder’s expectations are around the fixing of security vulnerabilities and for how long products are supported. Refer to Service Area 4 for more information.

**Sub-Function 1.4.1.2 Stakeholder Engagement**

Stakeholders of the organization's products and services will have questions, require assistance, or need remediation of reported security flaws. The PSIRT should actively engage with stakeholder requests, provide clear and accurate guidance around security vulnerabilities, and provide risk mitigations until such time security fixes can be provided to the stakeholder.

**Service 1.5 Incident Communications Coordination within the Organization**

A security incident touches on many internal groups and, possibly including products, within the organization. PSIRTs are a central point to coordinate vulnerability remediation efforts as well as serving as a hub for sharing information about an event to authorized internal stakeholders.

**Purpose:** Ensure that all parties within a business have information about the status of a security vulnerability response so they can make educated decisions about the next steps to take. Communication can take many forms (email, traditional mail, RSS feeds, social
media, etc.) but ultimately all outlets provide clear, timely, accurate information around security vulnerabilities and security incidents of concern for stakeholders.

**Outcome:** Internal stakeholders will be apprised of the scope and impact of threats to the organization’s offerings. Stakeholders should be informed so they can take the appropriate next steps as the security vulnerability is remediated, and as mitigations are made available.

**Function 1.5.1 Provide Communication Channels/Outlets**

To engage effectively with stakeholders, the PSIRT must provide an assortment of communication channels. Different stakeholders may prefer certain outlets over others. The PSIRT should account for the widest possible audience as communications are crafted and released. The PSIRT also should be equipped to intake security reports, comments, and questions from a variety of sources.

**Purpose:** Provide methods to stakeholders to allow communication with the PSIRT.

**Outcome:** These channels, whether they be email, chat, web form, etc. allow internal stakeholders to communicate and share information with the PSIRT.

**Sub-Function 1.5.1.1 Provide clear channels on how to communicate vulnerability reports to the PSIRT**

Stakeholders should have avenues to submit questions, check the status of flaws, and report issues to the PSIRT. If a stakeholder is impacted by or discovers a security vulnerability, they should easily be able to make and send a report to the PSIRT.

**Sub-Function 1.5.1.1.2 Provide internal communication channels**

To engage internal stakeholders, the PSIRT should provide communications channels to advertise the remediation status of vulnerabilities. Internal stakeholders should be able to easily contact the PSIRT and understand what to expect from inquiries.

**Sub-Function 1.5.1.1.3 Provide external communication channels**

To engage external stakeholders, the PSIRT should provide communications channels to advertise the remediation status of vulnerabilities. This would include vetting/qualifying activities around external communication to ensure their validity and that they get appropriately routed to internal associates.

**Function 1.5.2 Secure Communications Management**

Oftentimes the PSIRT must handle information that is considered confidential (i.e., issues that are under embargo). The PSIRT needs to be able to securely and privately communicate with finders, other organizations, or with assorted internal resources.
Abiding by the disclosure agreements and only communicating via private methods helps build confidence from finders. Protecting the confidential vulnerability information from unauthorized parties also helps ensure the issue can be appropriately and effectively managed, per the terms of the embargo. Secure channels also can help protect the identity of finders that do not wish to be revealed. A retention policy should be established to ensure data is properly disposed of after its use has ended.

**Purpose:** Provide facilities for parties to privately exchange information around security vulnerabilities. These channels provide protection of the confidentiality of the security vulnerability and that of the finder until such time they can be publicly disclosed.

**Outcome:** Parties involved in supporting security issues can share information privately with others that have need-to-know around an issue. Finders are more likely to come back to the organization with future reports if they feel their concerns are protected by the organization.

**Sub-Function 1.5.2.1** Provide secure communications channels

The PSIRT should ensure that vulnerability finders and partners working on vulnerabilities impacting the organization’s offerings have private and secure methods to share information.

**Sub-Function 1.5.2.2** Provide secure file transfer capabilities

The PSIRT should ensure that vulnerability finders and partners working on vulnerabilities impacting the organization’s offerings have private and secure methods to share information.

**Function 1.5.3** Security Defect Tracking System Updates

The PSIRT should have access to a system of record for all product defects and be able to create and use a system for the tracking and information-sharing around security vulnerabilities. Persons with a need-to-know should be able to access and update these vulnerabilities.

**Purpose:** Proper recording and tracking of security defects allows the organization to say when and where vulnerabilities were addressed. This defect system also allows communication between the PSIRT, finders, and engineers actively working on solving the problem.

**Outcome:** With security vulnerabilities appropriately tracked using a system, all parties that require access to information around a flaw can review history, progress, and comments about it.

**Sub-Function 1.5.3.1** Provide security defect tracking for vulnerability finders
All security defects should be tracked. Systems should be accessible (within least
privilege model) with internal and external parties to update and track progress.
External finders should receive adequate communication around the status of the
reports they have filed with the PSIRT.

**Sub-Function 1.5.3.2** Provide process to intake, triage, route, and prioritize
security vulnerabilities in defect tracking system

The PSIRT should ensure that vulnerability finders and partners working on
vulnerabilities impacting the organization’s offerings have private and secure
methods to share information.

**Function 1.5.4** Information Sharing and Publishing

After an issue has been addressed, the PSIRT should share it with all impacted
stakeholders. All impacted stakeholders should understand what the security
vulnerability is, what its severity and impact are, what possible risks could be exploited,
and how to resolve the issue or mitigate it until such a time that fixes can be made
available.

**Purpose:** Share details about security vulnerabilities that have been reported and
remediated. Stakeholders should be able to receive treatment or alternative mitigations
to contain the risk until formal fixes can be provided.

**Outcome:** Stakeholders will be informed about security issues, how they could be
affected by them, and how they were remediated. Stakeholders that receive timely
information and updates are more likely to view the organization positively and either
continue with the offerings they have or expand future usage of the organization.

**Sub-Function 1.5.4.1** Provide multiple methods of communication for
advertisement of vulnerability remediation

Different stakeholders will prefer different methods of interaction/communication
as vulnerabilities are disclosed to the public. The PSIRT should ensure that in
addition to traditional advisory-style updates, that other methods are used to
ensure maximum engagement and awareness from stakeholders around the
vulnerability. After vulnerabilities have been remediated, the PSIRT should use
multiple different methods to advertise the fix, and how to acquire it.

**Sub-Function 1.5.4.2** Provide methods for stakeholders to provide feedback on
communications, process, and performance around vulnerability remediation

Feedback helps improve processes and response in the future. It can highlight areas
the PSIRT is strong at, and should continue performing in areas where the PSIRT
needs to develop and improve further.
Service 1.6 Reward Finders with Recognition & Acknowledgement

When security vulnerabilities are discovered it is expected to cite where they came from. Acknowledging the finder helps establish their credibility within the community in addition to expressing appreciation for partnering with the PSIRT on the flaw.

**Purpose:** Finders are acknowledged for their effort to disclose product vulnerability responsibly. Finders can build up their reputation via these acknowledgements to construct an expertise portfolio and show value to the organization.

**Outcome:** A positive collaboration with finders will improve product security. Finder acknowledgement is beneficial to internal employees to build up their reputation and show off their expertise.

**Function 1.6.1 Provide Acknowledgements**

Acknowledgement of the person(s) responsible for discovering a security vulnerability is a vital element within the security vulnerability workflow. The small expression of gratitude builds trust and respect within the community, and shows that the organization is responsive to security concerns.

**Purpose:** Finders are acknowledged for their effort to disclose product vulnerability responsibly. Finders can build up their reputation via these acknowledgements to construct an expertise portfolio.

**Outcome:** A positive collaboration with finders will improve product security. Finder acknowledgement is beneficial to finders to build up their reputation and encourages the finder to send future vulnerability reports to the PSIRT.

**Sub-Function 1.6.1.1 Provide acknowledgements for security vulnerability finders in defect tracking systems/release notes**

Written acknowledgement of a finder’s efforts and involvement in the discovery of a security vulnerability is the single most effective and inexpensive tool the PSIRT has to reward these individuals. It is traditional to include acknowledgement of the finder(s) in security advisories and software release notes. The PSIRT will need to understand how internal attribution of found vulnerabilities will be communicated.

**Sub-Function 1.6.1.2 Provide acknowledgements for security vulnerability finders in public security advisories and on web properties**

Written acknowledgement of a finder’s efforts and involvement in the discovery of a security vulnerability is the single most effective and inexpensive tool the PSIRT has to reward these individuals. It is traditional to include acknowledgement of the finder(s) in security advisories and software release notes and CVE text.
Function 1.6.2  Reward Finders

To generate good-will and to encourage further sharing of research, the PSIRT can elect to develop a program to reward or incent this good-behavior in the hopes that it will continue and expand in the future.

**Purpose:** Reward person(s) who report security flaws in the organization’s products and services. Rewards can take many forms from electronic/physical thank you notes, to organizational swag, to monetary gifts, or other merchandise/enticements. The PSIRT needs to provide transparency around the rewards given and the rules for such awards.

**Outcome:** This practice is designed to generate good-will toward the PSIRTs organization and encourage future continued collaboration around security issues.

**Sub-Function 1.6.2.1  Start a rewards program for vulnerability finders**

The PSIRT can sponsor a rewards program designed to encourage positive behavior in security finders. Rewards could be monetary, corporate swag, or any number of things a security finder might value above their acknowledgement in discovering the issue.

**Purpose:** Reward positive behavior in security finders and show that the organization cares about solving security vulnerabilities.

**Outcome:** Finders will responsibly disclose vulnerability information as opposed to publicly first.

**Sub-Function 1.6.2.2  Start a monetary bug bounty**

One form of a reward can be monetary compensation. Some organizations will pay finders that disclose vulnerability information to them.

**Purpose:** A monetary bug bounty provides direct monetary compensation to finders for their effort to research and report vulnerabilities.

**Outcome:** Finders are compensated via monetary instruments for their effort.

**Sub-Function 1.6.2.3  Start a ‘Points Board’**

Another form of compensation is a “Points Board”. This gamifies finding and reporting security vulnerabilities, and encourages friendly competition by promoting “leaders” and providing rankings for finders to brag over.

