Summer 2018 | 18

Product Security Incident Response Team (PSIRT) Services Framework

Version 1.0

Table of Contents

PSIRT Services Framework

Purpose

The *Services Frameworks* are high-level documents detailing possible services that computer incident response teams (CSIRTs) and product incident response teams (PSIRTs) may provide. They are developed by recognized experts from the FIRST community. FIRST strives to include feedback from all sectors, including CSIRTs with a national responsibility, private sector CSIRTs, and PSIRTs as well as other stakeholders. These documents were intended to provide a foundation for the development of new training material. However today they are used in a much wider scope, for example when defining an initial service catalogue for new teams.

In the creation of the CSIRT Services Framework it became clear that PSIRTs do provide quite different services and typically operate in quite different environments. It was thus decided to create a separate document covering PSIRTs. The two documents will be aligned, highlighting the many similarities shared. The development of the frameworks is driven by the Education Advisory Board.

The Frameworks exist to assist organizations in building, maintaining, and growing the capabilities of their CSIRTs or PSIRTs. The Frameworks are guides and identify various models, capabilities, services, and outcomes. In this way, teams are free to implement their own model and to build capabilities that meet their stakeholders' unique needs. The Frameworks seek to assist security incident response teams (SIRTs) by identifying core responsibilities, providing guidance on how to build capabilities to meet those responsibilities and offering insights on how teams can add and communicate value to their larger organizations.

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. PSIRT functions may also add value by providing guidance and oversight for the handling of internally found security issues.

PSIRT Framework Structure

SERVICE AREAS – SERVICES – FUNCTIONS – SUB-FUNCTIONS

SERVICE AREAS

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

SERVICES

A service is a set of recognizable, coherent functions towards a specific result on behalf of or for the stakeholder of an incident response team.

A service is specified by the following template:

- A "Description" field describing the nature of the service.
- A "Purpose and Outcome" field describing the intent and measurable results of the service.

FUNCTIONS

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

A function is described by the following template:

- A "Description" field describing the function.
- A "Purpose and Outcome" field describing the intent and measurable results of the service.
- The list of sub-functions that can be performed as part of the function.

SUB-FUNCTION

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

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 a 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 entities. The important point to take away is that both PSIRTs and CSIRTs do 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

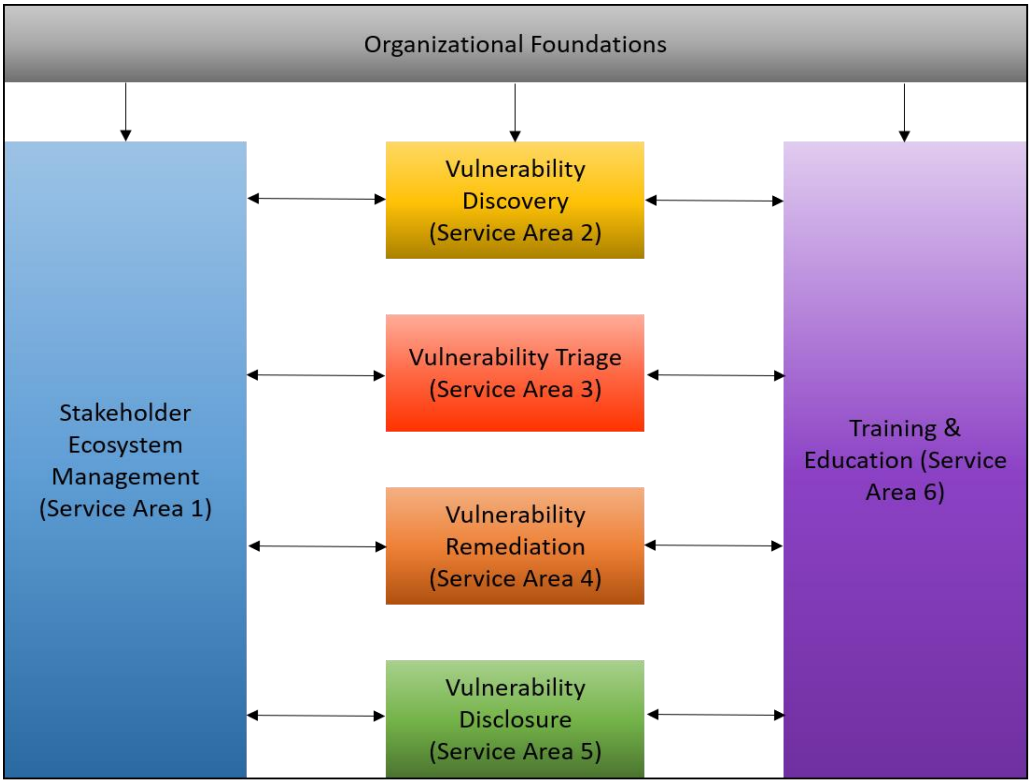


Figure 1: Organizational Structure

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 has several core responsibilities:

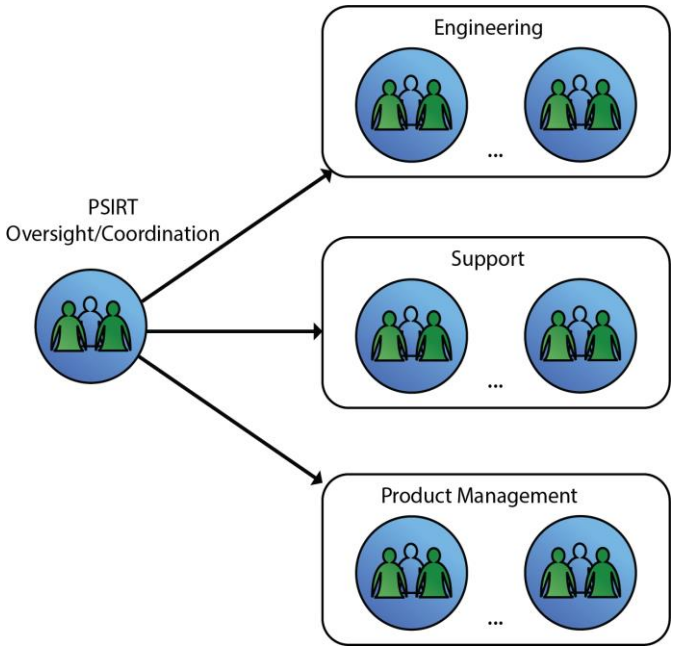


Figure 2: Distributed Model

- 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 Product Owner/Manager and the security engineer of new security vulnerabilities, assisting in the development of remediation plans, and drafting/publishing 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 and do not report to the PSIRT Operations.

Centralized Model

The Centralized model has a larger PSIRT staff drawn from multiple departments that report to one or more senior executives responsible for the organization's product security. This model might have a structure similar to the following:

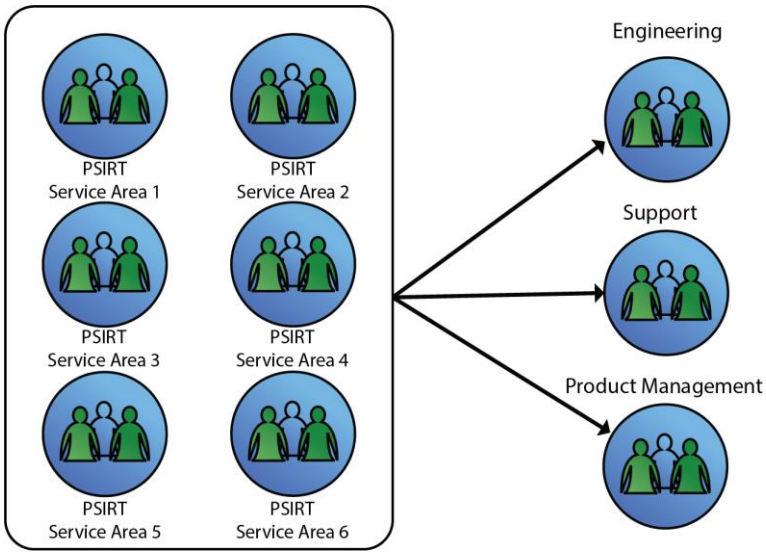


Figure 3: Centralized Model

- *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 and the 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 models. An organization may choose to implement some characteristics and features of both models, creating a hybrid that takes into account the following factors:
- Organizational corporate structure and size
- Product portfolio size and diversity
- Product development strategy

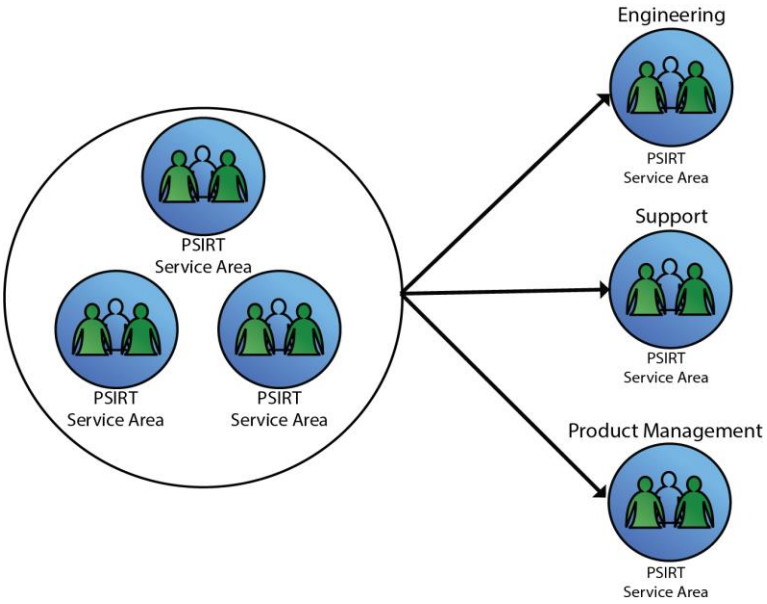


Figure 4: Hybrid Model

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 who 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 impose greater requirements on the formation, strategies, policies, and operational characteristics of a PSIRT than the stakeholders.