Service 1.7 Stakeholder Metrics

Providing details around PSIRT volume, performance, or other measurements is critical in keeping stakeholders aware of the effectiveness of the PSIRT. Different stakeholders will have unique viewpoints that must be addressed with potentially differently formatted artifacts (or views). The PSIRT must understand how each stakeholder group desires to consume this
information. These metrics could be Key Performance Indicators (KPIs) for the PSIRT. **Function 2.5.1** speaks to Operational Reporting the PSIRT should consider providing to ensure smooth operations. **Function 2.5.2** reviews Business Reporting that the PSIRT can consider providing to stakeholders.

**Purpose:** Provide data around PSIRT measurement and performance. This helps stakeholders understand how effective the PSIRT is in providing a given area or service.

**Outcome:** By reviewing the PSIRT's metrics, stakeholders should know how effectively a PSIRT is providing a service and be able to provide feedback to make adjustments to that service delivery.

### Function 1.7.1 Understand Stakeholder Artifact Requirements

The first step to effectively articulating how a PSIRT is delivering services is to understand the unique viewpoints of each stakeholder group. Some stakeholders may be concerned about timeliness of security patches, while others may be focused on financial dimensions of the PSIRTs operation. Each viewpoint is valid, and requires different artifacts to effectively communicate the desired information. Each stakeholder group should be polled to understand what aspects of the PSIRT they require data on, and the best method to share that information.

**Purpose:** Understand what a stakeholder cares about in regard to the PSIRT's operation and services. Once these requirements are gathered and agreed upon, a delivery method/medium and cadence of updates needs to be selected.

**Outcome:** A documented list of stakeholder artifact (report/view/dashboard) requirements will be created for upkeep.

#### Sub-Function 1.7.1.1 Gather Internal Stakeholder requirements for metrics and deliverables

Internal stakeholders will be concerned with a specific set of data that other stakeholders may not be. For example, such metrics could be around performance of the extended patch remediation team, costs, and quality.

#### Sub-Function 1.7.1.2 Gather External Stakeholder requirements for metrics and deliverables

External stakeholders will be concerned with a specific set of data that other stakeholders may not be. Such metrics could be around time-to-deliver-from-public-notice, reissuance of patches (bad patches), or others as examples.

### Function 1.7.2 Collect Stakeholder Metrics

The processes and actions required to document the requested metrics for all
stakeholder groups. Wherever possible, the tooling the PSIRT uses should be able to collect and provide information about the PSIRTs processes and performance. Ideally metrics should be stored in a centralized location (a database, spreadsheet, or other tool) so that historic performance can be periodically reviewed, and so that the differing stakeholder views can be easily addressed with minimal additional labor.

**Purpose:** Gather, generate, aggregate, and/or collect the data points necessary to satisfy stakeholder requirements around dimension of PSIRT performance. This information should be centrally stored for historical review and stakeholder reuse (i.e., two or more stakeholder groups desire the same information).

**Outcome:** Desired stakeholder metrics will be collected for the creation of artifacts (reports, view, dashboards, etc.).

**Sub-Function 1.7.2.1** Gather stakeholder metrics

The PSIRT should create processes and methods to collect the required metrics at the prescribed intervals (SLAs/OLAs).

**Sub-Function 1.7.2.2** Store stakeholder metrics

The PSIRT will need to conduct historical analysis on performance and other trends, so it is useful to develop a repository for this data so that it can continue to be leveraged in the future.

**Function 1.7.3** Analyze Stakeholder Metrics

Data without context is meaningless. Incorrect assumptions can be inferred and services may not be adjusted to meet changing business or stakeholder demands. Once the PSIRT has collected the required data, effort must be spent in reviewing that data and providing necessary context around what that data means to the stakeholder.

**Purpose:** Understand the meaning of the data collected and provide context to the stakeholder about what to do with the information. Ideally the stakeholder should be able to understand how a given Key Performance Indicator (KPI) is performing, what factors influenced it during the reporting period, and be able to see trends in that KPI.

**Outcome:** Historic data will be kept and compared to current performance to identify trends.

**Sub-Function 1.7.3.1** Analyze and review metric data

Data without context is less useful. The PSIRT should spend time and effort to review collected data and provide context along with the metric reporting.

**Sub-Function 1.7.3.2** Analyze data trends and historic performance
As historic data is gathered, unique trends or chronic issues may be identified that the PSIRT or its partners can address.

**Sub-Function 1.7.3.3** Provide context to data so that Stakeholders can appropriately understand what will be provided to them and provide a way to address questions or concerns.

**Function 1.7.4** Provide Stakeholder Metric Artifacts

After metrics data has been collected and analyzed it must be delivered to stakeholders in an agreed-upon format. This format can be referred to as an artifact, or as a view to address a stakeholder viewpoint. These artifacts could take the form of a web page, an email, a more formalized report, or other method.

**Purpose:** Stakeholders should be given metrics data in a format they can digest to provide insights and understanding on the PSIRT performance in delivering services. This data should be understandable, and have sufficient context to help the stakeholder make decisions based off of that performance.

**Outcome:** Metrics will be provided to stakeholders in the appropriate format at the agreed upon timeframes.

**Sub-Function 1.7.4.1** Provide stakeholders artifacts describing required metrics

Each stakeholder has a unique viewpoint they represent. Each viewpoint needs to be addressed with a view of the data in the form of some reporting artifact. These artifacts may need to be adjusted to match differing viewpoints. Artifacts could include reports emailed or posted to a web page, dynamic web portal, executive briefs, charts, graphs, or any number of other data delivery mechanisms.

**Sub-Function 1.7.4.2** Review metrics data and improve processes or service offerings as needed

One of the PSIRTs strongest goals should be to constantly improve the process of vulnerability management. Reviewing performance metrics and stakeholder feedback helps the PSIRT identify areas to focus on or improve.
This service area describes the services and functions a PSIRT may perform to discover potential vulnerabilities. Operation of this service area will trigger the vulnerability handling process described in other sections of this document. Maturity of a PSIRT may be measured via the availability and efficiency of the difference services prescribed in this service area.

**Purpose:** Establish processes and mechanisms to collect intelligence related to product vulnerabilities, vulnerable third-party components or architectural weaknesses from various sources.

**Outcome:** Increase situational awareness for reports and potential vulnerabilities that require action by the stakeholders.

### Service 2.1 Intake of Vulnerability Reporting

For a PSIRT the main scenario is the intake of reports affecting a stakeholder’s product. A key element for the intake of vulnerability reports is to set-up and maintain the required infrastructure, define and advertise contact points, and define and maintain readiness.

**Purpose:** Establish processes and mechanisms that will allow an entity to easily report a vulnerability in a stakeholder’s product, and maintain readiness of the PSIRT in case of a vulnerability report.

**Outcome:** PSIRT readiness for and professional intake of vulnerability reports.

#### Function 2.1.1 Ensure Reachability

PSIRTs must create awareness of their existence, and be available to external parties or internal escalation paths. A clear and defined communication channel may help finders, partners, or stakeholders report a vulnerability to PSIRTs.

**Purpose:** Allow an entity interested in reporting a vulnerability to easily find the required contact information and preferred way of submission.

**Outcome:** Obtain higher number of reports and preclude any claims that the PSIRT was unavailable to accept the submission of vulnerability information.

**Sub-Function 2.1.1.1** Define preferred way and form of report submission
Expect to receive vulnerabilities through various channels and of variable quality. It is still helpful to define the best way to process a report. This can be a web form, a public ticketing system, an e-mail address, a support hotline, or any other means of submission.

**Sub-Function 2.1.1.2** Publish contact details

The preferred contact information for the PSIRT should appear in product documentation, advertised on the company’s web page, indexed in search engines, registered in major CSIRT/PSIRT lists, and communicated to Common Vulnerability Enumeration (CVE) issuing entities such as CVE Numbering Authorities (CNA) and announced in security communities.

**Sub-Function 2.1.1.3** Register common points of contact

It is helpful to reserve common terms related to PSIRT such as ‘psirt@’, ‘incidents@’ or ‘security@’ within your company’s domain name. Such reservation will help to direct relevant PSIRT communication to you.

**Sub-Function 2.1.1.4** Connect the PSIRT within the company

Ascertain that stakeholder service (for stakeholder request or vulnerability reports), the communications department (for media requests), as well as your product development teams (for escalating critical internal findings) are aware of the PSIRT and know how to contact it.

**Sub-Function 2.1.1.5** Define and maintain readiness

Depending on the industry and the requirements set forth by the stakeholders, establish on-call or follow the sun duty to maintain the necessary readiness to respond to critical reports.

**Sub-Function 2.1.1.6** Prepare for encrypted submissions

Vulnerability reports often contain sensitive information about the operational environment and products the vulnerability was observed in. To avoid accidental information leakage or disclosure, promote means to submit reports in an encrypted manner, such as S/MIME or PGP protected e-mails or an HTTPS enabled web form.

**Function 2.1.2 Handle Vulnerability Reports**

Vulnerability reports are received from diverse sources and in various forms. Regular monitoring of incoming communication channels and timely response to incoming reports is crucial. Response times to external finders should be defined in a Service Level Agreement (SLA), internal to the company.

**Purpose:** Provide processes and mechanisms to receive vulnerability reports from other parts of the vendor company, stakeholders, and third parties (finders, other PSIRTs, CSIRTs, etc.).
Outcome: Professional handling of vulnerability reports from third parties.

Sub-Function 2.1.2.1  Monitor communication channels

Check the advertised means of contacting the PSIRT regularly, as well as other available channels such as general-purpose e-mail inboxes or company social media accounts.

Sub-Function 2.1.2.2  Process reports in isolation

Vulnerability reports will be investigated by the PSIRT which is therefore easy to target through a malicious submission. Prepare policies and technical procedures to protect the working environment from such attempts by providing means to securely process vulnerability reports.

Sub-Function 2.1.2.3  Acknowledge reports timely

The detailed analysis of the report is often complex and time consuming, but mere acknowledgement of the report can be quickly achieved. Prompt reaction shows the report is taken seriously and greatly helps create a relationship of trust. Subsequent communication throughout the handling process can be built upon this first engagement and it shows the PSIRT is committed to comprehensible resolution.

Service 2.2 Identify Unreported Vulnerabilities

Vulnerabilities disclosed to the vendor directly or from reporting parties are straightforward to take in. However, it is important to realize there are additional vulnerabilities that may be disclosed via informal channels like news outlets, technical blogs, expert databases, social media or technical publications and conferences.

Purpose: Maintain situational awareness, reduce time of detection for threats affecting a stakeholder’s product as well as reducing the probability of full disclosures.

Outcome: Increased situational awareness in terms of security threats for a stakeholder’s product portfolio.

Function 2.2.1  Monitor Exploit Databases

Publicly available exploit databases or commercial feeds should be monitored actively to discover potential zero-day vulnerabilities that require investigation. A fully-functional exploit may lead to a company’s proactive communication with its stakeholders.

Purpose: Discover vulnerabilities that were never reported via proper channels.

Outcome: Enhanced knowledge about existence of functional exploits on the market.

Function 2.2.2  Monitor Conference Programs

Relevant security conferences should be monitored to identify submissions of interest. Although conferences often require coordinated or responsible disclosure by the presenting party, this proves only effective for specific products. Submissions might be
discussing broader topics such as protocol flaws that could require work of a PSIRT. If
the abstract raises questions, it is a good idea to engage with the finder at an early stage
to clarify if action needs to be taken. In addition, presence on conference and pro-active
engagement with authors can promote direct contact to the PSIRT for future research.

**Purpose**: Prevent surprise by any uncoordinated disclosure or identify flaws that could
directly or indirectly impact products of the stakeholders that the authors had not yet
considered.

**Outcome**: Opportunity to actively approach the authors before any publication to clarify
whether any products of the stakeholders are affected or whether there was a problem
in submitting a report.

**Function 2.2.3  Monitor Publications by Renown Finders**
Pay attention to publication by finders who have a track record of relevant publications
or extensive expertise with either the industry or specifically a company’s products and
services. Their scientific works, blogs posts, or mailing list participation may hint on
possible vulnerabilities or weaknesses that require attention.

**Purpose**: Maintain state of the scientific and technical knowledge on security topics
relevant for the stakeholders.

**Outcome**: Expertise in common threats, weaknesses, and possible countermeasures to
support the stakeholders when resolving product security issues.

**Function 2.2.4  Monitor Mass Media**
Especially in cases of catastrophic incidents to stakeholder installations or personnel,
the mass media often is first to pick up. Monitoring of mass media can help to detect
situations where the stakeholders of the PSIRT are potentially an important or
predominant supplier.

**Purpose**: Refuting a product vulnerability has contributed to the occurrence of the
incident.

**Outcome**: Increased readiness in the event stakeholders or the media inquire about
product vulnerabilities that could have been involved in causing the incident.

**Service 2.3 Monitoring for Product Component Vulnerabilities**
Vulnerabilities roughly fall into three categories: (1) vulnerabilities in a product’s very own
source code, (2) vulnerabilities in product components maintained by vendor-internal sources,
and (3) vulnerabilities in components provided by vendor-external sources (third-parties). From
a product’s perspective, (2) and (3) are external components, but vulnerabilities in these
components can ultimately impact the superseding product. Although a product owner has
only indirect control over the remediation of the underlying issue, the end-stakeholder sees
some degree of ownership over the supply chain and the remediation of the vulnerability with
regard to the affected product. This is especially the case, when the vulnerable component
cannot be updated independently from the including product. Included open source
components are also considered third-party components.

**Purpose:** Identify, gather, and monitor vulnerabilities in the supply chain of a
stakeholders’ products, and notify product teams on vulnerabilities affecting their
product.

**Outcome:** Greater insight into an early identification of vulnerabilities inherited from the
supply chain that affect a stakeholders’ products.

### Function 2.3.1 Inventory of Product Components

Keep a list of vendors, products and versions provided by external and internal parties
that are included in products. This is essential to quickly identify affected products for
inherited vulnerabilities.

**Purpose:** Identify products including vulnerable components that could potentially lead
to a vulnerability in the product itself.

**Outcome:** Completed bill of materials for all products to search for vulnerable product
components.

### Function 2.3.2 Monitor Third-Party Advisories

Obtain timely information about vulnerabilities in third-party components by
subscribing to vendor advisories or establishing specific communication channels to
suppliers. Subscribe to security mailing lists for open source projects. This can be
supported by the use of vulnerability information providers.

**Purpose:** Identify vulnerabilities in third-party components that result in a vulnerability
of a stakeholder’s product.

**Outcome:** Possibly initiate the vulnerability handling process before an external report
for affected products occurs.

### Function 2.3.3 Monitor Vulnerability Intelligence Sources

It might not always be possible to subscribe to vendor advisories for third-party
components. This is when the vendor does not publish advisories, the vendor went out
of business or the open source community around the component is not proactive.
Resources such as the National Vulnerability Database (NVD) or commercial intelligence
sources can help identify vulnerabilities that have not been advised.

**Purpose:** Identify vulnerabilities in third-party components that have not been advised.

**Outcome:** Greater insight into vulnerabilities that would have gone unnoticed.

### Function 2.3.4 Set-up Procedures for Intake of Vendor-Internal Supply Chain

Vulnerabilities

Product components from vendor-internal sources will in most cases not issue public
advisories on resolved security issues. In order to obtain information about
vulnerabilities in the vendor-internal supply chain, set-up specific communication
channels with such suppliers.

**Purpose:** Identify vulnerabilities in vendor-internal supply chain that result in a vulnerability of a stakeholder’s product.

**Outcome:** Greater insight into vendor-internal supply chain vulnerabilities that would have gone unnoticed.

### Function 2.3.5 Notification of Internal Development Teams

Establish automated channels to distribute identified third-party vulnerability notifications directly to the development teams of affected products. Often it is sufficient to follow the instructions of the upstream vendor to fix the issue in the downstream product. In accordance with the prioritization policy, define when vulnerabilities should be triaged differently and escalated to PSIRT handling. The latter is especially important if an end-stakeholder needs to take action to obtain a fixed version of the product in order to secure operation.

**Purpose:** Selectively inform development teams about vulnerable dependencies and patch information (if available) to allow fixing in the next product release.

**Outcome:** Reduce effort for PSIRT manual vulnerability handling as advisory information from third-party can be processed directly in the development processes.

### Service 2.4 Identifying New Vulnerabilities

A PSIRT may actively engage in internal discovery of new vulnerabilities as an opportunity to address security issues with products with a lesser management of external relations and potentially less coordination effort. Such activities should complement security verification activities that are part of the SDL. PSIRT activities may include red teaming prior to product release or in maintenance phase, as well as providing security testing tool expertise to R&D.

**Purpose:** Detect product vulnerabilities before external parties do.

**Outcome:** Expertise, procedures, and mechanisms for internal product vulnerability discovery.

### Function 2.4.1 Vulnerability Assessment

Vulnerability assessment is the practice of actively seeking to discover currently unknown vulnerabilities. This can include a wide range of techniques and tools such as red teaming, grey box/black box security assessments, or reverse engineering.

**Purpose:** Detect vulnerabilities through proactive mechanisms.

**Outcome:** A complementing quality assurance step to SDL security verification activities.

#### Sub-Function 2.4.1.1 Vulnerability assessment of products

The analysis results of a penetration tester challenging the security controls of a product can be of great help to developers looking to improve the posture of their
product before it is released to the market or when preparing an update.

Sub-Function 2.4.1.2 Vulnerability assessment of third-party component

For components that are obtained from third-parties, in addition to general procurement management, confidence in the quality of the component is increased through dedicated vulnerability assessment. Especially for critical components, this is completion for a high quality due diligence.

Function 2.4.2 Maintain Expertise for Security Testing Tools

Both commercial entities and communities are constantly developing new security analysis and offensive tools. The PSIRT security team should maintain up-to-date knowledge of available tools. This is useful for conducting assessments of products, validating findings from external finders, or the direct development teams choosing the right tools for their internal tests.

Purpose: Provide well-prepared expert team with the skill to handle complex tools and provide advice on the usage.

Outcome: Leverage the best tools available.

Sub-Function 2.4.2.1 Training of PSIRT staff on security testing tools

Training of staff is a key element of maintaining up-to-date knowledge of available security testing tools. Service 6.3 Secure Validation elaborates on PSIRT staff training in more detail.

Service 2.5 Vulnerability Discovery Metrics

Providing details around PSIRT volume, performance, or other measurements is critical to keep stakeholders aware of the effectiveness of the PSIRT (also see Operational Foundation Section 10: Evaluation and Improvements). Different stakeholders will have unique viewpoints that must be addressed with potentially differently formatted artifacts (or views). The PSIRT must understand how each stakeholder group desires to consume this information. These metrics could be KPIs for the PSIRT.

Purpose: Provide data around PSIRT measurement and performance. This helps stakeholders understand how effective the PSIRT is in providing a given area or service.

Outcome: By reviewing the PSIRTS metrics, stakeholders should know how effectively a PSIRT is providing a service and be able to provide feedback to make adjustments to that service delivery.

Function 2.5.1 Operational Reports

Operational reports provide information on the volume as well as the types of vulnerabilities being discovered. These reports may be published on a regular basis internally within the PSIRT as well as with internal stakeholders.
Purpose: Collect data regularly for general reporting.

Outcome: Determine areas requiring analysis, resource, improvement.

Sub-function 2.5.1.1 Total of discovered vulnerabilities vs. confirmed
This data helps capture the volume that a PSIRT handles from a resource perspective. This data may be broken down to business unit level, product type, or specific products.

Sub-function 2.5.1.2 Total of confirmed vulnerabilities broken down by third-party component
This data helps capture the risk associated with embedded specific third-party components.

Sub-function 2.5.1.3 Total confirmed vulnerabilities broken down by CWE
This data can be fed upstream to the Security Development Lifecycle and impact Training and Education. This data may be broken down to business unit level, product type, or specific products.

Sub-function 2.5.1.4 Total discovered vulnerabilities broken down by vulnerability discovery approach
This data helps identify easy-to-spot vulnerabilities and can be fed upstream to the Security Development Lifecycle. This data may be broken down to business unit level, product type, or specific products.

Sub-function 2.5.1.5 Total discovered vulnerabilities broken down by source
This data helps describe how well-known the PSIRT is.

Function 2.5.2 Business Reports
Business reports provide information on the vulnerability response health of an organization as it relates to handling and responding to security vulnerabilities.

Purpose: Establish metrics to define organization’s definition of success and collect data regularly for management reporting to identify risks.

Outcome: Dashboard highlighting successes and opportunities for improvement

Sub-function 2.5.2.1 On-time response rate
This data captures how well the PSIRT is doing in time for initial response to vulnerability reports within the respective SLA timeframes.

Sub-function 2.5.2.2 Total down time of PSIRT communication channels
This data captures if the PSIRT communication channels were available as defined in SLA.
Sub-function 2.5.2.3  Time to triage rate
This measures the time from initial report intake to completion of triage activities. This data captures the performance and/or workload of PSIRT staff.