What does the PSIRT 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.

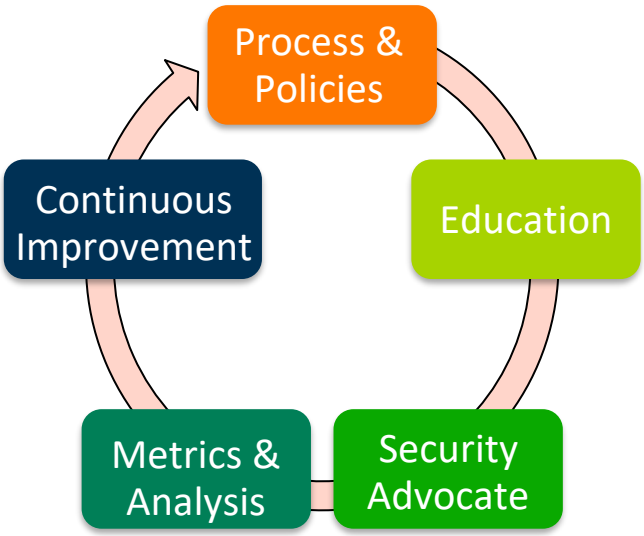


Figure 5: General PSIRT Activities

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 with these policies.

Educating Stakeholders

Along with PSIRT policies and procedures, the PSIRT 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 reporting does not define the requirements, 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 go into more detail 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 detail, while Tasks and Actions identify how it is being done at different levels of detail. Tasks and Actions are being published later 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**- criteria that define the types of bugs that qualify as a security vulnerability. Bugs that meet these criteria will be processed as a vulnerability through the PSIRT standard operating procedures.

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

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

-**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**- a set of criteria that must be met before the 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

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

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

-**Remediation (or Remedy)**- [5]a change made to a product or online service to remove or mitigate a vulnerability. A remediation typically takes the form of a binary file replacement, configuration change, or source code patch and recompile. Different terms used for "remediation" include patch, fix, update, hotfix, and upgrade. Mitigations are also called workarounds or countermeasures.

-**Risk**- [6]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**- [7]a risk response strategy whereby the project team decides to acknowledge the risk and not take any action unless the risk occurs.

-**Risk Register**- [8]a document in which the results of risk analysis and risk response planning are recorded.

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

-**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.

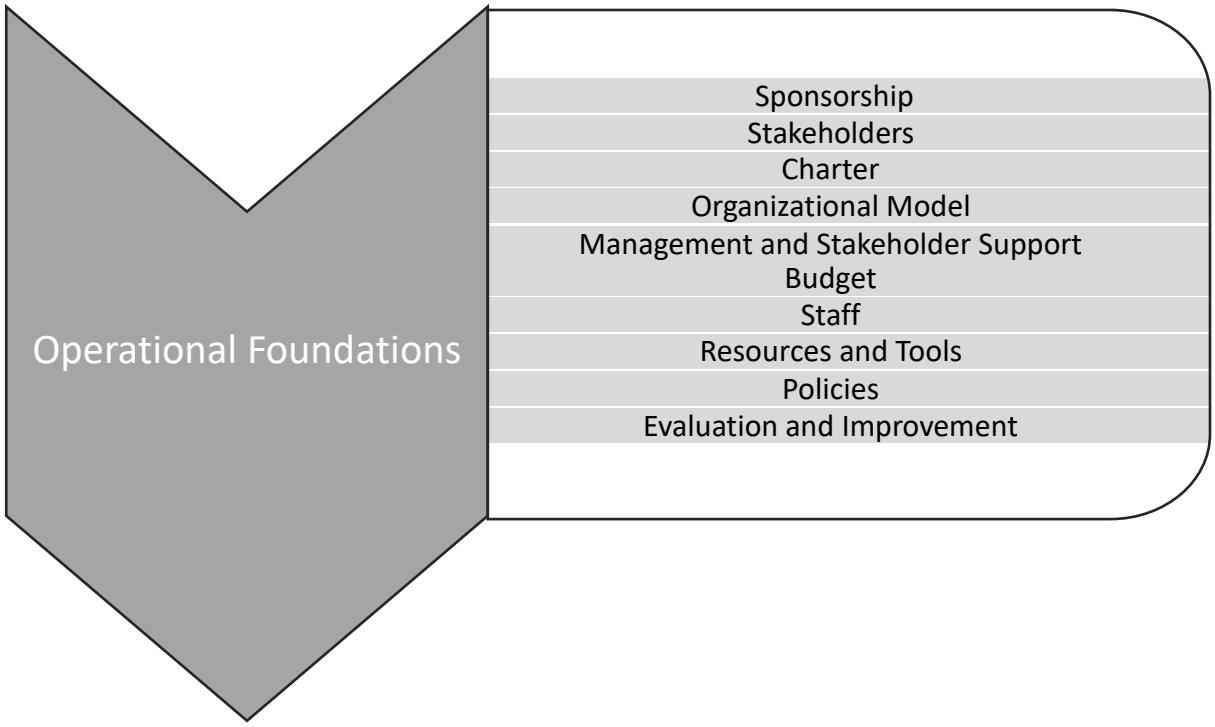
-**Stakeholders**- [9]PSIRT stakeholders are the groups that build and modify the product or product components and ensure an appropriate product communication strategy, and groups who can benefit from product security. In short, PSIRT Stakeholders either contribute to or benefit from product security and incident response.

-**Third-Party**- any upstream supplier or producer that provides components incorporated into a product or solution/service.

-**Vendor**- [10]a person or organization that developed the product, or service, or is responsible for maintaining it.

-**Vulnerability**- [11]weakness of software, hardware, or online service that can be exploited.

[5] ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability disclosure- Terms/Definitions 3.6
[6] ISO 31000:2009/ ISO Guide 73:2002 Risk management — Principles and guidelines- Terms/Definitions 2.1
[7] The Project Management Body of Knowledge (PMBOK) Guide and Standards
[8] The Project Management Body of Knowledge (PMBOK) Guide and Standards
[9] Architecture Content Framework
[10] ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes- Terms/Definitions 3.7
[11] 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. Strategic

A. 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:** Ongoing funding and support based on 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.

B. 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**: A 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 (Service 1.1 Internal Stakeholder Management, Service 1.2 Finder Community Engagement, Service 1.3 Community and Organizational Engagement, and Service 1.4 Downstream Stakeholder Management) for related information.

C. 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/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).

D. 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" for descriptions of some common organizational models (e.g. distributed model, centralized model, hybrid model). See Service 1.5 Incident Communications Coordination within the Organization for more related information.

E. Management and Stakeholder Support

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

***Purpose**: Inform and obtain 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.

II. Tactical

A. 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 and benefits, plus other encumbered costs), equipment, and other capital expenses (e.g. information technology systems/devices, software licenses), and training budget (including travel expenses).

B. 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 positions or roles and responsibilities for individual members of the PSIRT, as well as the competencies (knowledge, skills, and 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 Training the PSIRT for related information.

C. 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 Vulnerability 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)

III. Operational

A. 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's authority and its governance/operations. 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.

B. 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 identify 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 Postmortem 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 PSIRT's operations.