Sub-function 2.5.2.4  Number of full disclosures, vulnerabilities exploited in the wild and vulnerabilities identified through media
This data captures the risk to a stakeholders’ products.
Vulnerability intake and triage commence the case management function of a PSIRT. While the order of operations is very similar among PSIRTs, there are variations within, such as the exact point of when a ‘case’ is created or the personnel performing different functions within a case. Where organizations receive a high volume of vulnerability reports, they may consider performing initial triage to validate reports before cases are created. In contrast, in organizations where the volume of vulnerability reports is low, a case may be made before triage. The ultimate goal among PSIRT is to create an efficient and defined process.

**Purpose:** Define how vulnerability reports will be triaged.

**Outcome:** Establish process across the PSIRT and related engineering teams.

### Service 3.1 Vulnerability Qualification

Organizations define an appropriate qualification criteria to the type and scope of issues it is willing to address. Such qualification criteria will help to set the security baseline and help with triaging incoming vulnerability reports effectively. Further, the organization should define the difference between a security “vulnerability” and a security “issue” to make it clear which issue types go into the vulnerability patching process. For example, a security vulnerability might be defined as an exploitable condition where a security issue might be defined as a method of bypassing a security mitigation.

**Function 3.1.1 Quality gate and Bug bars**

Quality gate and bug bars are used to establish minimum acceptable levels of security quality, and prioritization criteria for security vulnerabilities. Defining these criteria before products are released provides transparency to the vulnerability handling process by pre-determining what the PSIRT will qualify as a product vulnerability that should be remediated.

**Purpose:** Define clear minimum standards and prioritization criteria to provide transparency to internal and external stakeholders.

**Outcome:** Provide clear expectations to engineers and finders alike on what constitutes a vulnerability. Further prioritization criteria will mitigate confusion and disputes in managing the vulnerability lifecycle – from initial triage to patch communication.

**Sub-Function 3.1.1.1 Document product security vulnerability definitions**

The quality gate or bug bar should be documented, stored in a central location, and be part of the standard training for developers/engineers.
Sub-Function 3.1.1.2  Engage with product development teams

In the event that there are multiple products and product development teams within an organization, engaging across all of them to standardize the definition of a product security vulnerability is critically important.

Function 3.1.2  Continuous improvement

A mature PSIRT should adopt the mindset of continuous improvement to revise its qualification criteria where appropriate to reflect preceding experience, industry best-practices, product changes, and stakeholder feedback. It is important to communicate changes to internal and external stakeholders to manage their expectations.

Purpose: Recognize that the qualification criteria are subject to revision. The dynamics surrounding PSIRT such as stakeholder expectations, industry trends, or the volume of incoming vulnerabilities will likely lead to frequent adjustments.

Outcome: A fluid vulnerability qualification criteria will lead to an efficient vulnerability qualification practice.

Sub-Function 3.1.2.1  Collect data

Collect data on the triage process including number of incoming reports, how many qualify as a vulnerability, how many do not qualify, and any discrepancies encountered.

Purpose: Drive improvements based on data.

Outcome: Changes to quality gates and bug bars are data driven.

Service 3.2 Established Finders

As an organization’s PSIRT matures, the team may notice a group of habitual finders responsible for reporting an above-normal volume of vulnerabilities. It is recommended to consider the finder’s reputation and historical high quality of submissions, that some functions be bypassed such as qualification and triage to move directly to root cause analysis and remediation development. This may help to improve process efficiency and foster finder relationships.

Purpose: Understand the research community and who most commonly reports vulnerabilities in your products and services and consider immediate escalation of reports from highly trusted finders.

Outcome: Reduce response time for high quality finders.

Function 3.2.1  Finder Database

Develop and maintain a database of individuals and organizations who have reported vulnerabilities to you in order to track history, outcomes, and any other case handling
considerations for that finder.

**Purpose:** Improve the efficiency of the triage process and foster better relations with finders who have a track record for quality submissions.

**Outcome:** Reports from qualified finders move through the system faster. Finders are satisfied with outcomes and remediation is produced before any potential public disclosure timelines.

**Function 3.2.2 Accelerated Handling for Established Finders**

Some finders may be prolific or consistent (vetted/credibility) in finding and reporting software bugs in your products or services. They may for example use custom fuzzing tools and report crashes without a specific write up or proof of concept. When the finder is well known to you and you have determined that the majority of the issues they report will be fixed, consider skipping the qualification/vetting process all together and moving straight to remediation.

**Purpose:** Improve the efficiency of the triage process and foster better relations with finders who have a track record for quality submissions.

**Outcome:** Reports from qualified finders move through the system faster. Finders are satisfied with outcomes and remediation is produced before any potential public disclosure timelines.

**Function 3.2.3 Finder Profile**

Consider building profiles on finders to inform handlers how to best work with them. Profiles might contain things such as geographic location, languages spoken, conferences they have presented at, methodologies used to find vulnerabilities, products/technologies they typically focus on, do they practice coordinated vulnerability disclosure, do they like to present their findings at conferences, do you pay them bounties or have you offered other incentives, etc. Consult with legal and/or compliance teams to determine what information can be collected and how long it can be kept.

**Purpose:** Get to know the people who find vulnerabilities in your products.

**Outcome:** Handling can be tailored for a specific finder for the most positive outcomes.

**Function 3.2.4 Defining Finder Report Quality**

Organizations may want to consider defining and publishing guidelines for what constitutes a minimum quality vulnerability report in order to provide finders guidance on the type of information you need to quickly assess their report. A baseline might include, but not be limited to, a write up, reproduction steps, platform(s) tested on, and proof of concept.

**Purpose:** Provide guidelines to finders on the baseline for a quality vulnerability report.
Outcome: Back and forth between the vendor and finder is minimized and the vendor can focus quickly on a fix plan.

Service 3.3 Vulnerability Reproduction

Beyond qualification, unless otherwise specified, PSIRT needs to ensure the finder’s report is reproducible to validate and understand the conditions which lead to the vulnerable state.

Purpose: Provide the tools and environment for qualifying vulnerability reports.

Outcome: Efficient, safe, and secure vulnerability report validation.

Function 3.3.1 Establish Service Level Agreement for Vulnerability Reproduction

A PSIRT may not have sufficient technical expertise to reproduce all incoming vulnerabilities. PSIRTs may need to consult, work with, or rely on expertise within the product development or other teams so it is important to have clear aligned and defined agreement to ensure the needed expertise is readily available. Ideally a dedicated full and/or part time resources is recommended. However, if due to budget constraints this is not possible, at a minimum, subject matter experts should be pre-identified as part of the PSIRT plan who can serve on short notice for limited periods of time in case of an incident.

Purpose: Recognize the PSIRT does not have technical expertise to reproduce all incoming vulnerabilities.

Outcome: Prior internal alignment will ensure expertise is readily available on short notice to help reproduce vulnerabilities.

Function 3.3.2 Reproduction Test Environment

A dedicated test environment should be set up for PSIRT or dedicated team to reproduce the vulnerability. The test environment should be isolated, to avoid malicious activities and logging in validating a finder’s report. Where appropriate, a dedicated network environment, simulations, or virtualization can be used to create a safe environment.

Purpose: Create a safe environment to allow inspection and reproduction of vulnerabilities.

Outcome: A well-deployed reproduction test environment will help to process and qualify vulnerabilities efficiently, while limiting the vulnerability to the scope of the test environment.

Function 3.3.3 Reproduction Tools

Teams engaged in reproducing reported vulnerabilities need to have tools and updated product licenses at their disposal to perform these operations (e.g., a debugger).

Purpose: Ensure reproduction teams have the tools they need.

Outcome: Assurance reproduction of reported vulnerabilities is as efficient as possible.
Function 3.3.4  Vulnerability Storage

Given the sensitive nature of vulnerability reports, every effort should be taken to safeguard them. If possible, this information, including any proof of concept files, etc., should be stored on a separate network that is limited to only those who need access using multi-factor authentication.

*Purpose:* Keep sensitive and potentially damaging vulnerability information secure.

*Outcome:* Sensitive information is kept secure with limited access and is not susceptible to a compromise of the organization's primary network.

Function 3.3.5  Affected Products

During reproduction, the team doing the analysis should work to determine which products are affected and if any variants of the vulnerability exist. See also Product Lifecycle Management section 4.1.1.

*Purpose:* Gain a complete understanding and scope of the vulnerability across products.

*Outcome:* Fixes for the vulnerability are comprehensive across supported products.
Service Area 4 Remediation

This service area captures the different services required to deliver and announce security fixes to both stakeholders and downstream vendors. The delivery mechanism for a remediation should be determined based on impact of the vulnerability to stakeholders when exploited. Processes should be established to ensure that security fixes are delivered on a predictable schedule so both stakeholders and downstream vendors can plan accordingly for the test and deployment of these security fixes.

**Purpose:** Highlight the processes and mechanisms required to release and announce security fixes to stakeholders and downstream vendors.

**Outcome:** Enable stakeholders and downstream vendors to plan accordingly for security fixes.

---

### S4.1 Security Patch Release Management Plan

- **Step 1:** Incident?
  - Yes: S4.3 Incident Handling
  - No: Normal
- **Step 2:** S4.3 Incident Handling

### S4.2 Remediation

- Analysis
- Resolution
- Delivery

### S4.4 Vulnerability Release Metrics

### F4.2.4 Risk Management Analysis

### S1.5 Incident Communications Coordination within Organization

---

Yes

Normal

Expedite
Service 4.1 Security Patch Release Management Plan

This service focuses on providing guidance around how the vendor plans to establish a cadence for releasing security fixes for supported product versions in the market. Stakeholders, especially in the enterprise space, need to plan for the deployment of security fixes. Some deployments, like cloud, may have automatic updates or a different patch management policy.

**Purpose:** Educate constituency on what products will be supported, mechanisms for delivering security fixes as well as the cadence in which they will be delivered.

**Outcome:** Stakeholder will be able to plan in advance for deployment of security fixes.

Function 4.1.1 Product Lifecycle Management

Companies may have different support policies and agreements with stakeholders. Based on these factors, a PSIRT may partner with business units/lines of businesses and stakeholder support to determine how and if, they will support products which have fallen out of the support scope or support obligations. This could depend on the severity of the vulnerability and may involve inputs from business units/lines of businesses and stakeholder support.

**Purpose:** Provides a clear policy to product teams on how an organization will support products with security vulnerabilities.

**Outcome:** Clear policy on what the business unit/line of business expectations is in delivering security fixes for those types of products.

- **Sub-Function 4.1.1.1** Build a product inventory of all the products released to market to ensure all supported applicable products are assessed and remediated.
- **Sub-Function 4.1.1.2** Understand the different types of product support models including paid services, extended warranties, maintenance agreements or contracts with specific stakeholders.
- **Sub-Function 4.1.1.3** Identify at what point a product is no longer supported within the product lifecycle.

Function 4.1.2 Method of Delivery

PSIRTs may partner with product teams and stakeholder support to identify the different options for delivering security fixes to stakeholders. The criteria for determining when to deploy a security fix through the means identified should also be developed.

**Purpose:** Maintain a consistent mechanism to deliver remediated vulnerabilities based on a set of conditions.

**Outcome:** Stakeholders can plan and easily deploy security fixes.

- **Sub-function 4.1.2.1** Understand the different content types for packaging a security fix such as RPM.
Sub-function 4.1.2.2 Understand the different mechanisms for delivering security fixes such as hot fix, patch, maintenance releases and how to distribute fixes securely.

Sub-function 4.1.2.3 Identify across the different products how the security updates can be deployed for example remotely, customer installable, automatic updates or requires onsite.

Function 4.1.3 Delivery Cadence
Stakeholders and downstream vendors need to plan for security fixes so that they can maintain the security posture of their environment. By setting a cadence for when security updates will be delivered, this will enable stakeholders to schedule and plan resources for the necessary updates to their environments.

Purpose: Maintain a consistent cadence for when security updates are released to stakeholders.

Outcome: Stakeholders can plan and deploy the security updates.

Sub-function 4.1.3.1 Partner with product management teams and release management to determine the cadence for when security fixes should be delivered. Some security fixes are integrated in as part of a feature release and will be aligned to those release schedules. While others may require an emergency fix which is considered an out of band release.

Sub-function 4.1.3.2 Identify and document the exceptions for when a fix would not be delivered through the normal cadence.

Service 4.2 Remediation
This service relates to the management of reported vulnerabilities by finders and includes the response analysis as well as mitigation, and defines which versions will be remediated and may take into consideration how the remedy will be delivered. It may also consider any workarounds that can be immediately applied by the stakeholder prior to the security fix being delivered.

Purpose: Provide processes and best practices for delivering a remedy to a stakeholder based on the affected product(s), version(s) and stakeholders impacted.

Outcome: A security fix that is compatible with impacted products and stakeholder needs.

Function 4.2.1 Analysis
The impacted product may include a single software application, firmware or multiple hardware programs with different versions of software or firmware. A number of parameters need to be considered when crafting a remediation plan to ensure that your stakeholder needs are met.

Purpose: Determine affected product(s), versions and stakeholders.
**Outcome:** A security fix that is compatible with impacted products and stakeholder needs.

**Sub-Function 4.2.1.1** Validate the vulnerability report or incident against the quality gate or bug bar

See [Function 3.1.1 in the Vulnerability /Triage Service Area.](#)

**Sub-function 4.2.1.2** Identify affected products, versions and stakeholders as well as any variants that may need to be fixed at the same time.

**Sub-function 4.2.1.3** Review the support agreements and models associated with affected product versions

Refer to Sub-Function 4.1.1.2 in [Function 4.1.1 Product Lifecycle Management.](#)

**Sub-function 4.2.1.4** Root cause analysis

Understand the design or implementation flaw that caused the vulnerability.

**Sub-function 4.2.1.5** Determine the mechanism for rejecting a vulnerability

For example, a vulnerability may be a false positive or security design flaw.

**Sub-function 4.2.1.6** Remediation analysis

Determine the means to mitigate or remediate the risks created as a result of the vulnerability.

**Sub-function 4.2.1.7** Identify if there are any workarounds that can be implemented to mitigate the vulnerability while a fix is under development.

**Sub-function 4.2.1.8** Identify any exceptions where a vulnerability cannot be remediated

Refer to [Function 4.2.4 Risk Management Process.](#)

**Function 4.2.2 Remedy Resolution**

Prior to releasing a security fix for a reported vulnerability, it needs to be validated by a quality assurance (QA) engineer and if applicable, the finder who reported the vulnerability. This describes the process and mechanisms for validating the remedy internally as well as partnering with the finder to validate and sign off on the remedy.

**Purpose:** Provide a process and a mechanism to validate the remedy internally as well as partnering with the finder to sign off on the remedy, if applicable.

**Outcome:** Internal and/or external finder approval of the remedy that will be released.

**Sub-function 4.2.2.1** Validate to ensure all instances of the reported vulnerability have been remediated across all affected product versions.

**Sub-function 4.2.2.3** Obtain signoff of the remedy by the responsible QA
engineer or team. Remedy validation should be integrated into the standard testing/QA practice.

Sub-function 4.2.2.4 Partner with third-party finder or stakeholder to sign off on remedy.

Function 4.2.3 Remedy Delivery
As part of releasing a security fix for a reported vulnerability, the fix needs to be made available at the same time as the disclosure. Key stakeholders across the industry including the finder need to be kept informed. This describes the process and mechanism for coordinating the remedy and disclosure.

Purpose: The security fix is released at the same time as the disclosure and stakeholders are informed.

Outcome: Deliver security fix along with the disclosure to stakeholders.

Sub-function 4.2.3.1 Disclosure type
Determine the preferred mechanism for disclosing the vulnerability. This may be based on severity or type of vulnerability.

Sub-function 4.2.3.2 Coordinate the disclosure, if applicable.

Sub-function 4.2.3.3 Partner with stakeholder support or other stakeholders to post the remedy to web portal, stakeholder support site or Release to Manufacturing (RTM) as examples.

Sub-function 4.2.3.4 Partner with stakeholder support or stakeholders to release the disclosure of the reported vulnerability.

Function 4.2.4 Risk Management
It is a PSIRT responsibility to provide stakeholders with sufficient information so they are able to evaluate the risks to their systems resulting from vulnerabilities in their system and in the products the PSIRT organization supports. Risk management assessments should be conducted across the organization when a vulnerability is not remediated within a specific timeframe (per SLAs) or not remediated within a product. This includes having a transparent mechanism to quantify the risk as well as escalating up to, the appropriate stakeholders included in the organization’s Risk Register.

Purpose: Define a process for formal risk acceptance for any vulnerabilities not remediated within the internal SLAs time requirements.

Outcome: Transparency across the organization on the risks and assurance that the risks are appropriately escalated and acknowledged.

Sub-function 4.2.4.1 Identify which roles have the authority to accept the risk, for example Chief Information Security Office (CISO) /Chief Security Office (CSO) or Risk Manager, and which roles should be informed of the risk.

Sub-function 4.2.4.2 Define risk management practices for handling and
responding to risks within the organization including the set of conditions which
would trigger the process.

**Sub-function 4.2.4.3** Assess and quantify risks by conducting an assessment of
the risks to understand the threat and impacts to the business.

**Sub-function 4.2.4.4** Document the risk in the risk register

Assist the CSO, Risk Manager or other stakeholders in tracking both status of risk
evaluation and subsequently implementing recommendations.

**Sub-function 4.2.4.5** Recommendations

Update risk register with the findings and recommendations.

**Service 4.3 Incident Handling**

The PSIRT needs to have a mechanism to expedite remediation time to address “critical
vulnerabilities” which can be defined as active exploits in the wild, zero day, and in cases of
public disclosure. This service provides guidance for the incident as well as alerting stakeholders
and coordinating activities associated with the response, mitigation, and recovery of an incident
to reduce the time from report to delivery of the security fix.

*Purpose: Develop a plan to manage critical vulnerabilities and develop the ability to
mobilize all the resources required to address them.*

*Outcome: Delivery of emergency fixes for pending or public disclosure of a vulnerability
or other situation where stakeholders may be a risk and quick action is required.*

**Function 4.3.1 Establish Situation Room**

When incident management is required, establish a situation room including PSIRT,
Legal, Communications, Development, Stakeholder Support, Supplier and other roles as
needed. This can be a physical location or virtual as long as all parties are available to
respond as needed in a secure manner. Typically, both physical and remote options are
necessary to ensure stakeholder attendance. Resources should be identified ahead of
time in order to adequately support the incident management process.

*Purpose: Ensure stakeholders are available to answer questions and provide direction.
Assure the appropriate resources have been assigned to manage the incident.*

*Outcome: Organize vetted resources.*

**Sub-function 4.3.1.1** Identify resources required to handle and manage the
incident

Resources may include meeting rooms, private lines and additional man-power. For
long-term incident handling, food and accommodations should be considered.

**Sub-function 4.3.1.2** Identify all key stakeholders required to participate in
handling the incident as part of your incident response plan
This may be Communications, Developer leads, Legal as examples. See Service 1.1 Internal Stakeholder Management and Service 1.5 Incident Communications.

Sub-function 4.3.1.3 Assign clear roles and responsibilities to manage the incident

Personnel must know their roles and order of operations when a response is needed. Training and tabletop exercises should be conducted to prepare key response participants.

Function 4.3.2 Incident Management

When an incident is declared, the main focus of the PSIRT in partnership with their stakeholders is to reduce the impact of the incident and work to restore the business function of a product as well as their stakeholders.

Purpose: Create a playbook and execute a plan to contain the incident.

Outcome: Restore operations back to the product teams as well as stakeholders as soon as possible.

Sub-function 4.3.2.1 Information collection

Intake, cataloging, and storage of information related to the incident.

Sub-function 4.3.2.2 Incident handling is dependent upon analysis activities, which are defined in the “Analysis” section.

Sub-function 4.3.2.3 Response

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

Sub-function 4.3.2.4 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.

Sub-function 4.3.2.5 Incident post-mortem process

Action to review to identify improvements to processes, policies, procedures, resources, and tools to help mitigate and prevent future compromise.

Function 4.3.3 Communication Plan

All stakeholders and action owners must know the latest plans and progress to keep on track. Engage management as needed to break down any barriers that may impede open collaborative communication during an incident.

Purpose: Develop a communication plan and designate a central point of contact for the incident to keep everyone up to date on latest developments.
Outcome: Organize vetted communication.

Sub-function 4.3.3.1 Publication of information to internal stakeholders

Management of lists used to distribute announcements, alerts, data feeds or other publications for situational awareness.