Service Area 1

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. 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 would be beneficial to understand the viewpoints or artifacts or methods by which they desire to be engaged with (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 consumers 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

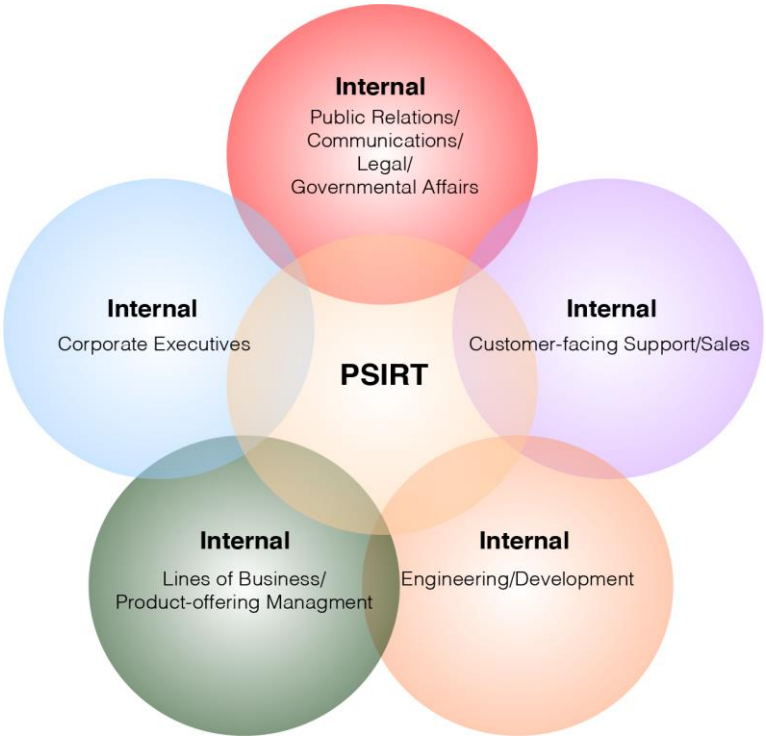


Figure 6: Internal Stakeholder Management

Define processes related to engaging with internal stakeholders to ensure both awareness and 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:** With highly engaged internal stakeholders, all PSIRT processes and outcomes should flow more smoothly. For example, flaws discovered by employees relieve the immediate pressure of external embargoes or media scrutiny, allowing the issue to be addressed on a schedule that benefits the organization, its consumers, and the greater community and minimizes risk to public disclosure of unfixed vulnerabilities.*

Function 1.1.1 Engage Internal Stakeholders

Maintain active dialog with internal teams involved around the development, testing, packaging, and maintenance of the organization's offerings. Internal stakeholders are not only engineering resources, but could also 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 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 Public Relations, Legal, and Corporate Communications

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 offers unique paths to critical stakeholders of the PSIRT, and lines of communication should be established prior to critical events or incidents to ensure all parties can effectively work together.

Sub-Function 1.1.1.3 Engage Lines of Business

Engaging with development stakeholders ensures issues are appropriately documented, prioritized and addressed. For example, engineers from the PSIRT 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.

Sub-Function 1.1.1.4 Engage Development/Engineering

Engineers from the PSIRT need to coordinate vulnerability remediation with the software engineering groups responsible for the flawed code. Engaging with development stakeholders ensures issues are 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 Customer-Facing Teams – Sales, Support

Engineers from the PSIRT 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.), internal/external Sales teams, or in-field resources (consulting, sales engineering, etc.).

Sub-Function 1.1.1.6 Internal Working Group Participation

In more mature organizations, engineers from the PSIRT 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.

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 the ability to demonstrate repeatable application of security standards through a product's lifecycle, stakeholders may lose faith in the organization's products, they may impose harsher requirements on the organization (burden of proof, right to audit, etc.), and could ultimately 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 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 Activities

SDL is a critical governance process that helps an organization produce stable, repeatable offerings that adhere to common standards. The PSIRT's 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

SDL is a critical governance process that helps an organization produce stable, repeatable offerings that adhere to common standards. The PSIRT's 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 Postmortem Process

As vulnerabilities are discovered within the organization's offerings, the PSIRT requires a process to review these issues be they code, process, or personnel-related, to provide 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 and corrected the issues. A postmortem is a meeting involving all internal stakeholders that participated 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 a vulnerability response, including security incidents, from the perspectives of all involved parties/teams. In times of a critical issue, the PSIRT can assist or lead the organization's response to remediating a publicly known, high-impact issue.*

Outcome: *The PSIRT will provide data around the organization's performance reacting to software vulnerabilities. This data will be incorporated into the "lessons learned" for future improvement during events.*

Sub-Function 1.1.3.1 Establish Product Security Defect Review Process

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

Sub-Function 1.1.3.2 Review Timing of Processes and Release Updates

Track areas of strength and weakness.

Sub-Function 1.1.3.3 Review High-Profile Incidents

Coordinate organizational lessons-learned, response and review for high-profile incidents, and provide reporting data to the business and other stakeholders as required.

Service 1.2 Finder Community Engagement

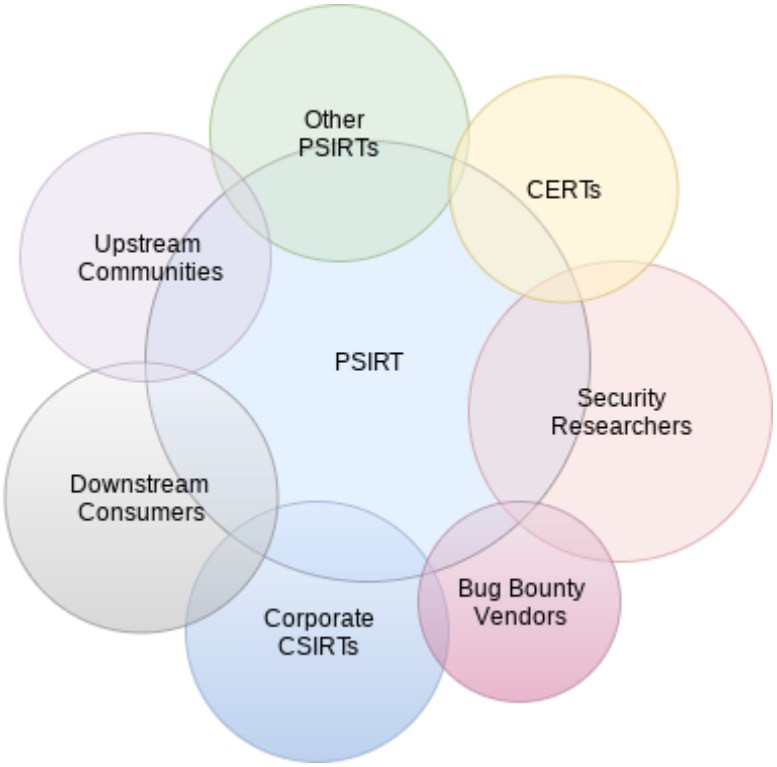


Figure 7: Example of External Stakeholders for the PSIRT

Services related to engaging the research community as a stakeholder. Finders have many varied roles and unique perspectives – they may be academics, development professionals, professional security finders, or hobbyists. Finders may be researching theoretical attacks or flaws in the hopes of publication and academic achievement, while others may be 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 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

Implement activities designed to maintain active dialogue with finders that have expertise in the security of a company's products and access to different channels. PSIRTs can conduct numerous activities to more deeply engage with their finder communities. These activities could include inviting well-qualified finders into private contracts, engaging with them at conferences and other events, or even sponsoring academic research.

***Purpose**: Build presence on social media sites. Monitor social media sites 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 higher-quality reports more frequently and with more advanced notice from highly engaged finders due to clearly defined communications expectations.*

Function 1.2.2 Engage with other PSIRTs

Nurturing relationships between peer PSIRTs 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 exposes the organization to the peer's expertise as the two groups consult on issues. The PSIRT should establish communication channels (both normal and secured) with key peer PSIRTs. Establishing and nurturing relationships with industry peers is critical for information sharing and coordinating on issues that affect both organizations.

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

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

Sub-Function 1.2.2.1 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, allowing the PSIRT to extend its internal capabilities by leveraging these external peers for information and/or assistance.

Sub-Function 1.2.2.2 Define Coordinated Disclosure Process

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 1.2.2.3 Establish Security Information-Sharing Process

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

Sub-Function 1.2.2.4 Participate in Industry SIGs and Working Groups

Working with peers on topics of industry interest supports and nurtures contacts and furthers the professionalization of the industry by collaboratively solving problems.

Function 1.2.3 Engage with Coordinators (CSIRTs and other Coordination Center Organizations)

Working with government CSIRTs 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), International Organization for Standardization (ISO), amongst others. Groups that participate could be viewed based on 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 CSIRTs enables the trust and contacts needed to obtain potential vulnerability reports at early stages.*

Outcome: *Good relationships with CSIRTs and other coordination center organizations are valuable for becoming aware of vulnerabilities early on. A faster response rate can be expected.*

Sub-Function 1.2.3.1 Engage Communities and Partners

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

Function 1.2.4 Engage with Security Researchers

Security researchers come in many varieties – academics, hobbyists, and professional security practitioners, to name a few. These persons are the primary finders of vulnerabilities across the industry. Researchers will attempt to contact the owner of a product, but for assorted reasons they will not always reach the appropriate party. PSIRTs will passively receive reports from these individuals or groups and be forced to work on externally controlled timeframes. It is in the PSIRT's best interest to take a proactive approach with security researchers who are involved in studying areas that

affect the PSIRT's products, and to positively engage with those groups to have greater visibility into discovered issues.

Sub-Function 1.2.4.1 Engage with Security Vendors

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

Sub-Function 1.2.4.2 Document Relevant Security Vendors

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 that all involved parties understand how they should behave, what resources they can access, how data is shared, and with whom it is shared.

Sub-Function 1.2.4.3 Document Methods to Engage with Security Vendors

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

Function 1.2.5 Engage with Bug Bounty Vendors

Building a relationship with bug bounty vendors to enhance 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 Service Level Agreements (SLAs) for vulnerabilities to be addressed.*

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

Sub-Function 1.2.5.1 Document and Define Relevant Bug Bounty Programs

Document and define bug-bounty vendors applicable to the offerings the organization provides.