Sub-function 4.3.3.2 Public relations are well managed and coordinated

Ensure information is disseminated to the media and stakeholders, but only through authorized organizational channels. This includes social media postings.

Sub-function 4.3.3.3 Recovery activities are communicated to internal stakeholders, executives, and management teams.

Sub-function 4.2.3.4 Incident postmortem briefings are conducted by PSIRT and feedback is collected to improve incident response as well as SDL activities (what SDL activity could have or should have prevented the issue in the first place?).

Service 4.4 Vulnerability Release Metrics

Data to be collected should include, but may be limited to, issue volume, classification, fix time, affected products or services

Purpose: Collect data regularly for management reporting.

Outcome: Determine areas requiring analysis, resource, improvement.

Function 4.4.1 Operational Reports

Operational reports provide information on the volume as well as the types of vulnerabilities being reported and confirmed across the different products and versions. These reports should be published at least on a regular basis internally within the PSIRT as well as with internal stakeholders.

Purpose: Collect data regularly for general reporting

Outcome: Determine areas requiring analysis, resource, improvement

Sub-function 4.4.1.1 Total number of vulnerabilities reported versus confirmed (by product/business units)

This data helps capture the volume that a PSIRT handles from a resource perspective.

Sub-function 4.4.1.2 Total confirmed vulnerabilities broken down by third-party component

This data helps capture the risk associated with embedded specific third-party components.

Sub-function 4.4.1.3 Total confirmed vulnerabilities broken down by CWE (by
This data can be fed upstream to the Security Development Lifecycle and impact Training and Education.

**Function 4.4.2 Business Reports**

Business reports provide information on the health of the vulnerability response capability of an organization.

*Purpose:* Establish measurements of the organization's level of success in meeting the time bound commitments made in the SLAs. Regularly collect, analyze and disseminate data which measures the level of achievement of those goals.

*Outcome:* Creation of a dashboard highlights the successes and opportunities for improvement.

**Sub-function 4.4.2.1 On-time impact assessment**

This metric captures how well product teams are doing in completing impact assessments within the respective impact assessment SLA timeframes.

**Sub-function 4.4.2.2 On-time fix plan**

This metric captures how well product teams are doing in providing a fix plan within the specified SLA.

**Sub-function 4.4.2.3 Remediation Tracking**

This metric captures how well product teams are doing in providing a fix within the specified SLA timeframes.

**Sub-function 4.4.2.4 On-time remediation rate**

This metric captures how well product teams are doing in meeting the overall objectives or agreements for delivering a fix from time of report to delivery of a fix. This can be broken down by severity or by vulnerability type (product line, type of vulnerability).

**Sub-function 4.4.2.5 Number of incidents**

This data captures the risk to the organization.
Service Area 5 Vulnerability Disclosure

It is important to create a transparent and collaborative environment where vendors, coordinators and finders can share information with their stakeholders and each other and negotiate mutually agreeable disclosure plans. By partnering in this way, the primary needs of resolving vulnerabilities, protecting stakeholders and acknowledging finders can be achieved. The vendor should publish their vulnerability disclosure policy so it can be referenced by coordinators, and by other vendors as well as finders.

*Purpose:* Provide transparency to stakeholders and partners through collaboration with finders, coordinators and downstream vendors to responsibly disclose vulnerabilities and fixes.

*Outcome:* Increased trust, collaboration and control of the disclosure.

Be able to understand the flow through the disclosure process and how it interacts with the different services throughout the PSIRT Framework.
Service 5.1 Notification

This service involves determining the appropriate notification process to provide timely information about mitigation strategy, fixes, and workarounds to stakeholders so they are kept informed and can plan accordingly. In some cases, contractual agreements may exist between vendors and an upstream vendor which would require the upstream vendor to notify the vendor of any policy disclosed vulnerabilities or known incidents. The intent of the notification process is to ensure that all stakeholders and vendors can understand and manage the risk imposed by the vulnerability.

**Purpose:** Provide transparency to vendors and finders through collaboration.

**Outcome:** Increase trust and collaboration with finders.

Function 5.1.1 Intermediate Vendor (Downstream Vendor)

An intermediate vendor such as an OEM or partner may develop and/or produce a part, subsystem or software that is used in another vendor’s end product. In such instances, their PSIRT should make arrangements to share vulnerability information with their vendors. They should be conscious of the vulnerability handling policy of the different vendors. Sometimes these expectations are captured in a contractual agreement. The timeline for fix release and disclosure should be negotiated as soon as possible.

**Purpose:** Create environment of collaboration and clear expectations between OEM and partners and other vendors.

**Outcome:** Increase trust, collaboration and control of the disclosure between all parties involved.

Sub-function 5.1.1.1 PSIRTs may learn of vulnerabilities reported by their stakeholders and should notify the intermediate vendor PSIRT of those vulnerabilities.

Sub-function 5.1.1.2 An intermediate vendor who supplies components or tools to a vendor may learn of vulnerabilities reported directly to them and should notify their vendor PSIRTs.

Sub-function 5.1.1.3 PSIRTs should identify all of their intermediate vendors and consider partnering with legal to ensure that clauses are added to contractual agreements to ensure a timely response on vulnerabilities.

Sub-function 5.1.1.4 Vendor PSIRTs may inform their stakeholders especially if the intermediate vendor is not able to or takes a considerable time in remediating the vulnerability. Some cases, a vendor PSIRT, may apply a tiered notification process and notify those stakeholders which would be impacted the most by the given vulnerability.

Function 5.1.2 Coordinators

A coordinator may be asked by a PSIRT to partake in notifying other vendors as well as coordinating the timing of release for their advisories especially if multiple vendors are involved. Coordinators such as CERT or third-party coordinators provide value by getting
a multitude of different organizations to partner and collaborate on addressing a
vulnerability.

**Purpose:** Coordinators may be asked to step in and assist PSIRTs organization in both
notifying and collaborating on the vulnerability with all vendors.

**Outcome:** Increased trust, collaboration, and control of the disclosure between all
parties involved.

**Sub-function 5.1.2.1** Document and understand the different coordinators based
on vulnerability disclosure policy.

**Sub-function 5.1.2.2** Partner with a coordinator to ensure all affected vendor
PSIRTs has been notified.

**Function 5.1.3** Finder

A finder such as a customer or third-party researcher may notify a PSIRT of a
vulnerability through the channels documented in Vulnerability Discovery.

**Purpose:** Create environment of collaboration and clear expectations with finders.

**Outcome:** Increased trust, collaboration and control of the disclosure with finders.

**Service 5.2 Coordination**

Where appropriate, a vendor PSIRT should make arrangements to share vulnerability
information with coordinators or other vendors. They should be conscious of the vulnerability
handling policy of the vendor. Timelines for release and disclosure should be negotiated as
soon as possible.

**Purpose:** Set expectations for all parties involved when collaborating and planning the
disclosure.

**Outcome:** Increased trust, collaboration, and control of the disclosure.

**Function 5.2.1** Bi-Lateral Coordination

A vendor PSIRT is responsible for maintaining communication with finders who report
potential vulnerabilities. It is important for vendors to understand the finder’s intent,
agenda, and stance on vulnerabilities in general, and promote/ and facilitate responsible
disclosure on an agreed timeline. PSIRTs should consider acknowledging the finders
who adhere to the public disclosure.

**Purpose:** Create an environment of collaboration where finders know they will be taken
seriously.

**Outcome:** Negotiated disclosure plan that honors the efforts of the finder.

**Sub-function 5.2.1.1** Acknowledge receipt of vulnerability report from third-party
finder.

**Sub-function 5.2.1.2** Provide the finder regular updates on the status of the
reported vulnerability.

**Sub-function 5.2.1.3** Provide the fix to finder so they can validate it as well.
Sub-function 5.2.1.4  Provide credit by acknowledging the contributions of the finder who reported the vulnerability. Vendor should verify with the finder that the credit is welcomed.

Function 5.2.2  Multi-Vendor Coordination

Where appropriate, a vendor PSIRT should make arrangements for sharing vulnerability information with coordinators or other vendors. They should be conscious of the vulnerability handling policy of the vendor. Timelines for release and disclosure should be negotiated as soon as possible.

Purpose: Provide transparency to stakeholders and partners through collaboration with all parties to responsibly disclose vulnerabilities and fixes.

Outcome: Increased trust, collaboration, and control of the disclosure.

<table>
<thead>
<tr>
<th>Multi-party Stakeholder</th>
<th>Relationship to Self</th>
<th>Stake in coordination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upstream vendors</td>
<td>OEM supplier provides technology.</td>
<td>To provide security patch. It is recommended upstream vendors manage their downstream stakeholders (see Service Area 1.4).</td>
</tr>
<tr>
<td>Downstream vendors</td>
<td>Receives technology from upstream vendor.</td>
<td>To be notified to apply the security patch. It is recommended that downstream vendors define and engage with upstream vendors communities and partners (see Function 1.3.1).</td>
</tr>
</tbody>
</table>

Sub-function 5.2.2.1  PSIRT vendor acknowledges receipt of the vulnerability report from vendor or coordinator.

Sub-function 5.2.2.2  PSIRT vendor or coordinator may need to identify those vendors that are impacted by the vulnerability report.

Sub-function 5.2.2.3  PSIRT vendor or coordinator share vulnerability information across the different vendors.

Sub-function 5.2.2.4  PSIRT vendor or coordinator partners with vendors on the timing and availability of fixes, and how the downstream vendors may receive the fixes.

Sub-function 5.2.2.5  PSIRT vendor or coordinator validates with vendors that the security update addresses the vulnerability.

Sub-function 5.2.2.6  PSIRT vendor or coordinator negotiates across all vendors to agree on both how the vulnerability will be disclosed and the timing of when the
disclosure will be publicly released.

Service 5.3 Disclosure

When a security update is released there should be appropriate disclosures to ensure that stakeholders and vendors are properly notified of the security updates. For each, the audience needs to be well defined (there may be different audiences for different types of notices).

Purpose: Document code changes and the release of security fixes.

Outcome: Clarity regarding what updates has been made to the code and where to get them.

Function 5.3.1 Release Notes

Release notes, including readme and change history, should include CVE reference(s) for the security fix/mitigation. Release notes should clearly communicate how the vulnerability was addressed. Transparency is key in demonstrating that the fix offered is adequate and complete, and not a partial mitigation or a patch that possibly creates other functionality or security issues.

Purpose: Provide indication of security fixes included in the updated code.

Outcome: Stakeholder can protect themselves from possible exposure of the vulnerability.