Sub-Function 1.2.5.2 Engage Bug Bounty Vendors

Identify channels to engage these bug-bounty vendors in active dialogue.

Function 1.2.6 Anticipate the needs of CSIRTs

CSIRTs are a special category of "downstream" stakeholders that are purely focused upon security concerns. While these groups can typically be interacted with via standard stakeholder engagement practices and customer management, the PSIRT should understand the unique requirements and perspective of these security-focused groups that will contact and consume information from the PSIRT. This includes disclosure formats and timelines (see Service 5.3 Disclosure), as well as communication channels for specific requests.

Service 1.3 Community and Organizational Engagement

Two stakeholder groups that PSIRTs will interact with deserve additional attention. 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 your organization sources components or projects for its products. "Downstream" refers to individuals, groups, or organizations that source your organization's output as part of their offerings. Downstream engagement is covered in Service 1.4 Downstream Stakeholder Management.

A vibrant upstream community can help feed innovation into product streams as well as assist with the burden of complex vulnerability remediations, often compensating for the lack of crucial subject matter expertise within the organization. Likewise, cultivating professional relationships with individuals and teams from other organizations can help 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 and 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 a good reputation in the security community may help attract resources and collaborators to address critical situations.*

Function 1.3.1 Define & Engage with Upstream Communities & Partners

Often 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, original equipment manufacturers (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. Understanding how to contact these groups, and whom to contact, 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 that others receive from them.*

Outcome: *The PSIRT will better understand by whom and from where components are sourced. 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 Engage Communities and Partners

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

Sub-Function 1.3.1.3 Participate in Upstream Communities

Participation with upstream communities and partners helps build valuable inter-group trust, 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 and Industry Events

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

Sub-Function 1.3.1.5 Engage Community Security Teams

It is critical that the PSIRT understands how to contact upstream software/hardware/service providers' security teams (PSIRT, CSIRT, security engineers), and whom to contact. 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 Define & Engage with Downstream Communities & Partners

"Downstream" has many connotations, but that does not mean that the PSIRT should ignore these vital stakeholder groups. "Downstream" refers to any product, organization, or individual that takes the PSIRT's company's products and offerings and uses them for their own purposes. This most frequently takes the form of customers or consumers of the goods and services offered, but this is not always the case. Often another company could use or license the PSIRT's company's products and resell them as an offering through this third party, or in the case of open-source software, where this commonly occurs, one group will provide and maintain software and a large group of ancillary parties will leverage those resources, also known as being downstream from the source.

Sub-Function 1.3.2.1 Document and Define Downstream Communities, Consumers, and Partners

Downstream communities and partners consume code, and/or, knowledge and expertise that is incorporated into the organization's offerings. Ideally these relationships are documented in contracts, covered by non-disclosure agreements and other protections for the organization.

Sub-Function 1.3.2.2 Engage Downstream Communities

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

Service 1.4 Downstream Stakeholder Management

To engage your stakeholder base as a stakeholder, PSIRTs must establish 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.

Purpose: *PSIRTs need to build and maintain channels with the organization's stakeholder base to convey information about product security vulnerabilities or during Incident response events.*

Outcome: *Good relationships with your stakeholders 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 and opinions and obtain support 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 the 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 should be regarding 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 the remedy 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 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 Communication Channels

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 are 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 can also 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.

Function 1.5.3 Security Defect Tracking System Updates

The PSIRT should have access to system(s) of record for all product defects and be able to create and use a system for tracking and information-sharing around security 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 Flaw Defect Tracking for Products

Security defects should be tracked, and these systems should be accessible (within the least privilege model) with internal and external parties (if applicable) 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 Create and Publish Security Defect Tracking Process

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 make information available about what the security vulnerability is, what its severity and impacts 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 Communication Outlets

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, 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 methods to advertise the fix.

Sub-Function 1.5.4.2 Provide Feedback to Stakeholders

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

Acknowledging the finder helps establish their and their organization's (as applicable) credibility within the community in addition to expressing appreciation for partnering with the PSIRT on the flaw.

***Purpose:** Finders are acknowledged for efforts to coordinate disclosure of product vulnerabilities. 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 demonstrate 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

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, software release notes, and CVE text. The PSIRT will need to understand how internal attribution of found vulnerabilities will be communicated.

Function 1.6.2 Reward Finders

To generate positive outcomes for stakeholders and encourage further sharing of research, the PSIRT can elect to develop a program to reward or incent this collaboration 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 promotional merchandise (organizational swag), 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 goodwill toward the PSIRT's organization and encourage future continued collaboration around security issues.*

Sub-Function 1.6.2.1 Create Finder Rewards Program

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

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.

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 Reports and how the PSIRT should consider providing such reports ensure smooth operations. Function 2.5.2 reviews Business Reports 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 PSIRT's 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 chosen.*

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

Sub-Function 1.7.1.1 Gather Stakeholder Metrics Requirements

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.

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 PSIRT's 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 taken 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

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 Data Context

Provide context to data so that stakeholders can appropriately understand what will be provided to them and offer a possibility 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 another 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 on that performance.*

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

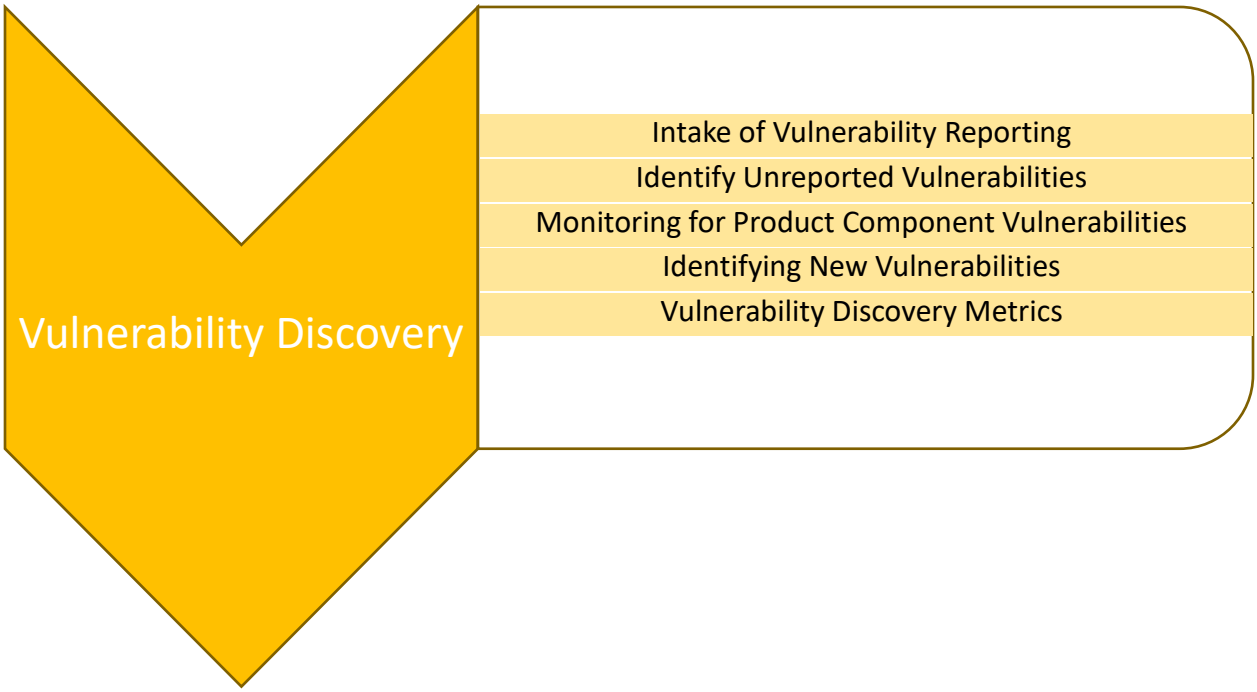
Sub-Function 1.7.4.1 Provide Stakeholder with Metric Artifacts

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 and Lesson Learned

One of the PSIRT's most important 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.

Service Area 2



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 a 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 Form 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 email 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), and 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 in which the vulnerability was observed. To avoid accidental information leakage or disclosure, promote means to submit reports in an encrypted manner, such as S/MIME or PGP protected emails 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 an 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 email 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 Timely Acknowledgement of Reports

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. Besides directly referencing products or brands, submissions might be discussing broader topics such as protocol flaws that may 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 Renowned 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 is often 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 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 remediated 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 stakeholder's products, and notify product teams on vulnerabilities affecting their product.*

***Outcome**: Greater insight into early identification of vulnerabilities inherited from the supply chain that affect a stakeholder's 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 a 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 to lessen management of external relations and potentially reduce overall coordination effort. Such activities should complement security verification activities that are part of the SDL. PSIRT activities may include product-security assessments prior to product release or in the maintenance phase, as well as providing security testing tool expertise to Research & Development. Internally found vulnerabilities impacting end users should be treated in the same manner as externally found vulnerabilities, including scoring and reporting, coordinated with the fix publication.