Sub-function 5.3.1.1 Define what vulnerabilities should be disclosed in the release notes.

Sub-function 5.3.1.2 Define the review process.

Sub-function 5.3.1.3 Conduct review and approval of disclosure.

Function 5.3.2 Security Advisory

Vendors should have a mechanism by which to release security advisories to stakeholders on a public web page and disclose vulnerabilities that have been remediated.

Purpose: Provide a public repository for published security advisories.

Outcome: Security advisories are available for review and action by constituency.

Sub-function 5.3.2.1 Define a security advisory template.

Sub-function 5.3.2.2 Determine the mechanism to deliver a security advisory (e.g., Common Security Advisory Framework (CSAF) or web document).

Sub-function 5.3.2.3 Define the set of conditions which would trigger the release of a security advisory. For example, if action needs to be taken to notify stakeholders that a hosted environment has been updated with a patch (breach scenario).

Sub-function 5.3.2.4 Determine the process for assigning a CVE ID to the vulnerability.

Sub-function 5.3.2.5 Request whether the finder seeks credit.

Sub-function 5.3.2.6 Define review process such as, who are the stakeholders
and when should the disclosure be crafted.

Sub-function 5.3.2.7 Conduct review process with defined stakeholders.

Function 5.3.3 Knowledge-Base Articles
Vendor should have a mechanism to publish knowledge-based articles which may accompany certain security updates which are deemed a lower severity or alternatively may be used as a means to communicate why specific reported vulnerabilities were rejected as false positives.

Purpose: **Provide a repository of knowledge base articles.**

Outcome: **Knowledge base articles are available for review and action by constituency.**

Sub-function 5.3.3.1 Define what vulnerabilities should be disclosed in a knowledge base article.

Sub-function 5.3.3.2 Define the review process.

Sub-function 5.3.3.3 Conduct review and approval of disclosure.

Function 5.3.4 Internal Stakeholder Communication
In addition to executive business owners who should be notified of vulnerability communication plans; there are many employees who are on the front lines working with stakeholders face to face and over the phone every day. Providing advanced, confidential notification and FAQ for coming advisories prepares those who may be asked about them upon publishing.

Purpose: **Inform executive business owners, global communications, and stakeholder-facing employees of ‘coming soon’ advisories and approved responses.**

Outcome: **Employees will be able to respond to stakeholders and media asking questions on day of advisory publication, resulting in controlling the message.**

Sub-function 5.3.4.1 Collaborate with internal stakeholders to craft and/or review language for their teams to use when customers ask about the vulnerability issue.

Service 5.4 Vulnerability Metrics
Data to be collected should include, but is not limited to issue volume, classification, fix time, affected products or services.

Purpose: **Collect data regularly for management reporting.**

Outcome: **Determine areas requiring analysis, resource, improvement.**

Function 5.4.1 Operational Reports
Operational reports may provide additional information on the volume of disclosures posted as well as the number of views for those artifacts. These reports should be published at least on a regular basis internally within the PSIRT as well as with internal stakeholders.

Purpose: **Collect data regularly for general reporting.**
Outcome: Determine areas requiring analysis, resource, improvement

Sub-function 5.4.1.1  Number of security advisories posted
The number of different disclosures can be reported and broken down by product. This may help drive you to have a technical resource assigned.

Sub-function 5.4.1.2  Number of CVEs posted to NVD
The number of CVEs assigned can be used to promote your status to a CVE Numbering Authority (CNA).

Sub-function 5.4.1.3  Page views on security advisories
This may drive your strategy to go towards proactive notification if the volume of stakeholders viewing your advisory is low.
Service Area 6 Training and Education

The world of product security is in a constant state of flux as new technologies, services, and integration make continuing training and education a top priority for security professionals. As software penetrates every aspect of the world we live in from our cars to our refrigerators, keeping up with the needs of securing products has never been more critical. A PSIRT plays a key role in supporting a strong curriculum in educating all stakeholders on the intricacies of developing, validating, and shipping products/services that meet the standards of today's connected world.

Training and education needs can vary significantly across a corporation. The concerns of a firmware developer vs. a software services developer are very different and often require very specific and unique types of training. For the sake of this document we will break out training needs into four stakeholder groups, PSIRT, product development, product validation and other stakeholders involved in the PSIRT process.

1) **PSIRT training** is unique since PSIRT members must be plugged into many aspects like legal, communications, and development.

2) **Product Development** (Internal Engineering and Development): Developers are highly skilled and focused in their skills and thus need training that is just as focused. Developing secure firmware that is very difficult to update in the field has very different requirements than that of a desktop application engineer.

3) **Product Validation** (Internal Engineering and Development): Validators require constant training to become familiar with the latest tools and techniques for things like pen-testing, vulnerability scanning, and early design reviews to catch issues before they have to be fixed.

4) **All other Stakeholders**: this group represents a less technical audience that requires a solid foundation in understanding the basics of developing, validating, and shipping secure products as well as in reacting when a shipped product has a vulnerability.

Secure development training is not considered as part of PSIRT program and is handled outside the PSIRT process. However, it is important that PSIRTs be champions of all aspects involved in bringing secure products to market and as such should partner with various development teams to make sure the appropriate training is in place. In many smaller organizations, there
may not be a separate group that takes the responsibility for making sure products are
developed with a security focus. In those cases, PSIRT may be involved in bridging the gap (this
is outside the scope of this document).

In each section, we will identify various stakeholder groups and summarize some focus areas
that may help a PSIRT team engage in meaningful discussions about training and educating
their stakeholders. PSIRTs may create all the training material in-house, use external material or
use external training resources to train their stakeholders.

Service 6.1 Training the PSIRT team

PSIRT Teams need to be at the forefront of what is happening in the world of security including
what's trending, new exploits, and industry activities to name a few. This broad level of
knowledge starts with requiring a solid foundation in general security world topics as
demonstrated by the leading security certifications. But certifications only provide a base that
needs to be constantly updated via activities like security focused conferences, industry
consortium involvement, and keen awareness of the industry as a whole by being an avid
consumer of blogs, industry press, consortium publications, etc. PSIRT members also need to be
aware of the constantly evolving world of security and privacy legislation which seems to
change rapidly.

Function 6.1.1 Technical training

It is important that PSIRT staff have a solid understanding of basic security concepts and
knowledge of the products that are being supported. The training material must be
regularly reviewed to ensure that as the security landscape changes, new vulnerability
techniques are being included in the training material.

Purpose: Train the PSIRT staff so that they understand the issue that is being reported
and can adequately perform the initial triage before handing it off to teams responsible
for developing, testing, and releasing fixes.

Outcome: PSIRT team has sufficient technical training to perform their duties.

The security concepts training would vary depending on the type of products that are
being supported by a vendor (e.g., hardware, firmware, software, networking, cloud
products or all of the above). At a very high level, the training must cover basic security
topics like common attacks, cryptography, confidentiality, integrity, availability,
authentication, authorization, access control models, multi tenancy, relevant
compliance, and regulations among others. This training should also include any
industry specific regulations that may impact PSIRT activities such as HIPAA for
healthcare verticals and PCI DSS for payment card vendors and banking. Some level of
product training must also be covered for PSIRT staff so that they are able to understand
the reported issues.
Function 6.1.2 Communications Training
Since the external finders report issues to the PSIRT, it is important that the PSIRT staff
is trained on the communication policies and soft skills that cover how to handle
communications with external finders and internal stakeholders in a timely manner.

Purpose: Ensure PSIRT staff follows the communication policies of the organization while
interacting with external entities thus eliminating any regulatory/legal issues that may
result from improper communication.

Outcome: PSIRT team will have sufficient communications training to perform their
assigned duties with clear accuracy and no ambiguity in communications.

Function 6.1.3 Process Training
There should be process guidelines that define how the reported issues will be tracked,
managed and measured. The roles of the various stakeholders involved in the process of
resolution of reported issues should be defined. The process should cover responding to
finders in a timely fashion and sending periodic updates to them for all open issues.
There should also be a well-defined and secure means of communicating information
between an external finder and the vendor.

Purpose: Ensure there is a smooth flow of information in managing product security
incidents which will result in timely resolution of issues.

Outcome: PSIRT members will be sufficiently training on internal processes so that they
can perform their duties.

Function 6.1.4 Task Tools Training
Sub-function 6.1.4.1 Bug tracking and other management tools for PSIRT and
the engineering staff

A formally acknowledged bug tracking tool should be identified for each product
(preferably the same for all products) in a given organization. All bugs should be
identified in this tool and security bugs should be uniformly identified as such. Only
those that have a need to know should be able to view and access the information
related to security vulnerabilities in a product. In addition, the tool should include
the capability to support program metrics requirements with both manual and
automated reporting capabilities.

Purpose: Ensure that issues are tracked effectively and vulnerability information is
safeguarded within the certified tracking tools where only those that have a
demonstrated need to know can access, track, and manage these issues.

Outcome: PSIRT members will be sufficiently trained and knowledgeable on tools
that they can perform their duties.

Sub-function 6.1.4.2 Third-party tracking tools

Most products include multiple third-party components (including open source) that are shipped with a product. The customers will often not know about the third-party software shipped within the product and hence would rely on the vendor to provide fixes or information on the patch. Hence it is important that internal third-party tracking tools be identified to cover the dependencies of vendor’s products on various third-party components. The National Vulnerability Database (NVD), third-party vendors’ security advisories and other external sites must be monitored to track the vulnerabilities and fixes for the third-party components so these fixes can be provided to the customer.

Purpose: Identify tools to track the third-party components embedded in products so the vulnerabilities can be tracked and released in these components.

Outcome: PSIRT members will have an understanding and be able to track third-party components within shipped products.

Function 6.1.5 Tracking All Training Initiatives

PSIRT team will need to track all the trainings that are available to various stakeholders. The team will need to ensure that all these trainings are delivered at a certain frequency as the security landscape is changing very rapidly and hence the trainings and processes will need to be continually redefined.

Purpose: Ensure all the trainings for various stakeholders are being tracked.

Outcome: PSIRT members will know various stakeholders have been trained on their roles in the PSIRT process.

Service 6.2 Training the Development Team

Secure Development refers to the methodologies and steps taken throughout the development process which are specifically designed to reduce the number and severity of vulnerabilities in software related products and services. By having a strong curriculum and a focus on secure development methodologies, vulnerabilities can be greatly reduced prior to product release which is much less expensive than dealing with them after the products are already released to the marketplace.