***Purpose**: Detect and fix product vulnerabilities prior to external discovery.*

***Outcome**: Expertise, procedures, and mechanisms for internal product vulnerability discovery and possible reduced coordination effort.*

Function 2.4.1 Product Security Assessment

Product security assessment is the practice of actively seeking to discover currently unknown vulnerabilities. This can include a wide range of techniques and tools such as penetration testing or vulnerability scanners. These grey-box/black-box security assessment techniques simulate company-external hacking as they refer to a methodology where the attacker has little, or no knowledge of the system being attacked.

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

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

Sub-Function 2.4.1.1 Security Assessment of your Products

The analysis results of a security assessment challenging the security controls of your 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 a remedy.

Sub-Function 2.4.1.2 Security Assessment of Third-Party Components

For components that are obtained from third parties it is recommended that there is a need for an increased dedicated security assessment, in addition to general procurement management procedures. This is especially needed for critical components to ensure 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 should maintain up-to-date knowledge of available tools. This is useful for conducting assessments of products, validating findings from external finders, or directing development teams choosing the right tools for their internal tests.

***Purpose**: Provide a 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 in 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

Figure 8: Vulnerability Discovery Metrics Process

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 III: 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 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 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, resources, 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 & 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 the 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 whether the PSIRT communication channels were available as defined in the 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 stakeholder's products.

Service Area 3 Vulnerability Triage and Analysis

Vulnerability intake and triage comprise the case management function of a PSIRT. While the order of operations is very similar among PSIRTs, there are variations, such as the exact point 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 created 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 appropriate qualification criteria to the type and scope of issues they are willing to address. Such qualification criteria will help set the security baseline and help with triaging incoming vulnerability reports effectively.

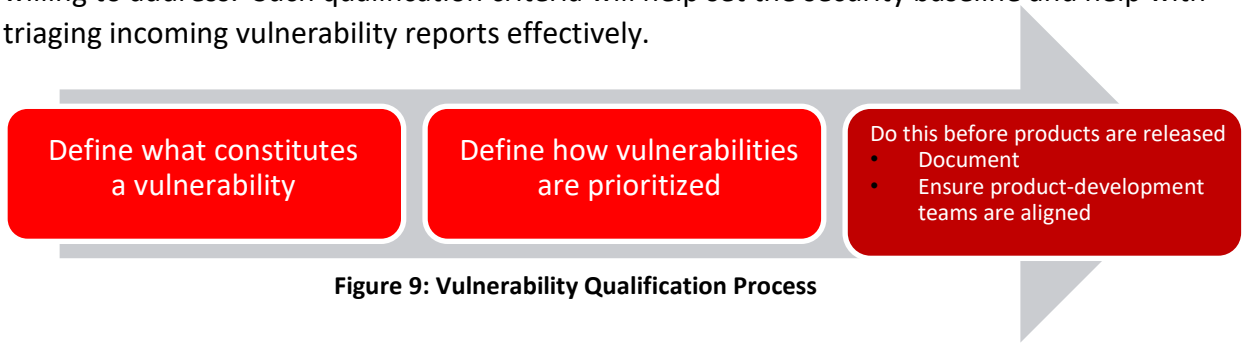


Figure 9: Vulnerability Qualification Process

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 past 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. For example, they may 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 altogether 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, if they practice coordinated vulnerability disclosure, if they like to present their findings at conferences, if 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 in order 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.*

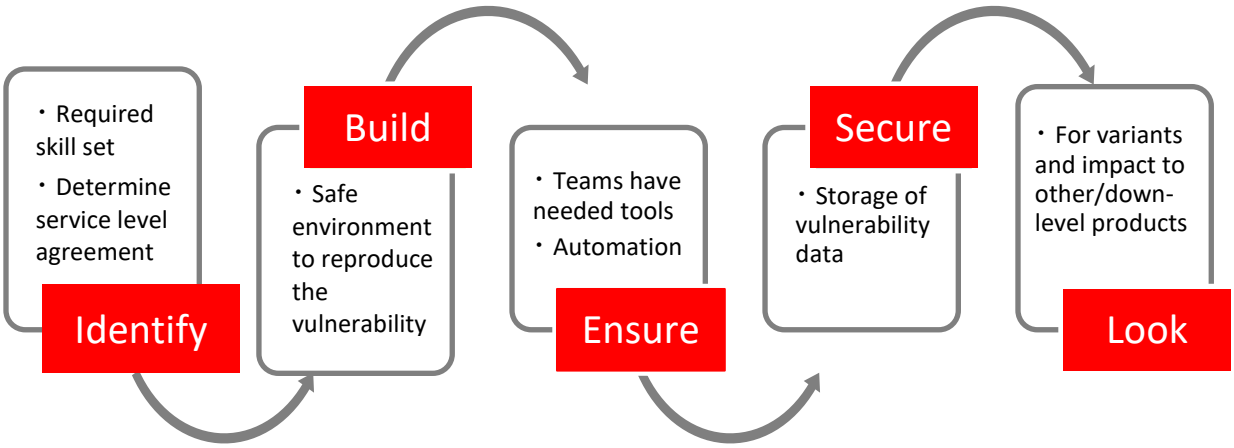


Figure 10: Vulnerability Verification/Reproduction

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

product development or other teams so it is important to have a clearly aligned and defined agreement to ensure the needed expertise is readily available. Ideally a dedicated full or part-time resource 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 process who can serve on short notice for limited periods of time in case of an incident.

***Purpose**: Recognize that 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 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**: Assure reproduction of reported vulnerabilities is as efficient as possible.*

Function 3.3.4 Vulnerability Storage

It is recommended that sensitive information, such as vulnerability reports, proof of concepts files, etc. should be stored securely and access limited to only those who need it and ensure security of the information at rest and in transit. For example, see ISO 27001.

***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 Impacted Products

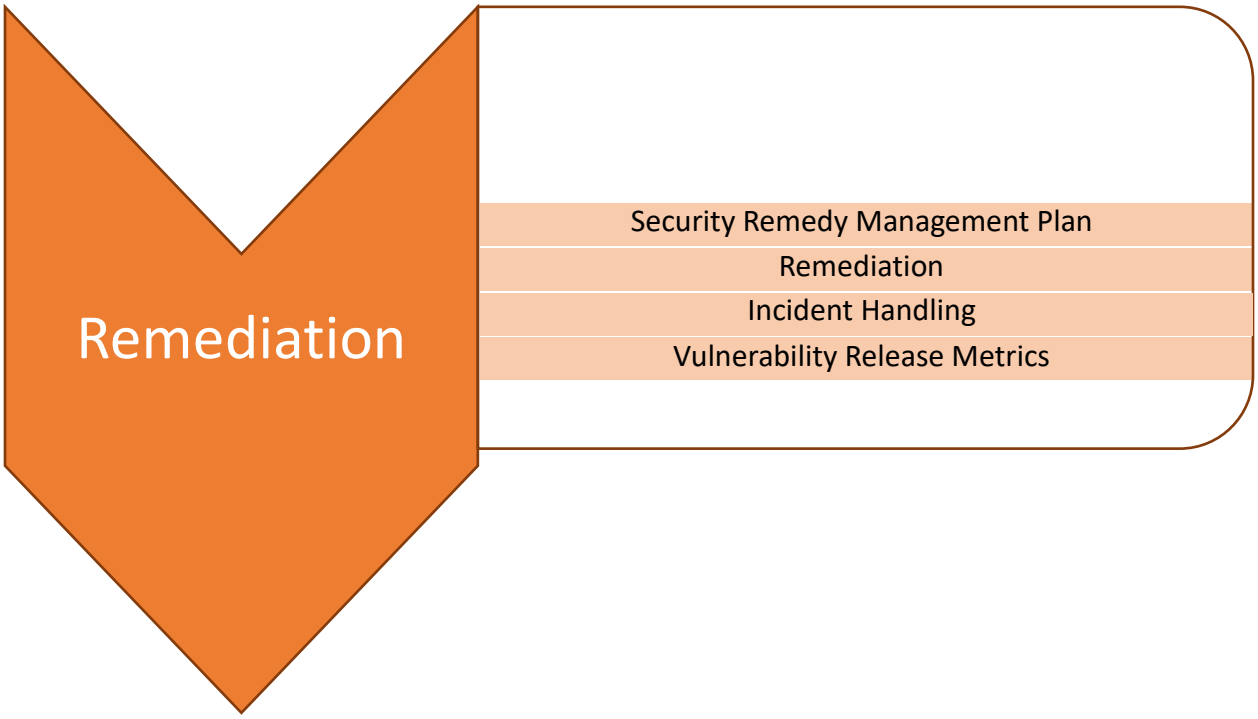
During reproduction, the team doing the analysis should work to determine which products are impacted and if any variants of the vulnerability exist. See also Product

Lifecycle Management section 4.1.1.

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

***Outcome**: Fixes for the vulnerability are comprehensive across supported products.*

Service Area 4



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

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

***Outcome**: Enable stakeholders and downstream vendors to plan accordingly for a remedy.*

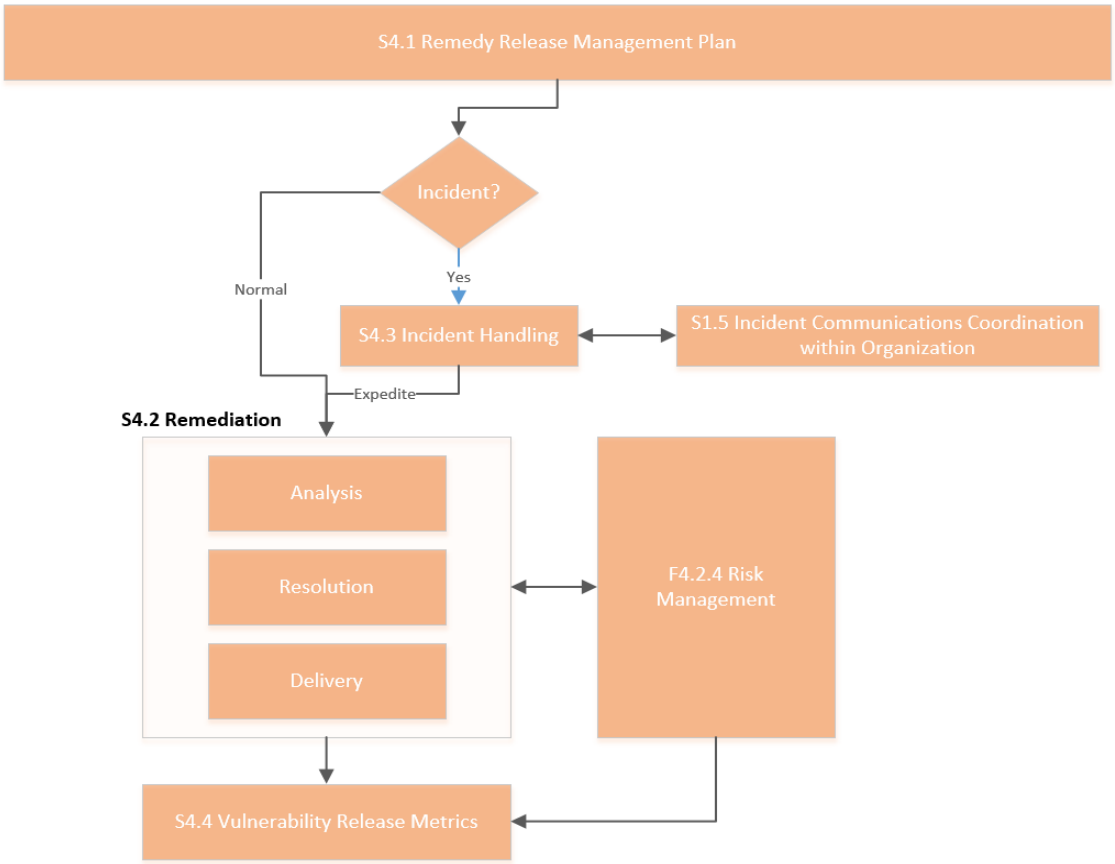


Figure 11: Example of a Core Remedy Release Process

Service 4.1 Remedy Release Management Plan

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

> ***Purpose**: Educate constituency on which products will be supported, mechanisms for delivering a remedy, and the cadence in which they will be delivered.*
>
> ***Outcome**: Stakeholders will be able to plan in advance for deployment of security fixes.*

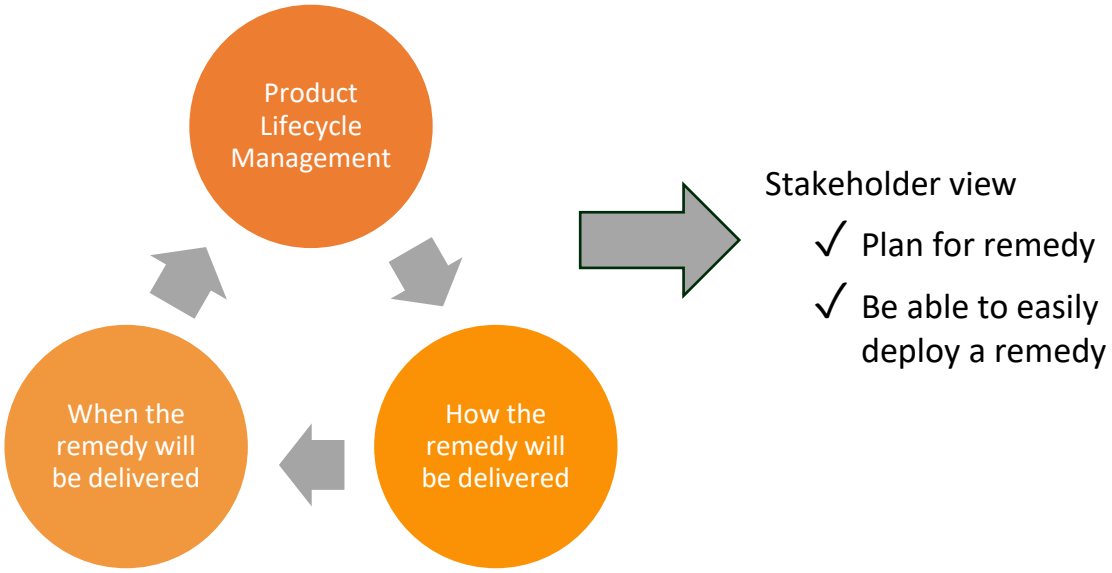


Figure 12: Setting the Foundation for Consistency

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 business 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 business 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 a remedy for those types of products.*

Sub-Function 4.1.1.1 Product Inventory

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 Support Models

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 Product Lifecycle

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 a remedy to stakeholders. The criteria for determining when to deploy a remedy 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 a remedy.*

Sub-function 4.1.2.1 Product Packaging Formats

Understand the different packaging formats relevant to delivering a remedy (e.g. binary executable, source code diffs, etc.).

Sub-function 4.1.2.2 Delivering a Remedy

Understand the different mechanisms for delivering a remedy such as hot fix, patch, maintenance releases, firmware updates, and how to distribute a remedy.

Sub-function 4.1.2.3 Deploying a Remedy

Identify across the different products how a remedy can be deployed, i.e. remotely, customer installable, automatic updates or requirements onsite.

Function 4.1.3 Delivery Cadence

Stakeholders and downstream vendors need to plan for a remedy so that they can maintain the security posture of their environment. By setting a cadence for when a remedy 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 a remedy is released to stakeholders.*

Outcome*: Stakeholders can plan and deploy the remedy.*

Sub-function 4.1.3.1 Remedy Delivery Cadence

Partner with product management teams and release management to determine the cadence for when a remedy should be delivered. Some remedies are integrated 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 Document Exceptions

Identify and document the exceptions for when a remedy 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. It also 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 remedy 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 remedy that is compatible with impacted products and stakeholder needs.*

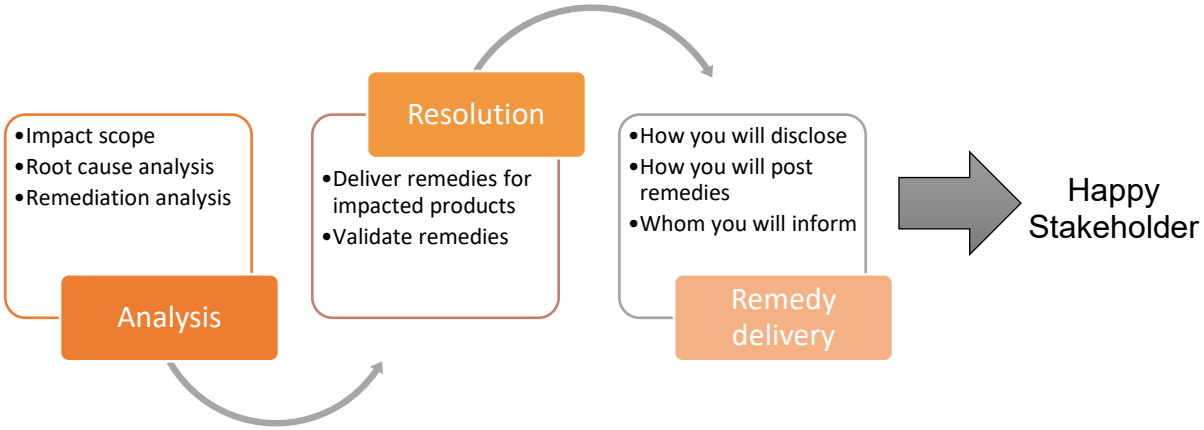


Figure 13: Remediation Process for the Reported Vulnerability

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 remedy that is compatible with impacted products and stakeholder needs.*

Sub-Function 4.2.1.1 Validate Vulnerability

Validate the vulnerability report or incident against the quality gate or bug bar. See Function 3.1.1 Quality Gate and Bug Bars.

Sub-function 4.2.1.2 Remediate Product Versions

Identify affected products and versions as well as any variants that may need to be

remediated at the same time.

Sub-function 4.2.1.3 Review Support Agreements

Review the support agreements and models associated with affected product versions. Refer to Sub-Function 4.1.1.2 Support Models.

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 Remedy Workarounds

Identify if there are any workarounds that can be implemented to mitigate the vulnerability while a remedy is under development.

Sub-function 4.2.1.8 Exceptions

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

Purpose: *Provide a process and a mechanism to internally validate the remedy 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 Reported Vulnerabilities that have been Remediated

Validate to ensure all instances of the reported vulnerability have been remediated across all affected product versions.