Secure development starts with product requirements and architecture. In addition, secure design reviews are key to spotting possible vulnerabilities before the product even goes into development.

There are numerous activities that are involved in a secure development program, the details of which are well outside the scope of this document. It is strongly recommended that a separate
program exists to manage an appropriate secure development lifecycle effort. This program should follow an accepted industry standard program model. An example of a Secure Development lifecycle is the Microsoft Secure Development Lifecycle model.

**Purpose:** Encourage the organization to have a proper Secure Development Lifecycle (SDL) program where development is trained on writing secure code and using documented security guidelines while creating the architecture and design of a product.

**Outcome:** Development teams will be able to write secure code and release more secure products.

Secure development training is not always considered as part of PSIRT constituency and may be handled outside the PSIRT process. In any case, it is an important step that must be considered by any vendor that cares about the secure posture of its products.

**Function 6.2.1 PSIRT Process Training**

Each member of the development process needs to comprehend why the PSIRT process exists, how it works, and what they need to do to develop products to support it. Often after a product is released, development teams move on to different projects and sustaining efforts are minimal. Training the teams and providing them with the appropriate methods to store key information about the product is critical for PSIRT to fully address a product vulnerability issue. Having information documented such as who was the security architect, the development lead, testing lead so that PSIRT teams can go back to those who know the most to assess risks and develop mitigations. This documentation should also include things such as: what are the 3rd party components that are being used, what is the product update process, what logging exists, what security exceptions were allowed and how are stakeholders notified. This information is also critical to PSIRT teams to close a security vulnerability. As new development team members come and go, refresher training is also critical.

**Purpose:** Ensure that all stakeholders understand the PSIRT process and how it relates to their role in product development.

**Outcome:** Culture of security among developers and better cooperation in dealing with vulnerabilities.

**Service 6.3 Training the Validation Team**

Validators need to be constantly updated on the latest tools and techniques for things such as pen-testing, vulnerability scanning, fuzzing, ethical hacking, and others. Training the validators on this falls under SDL and is outside the scope of this document. However, PSIRT team should encourage the organization to have a group that focuses on this.

**Purpose:** Encourage the organization to have a proper SDL program where proper security testing tools are identified.
Outcome: Higher quality and more secure products.

Just like secure development, secure validation training is not considered part of PSIRT constituency and is handled outside the PSIRT process. However, it is an equally important step that must be covered as part of SDL of a product by a vendor.

Function 6.3.1 PSIRT Process Training

Some members of the validation team may be involved in testing the fixes that are required to fix product vulnerabilities. These team members need to understand the PSIRT process, how it works, what are the expected timeframes and what their role is in the process. They would need a good understanding of the product life cycle so they know the supported versions that need to be tested for vulnerability fixes. They would need to also test the workarounds, if there are any. It will be important for them to also test for regressions.

Purpose: Ensure that all stakeholders understand the PSIRT process and how it relates to their role in product validation

Outcome: Culture of security among validators and better cooperation in dealing with vulnerabilities.

Service 6.4 Continuing Education for All Stakeholders

All stakeholders will require some level of training and awareness of the PSIRT program. There are many stakeholders that are involved in the end-to-end PSIRT process. Therefore, it is important to identify various stakeholder groups and develop training specific to their needs.

Purpose: Ensure that all stakeholder groups have the training or basic awareness they need to fulfill their role in the PSIRT program.

Outcome: Well-informed internal constituencies that know how they will work with the PSIRT in managing emergent vulnerability issues and what services PSIRT will offer in such situations.

Function 6.4.1 Training the Executive Management

This group is typically involved in initial sign off on the company’s communication, vulnerability protection and other policies. Management approval may also be required for creating security advisories. Also, executive management’s approval is often required for critical situations that create high risk, are highly visible or create high liability. Management may also want periodic status checks on the security posture of all products. Thus, it is important to inform management of the PSIRT processes.

Purpose: Make management teams aware of their role in the PSIRT program.

Outcome: Timely resolution of approvals that require management sign-off.
Function 6.4.2 Training the Legal Team
Legal is involved in setting up the initial corporate policies. Some finder-reported issues may have liability issues and may require assistance from legal groups so it is important to identify points of contact beforehand.

Purpose: Make legal team aware of their role in the PSIRT program and the involved timelines.

Outcome: Timely closure of security issues that require legal approval.

Function 6.4.3 Training the Government Affairs and Compliance Team
Government affairs folks are involved in regulatory compliance issues. Therefore, it is important to identify points of contact beforehand.

Purpose: Make the Government affairs team aware of their role in the PSIRT program.

Outcome: Timely resolution of security vulnerabilities that require complying to certain regulatory standards.

Function 6.4.4 Training the Marketing Team
Marketing is often involved when there is a risk to brand name. Also, security advisories may be reviewed by them and associated marketing information may be released alongside. Marketing teams are also involved in marketing the security aspect of products.

Purpose: Make the marketing teams aware of their role in the PSIRT program and educate them on what can and cannot be claimed regarding product security.

Outcome: Proper coordination between PSIRT and marketing teams will result in a well-aligned external security posture between the marketing material and security advisories.

Function 6.4.5 Training the Public Relations Team
Public Relations (PR) teams may be responsible for responding to external security posts or blogs, or press inquiries related to critical product vulnerabilities. Points of contact should be identified so PR can be involved if any external posting are required.

Purpose: Make the public relations teams aware of their role in the PSIRT program.

Outcome: Proper coordination between PSIRT and public relations teams will result in a good external security posture of the vendor.

Function 6.4.6 Training the Sales Team
Sales teams may be trained on basic security concepts and communications regarding security practices. Also, it is very important for salespeople to know what can and cannot be shared externally. It is recommended that sales employees redirect any concerns about security from stakeholders/prospects to either PSIRT staff or support staff as opposed to addressing them directly.
Purpose: Make the sales teams aware of what can and cannot be claimed regarding product security and where to go with questions they are unable to answer.

Outcome: Proper coordination between PSIRT and sales teams will result in meeting customer expectations.

Function 6.4.7 Training the Support Team
Support teams must be trained to handle security vulnerability reports from the customer. PSIRT may be involved in some cases for working these issues. Support should publish support policies that define the lifetime of every product, the versions supported and whether security advisories will be released. Most vendors only provide security advisories for the versions that are in support. So, these policies are critical and must be published on vendor’s website making it easily visible to stakeholders. PSIRT team typically maintains a close relationship with Support so they understand the kind of issues that are being reported by customers. Also, sometimes a finder may be a customer or the vice versa so handling of the issue may move between support and PSIRT.

Purpose: Make the support teams aware of their role in PSIRT process.

Outcome: Proper coordination between PSIRT and support teams will result in meeting both customer and reporter expectations.

Service 6.5 Provide Feedback Mechanism
Use information gained during the root cause analysis of the incident to educate the folks involved and prevent similar vulnerabilities in the future.

Purpose: Continuously improve training to keep up with the rapidly changing landscape of security industry.

Outcome: Higher quality training will result in improved experience for all stakeholders.
ANNEX 1: Supporting Resources

ISO 31000:2009 Risk management — Principles and guidelines
https://www.iso.org/iso-31000-risk-management.html

ISO/IEC 30111:2013 Information technology — Security techniques — Vulnerability handling processes


Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure

The Project Management Body of Knowledge (PMBBOK) Guide and Standards
## ANNEX 2: Pros and Cons of PSIRT Organizational Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| Distributed | A smaller core PSIRT operations team distributed work to PSIRT representatives across the different functional areas. (e.g. Support, Engineering, Product Management)                                                                                                                 | ● Ideal for large companies with large and diverse product portfolios.  
● Cost of PSIRT initiative defrayed.  
● Workload is distributed across the different function.  
● Scalable to grow with a growing portfolio                                                                                     | ● PSIRT organization has some authority to set policy and direction.  
● Often PSIRT does not directly control the resources that address the vulnerabilities and therefore have less control  
● Different product areas may put their own best interest ahead of the PSIRT activities.                                                                                     |
| Centralized | A larger PSIRT organization that is directly involved in all PSIRT activities (e.g. program management, triage, identification, remediation and communication) for all the different product areas.                                                                 | ● Ideal for smaller companies with smaller portfolios.  
● Central group of highly skilled product security experts.  
● PSIRT organization makes all of the decisions on PSIRT budgets, policies and resources.  
● Better control and accountability over the PSIRT operational activities.                                                                 | ● Does not scale well as the portfolios grows.  
● Major decisions will need to be made with the different functional manager’s cooperation or approval.  
● Costly to maintain a central team with specialized skills.                                                                                     |
| Hybrid | This is a combination of characteristics from both the centralized and distributed models.                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                  |
ANNEX 3: Types of Incident Response Teams

- **National CSIRT (Computer Security Incident Response Team)** – a national CSIRT refers to an entity which is constituted by a National Authority to provide national-level coordination of cybersecurity incidents. Its constituency generally includes all government departments and agencies, law enforcement and civil society. It also, generally, is the authority to interact with the national CSIRTs of other countries, as well as with regional and international players.

- **Critical Infrastructure / Sectoral CSIRT** – in charge of monitoring, managing and responding to cybersecurity incidents related to a specific sector (e.g. energy, telecom, finance)

- **Enterprise (Organizational) CSIRT** – An Enterprise CSIRT generally refers to a team in charge of monitoring, managing and handling cybersecurity incidents impacting the internal ICT infrastructures and services of a specific organization.

- **Regional / Multi-Party CSIRT** – a Regional / Multi-Party CSIRT refers to team or matrixed team in charge of monitoring, managing and responding to cybersecurity incidents related to a specific region, or a number of organizations.

- **Product Security Incident Response Team (PSIRT)** – a Product SIRT is a team within a commercial entity (typically a vendor) that manages the receipt, investigation, and internal or public reporting of security vulnerability information related to products or services commercialized by the organization.
Glossary

- **Actions** - the list of how something is done at varying levels of detail / maturity.

- **Capability** – a measurable activity that may be performed as part of an organization’s roles and responsibilities. For the purposes of the SIRT services framework the capabilities can either be defined as the broader services or as the requisite functions, tasks, or actions.

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

- **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 actions or tasks or in an aggregate of functions or services.

- **Red Teaming** - is a process designed to detect network and system vulnerabilities and test security by taking an attacker-like approach to system/network/data access. This process is also called "ethical hacking" since its ultimate purpose is to enhance security.

- **Tasks** - the list of actions that must be performed to complete the task.