Sub-function 4.2.2.3 Remedy Signoff

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 Validate Remedy with Finders

Partner with third-party finder or stakeholder to validate the remedy.

Function 4.2.3 Remedy Delivery

As part of releasing a remedy for a reported vulnerability, the disclosure timeframes may vary depending on your organization's business requirements. For example, some disclosures may align to when the remedies are available, others may align the disclosure to come after the remedies have been released, particularly if the remedies have been staged, or in some cases the disclosures may be prioritized based on stakeholder relationships (for example partners or critical entities). Regardless, key stakeholders across the industry including the finder need to be kept informed of the timeframes.

Purpose: *Disclosures are planned in accordance with remedies and stakeholders are kept informed of those timeframes.*

Outcome*: Deliver a remedy 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 Post Remedy to Internal Database

Partner with stakeholder support or other stakeholders to post the remedy to the web portal, stakeholder support site or release to manufacturing (RTM) as examples.

Sub-function 4.2.3.4 Release Remedy Disclosure

Partner with stakeholder support or stakeholders to release the disclosure of the reported vulnerability.

Function 4.2.4 Risk Management Process

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 Service Level Agreements or Objectives). 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 SLA's 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 Authoritative Roles

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 Process

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 Risk

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 non-coordinated public disclosures. 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 remedy.

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 at risk and quick action is required.*

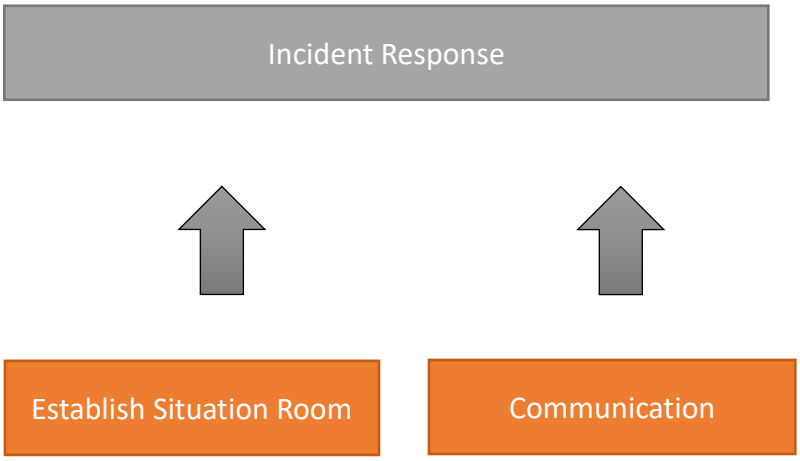


Figure 14: Incident Handling

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 or virtual location, 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 Incident Management Plan

Develop a plan to manage critical vulnerabilities and develop the ability to mobilize all the resources required to address them. It is important that incident response readiness is conducted to validate the preparedness of this plan to handle unexpected events and emergencies.

Sub-function 4.3.1.2 Identify Resources Required to Handle and Manage the Incident

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

Sub-function 4.3.1.3 Involve Stakeholders in Incident Response Plan

Identify all key stakeholders required to participate in handling the incident as part of your incident response plan. See Service 1.1 Internal Stakeholder Management

and Service 1.5 Incident Communications.

Sub-function 4.3.1.4 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 Analysis

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 Postmortem 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 the 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 Communicate Recovery Activities

Recovery activities are communicated to internal stakeholders, executives, and management teams.

Sub-function 4.3.3.4 Collect Incident Postmortem Feedback

Incident postmortem briefings are conducted by PSIRT, and feedback is collected to improve incident response as well as Security Development Library (SDL) activities (for example, what SDL activity could/should have prevented the issue in the first place?).

Service 4.4 Vulnerability Release Metrics

Data to be collected should include, but may not 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.*

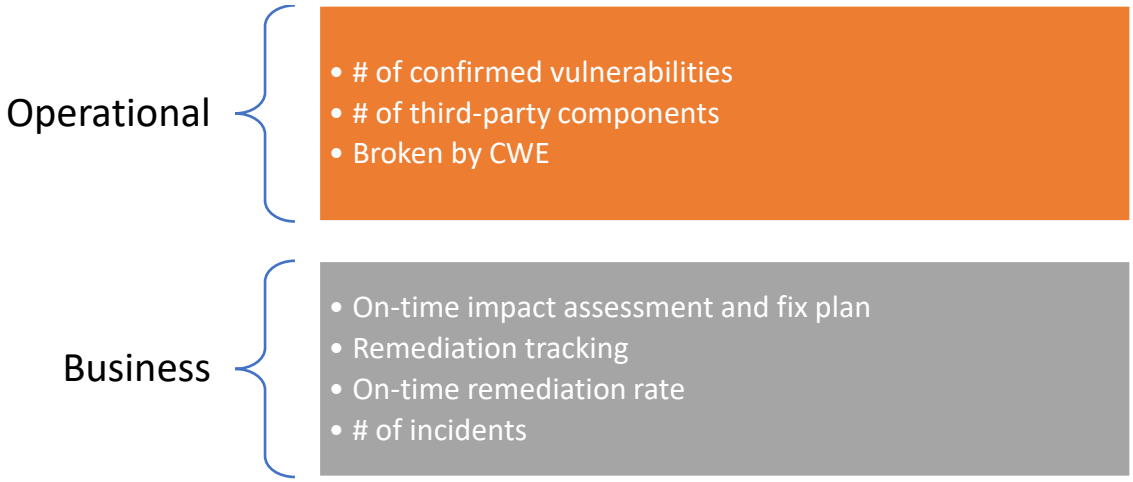


Figure 15: Operational and Business Metrics

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 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 vs. 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 product/BU)

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.

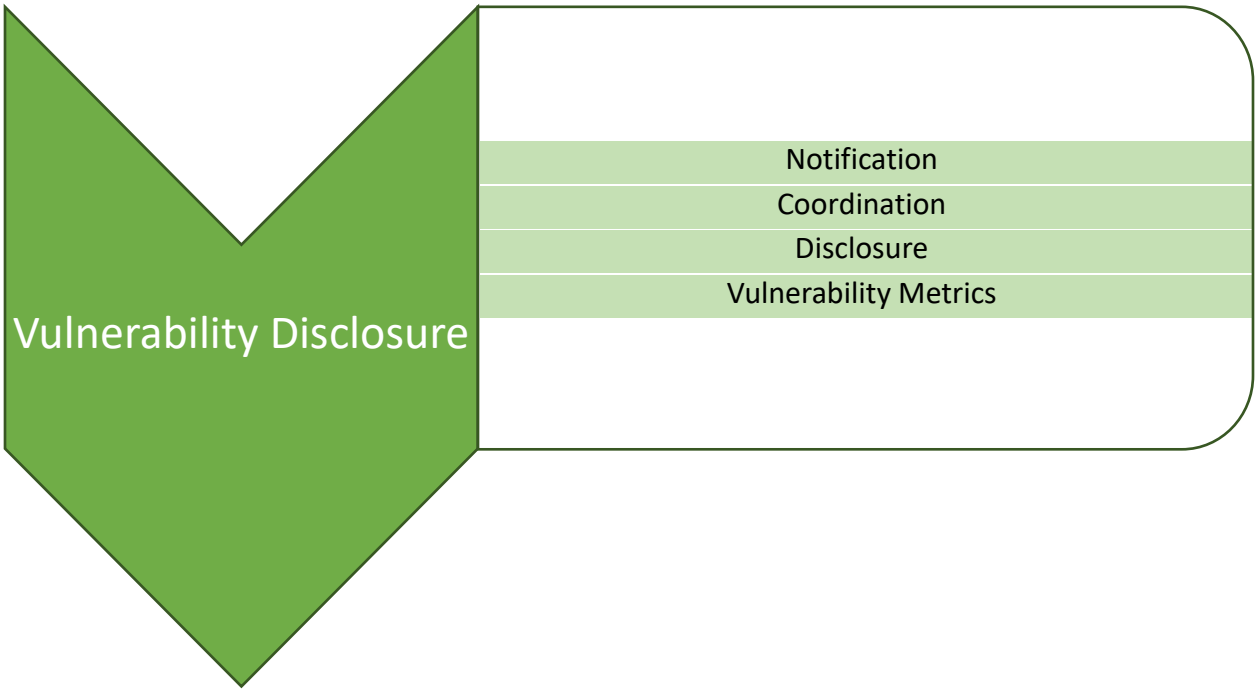
Sub-function 4.4.2.4 On-Time Remediation Rate

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



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.

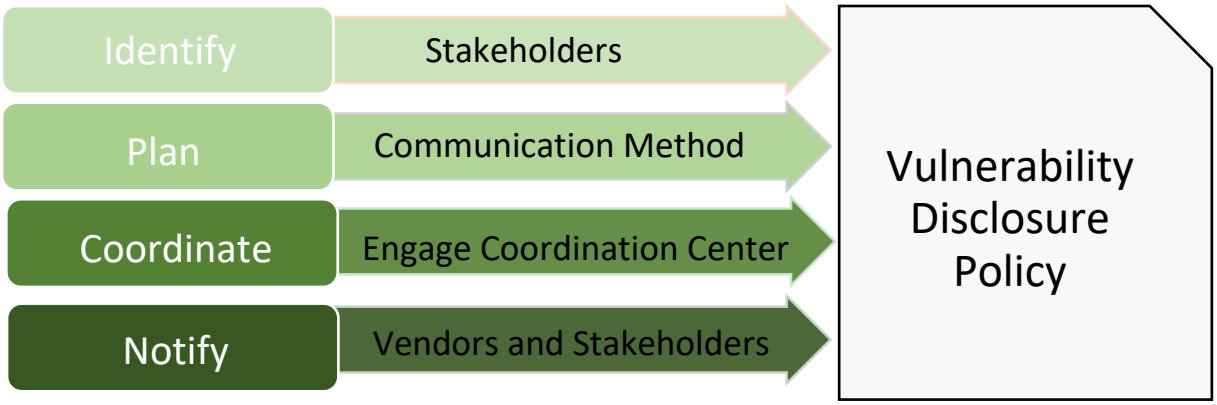


Figure 16: Vulnerability Notification Process

***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.*

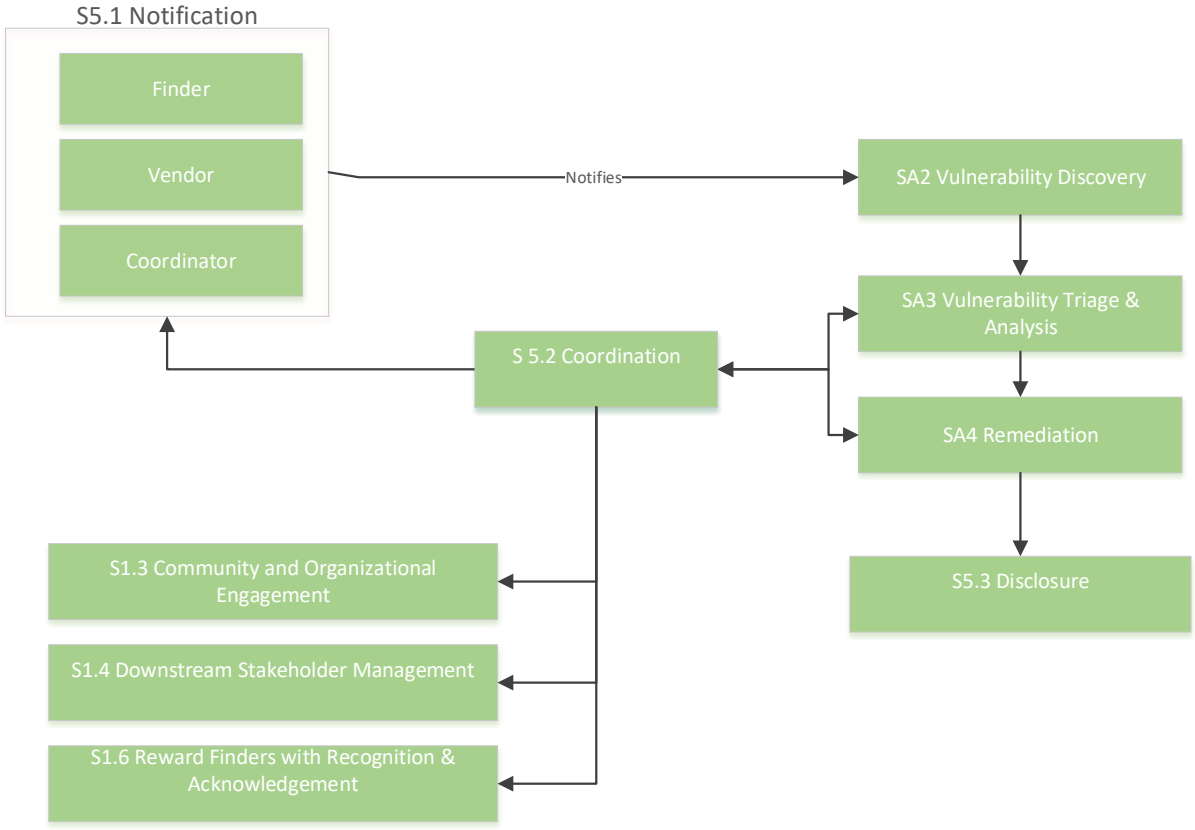


Figure 17: High-level example of Vulnerability Coordination

Service 5.1 Notification

This service involves determining the appropriate notification process to provide timely information about mitigation strategy, remedies, and workarounds to stakeholders so they are kept informed and can plan accordingly. In some cases, contractual agreements may exist between vendors – for example, an upstream vendor would be required to notify a downstream vendor of 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 aware of the vulnerability-handling policy of the different vendors. Sometimes these expectations are captured in a contractual agreement. The timeline for remediation and disclosure should be negotiated as soon as possible.

***Purpose**: Create an 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 PSIRT Reporting to Intermediate Vendors

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 Intermediate Vendor Reporting

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 Contractual Agreements

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 PSIRT Notification to Stakeholders

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

Function 5.1.2 Coordinators

A coordinator may be asked by a PSIRT to participate in notifying other vendors, as well as coordinating the timing of remedy for their advisories, especially if multiple vendors are involved. Coordinators such as the CERT Coordination Center (CERT/CC)[12] or third-party coordinators provide value by arranging for a multitude of different organizations to partner and collaborate on addressing a vulnerability.

***Purpose**: Coordinators may be asked to step in and assist the PSIRT 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 Coordinator Identification

[12] www.cert.org

Document and understand the different coordinators based on vulnerability disclosure policy.

Sub-function 5.1.2.2 Coordinator Engagement

Partner with a coordinator to ensure all affected vendor PSIRTs have 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 Service Area 2 Vulnerability Discovery.

***Purpose**: Create an 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 aware of the vulnerability handling policy of the vendor. Timelines for remediation and disclosure should be negotiated as soon as possible.

***Purpose**: Document the vulnerabilities that were removed from the product with the remediation.*

***Outcome**: Clarity regarding the benefit of implementing the remedy and where to find it.*

Function 5.2.1 Bilateral Coordination

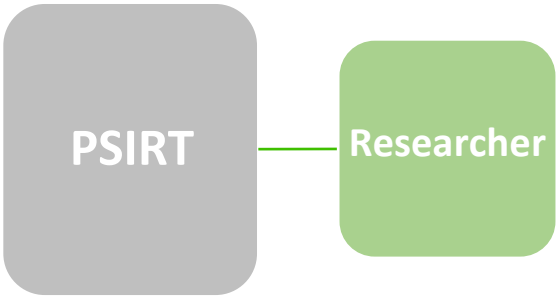


Figure 18: Bilateral Coordination

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, in order to promote and facilitate a coordinated 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 Report Receipt

Acknowledge receipt of vulnerability report from third-party finder.

Sub-function 5.2.1.2 Regular Updates

Provide the finder with regular updates on the status of the reported vulnerability.

Sub-function 5.2.1.3 Validation by Finder

Provide the remedy to the finder so they can validate it as well.

Sub-function 5.2.1.4 Finder Acknowledgement

Provide credit by acknowledging the contributions of the finder who reported the vulnerability. Vendor should verify with the finder that the credit is acceptable.

Function 5.2.2 Multi-Vendor Coordination

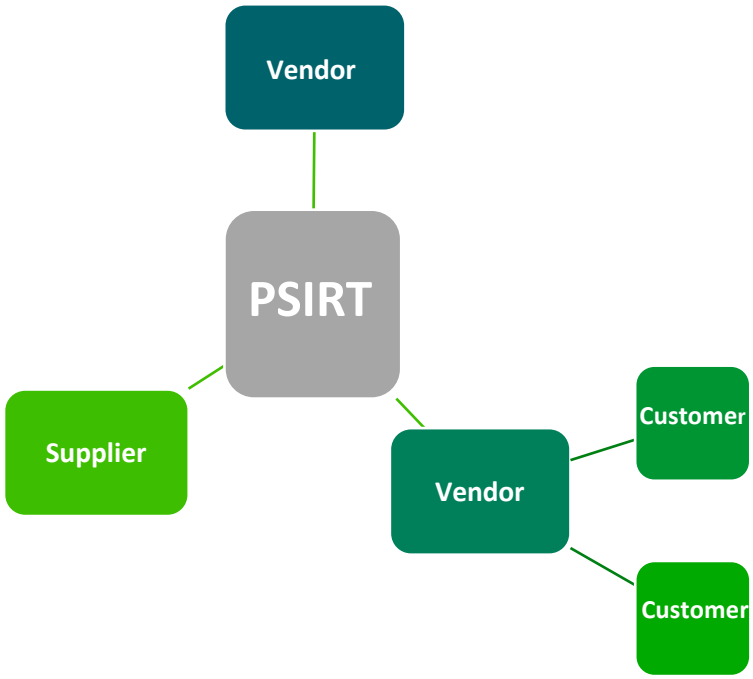


Figure 19: Multi-Vendor Coordination

Where appropriate, a vendor PSIRT should make arrangements for sharing vulnerability information with coordinators or other vendors. They should be aware of the vulnerability handling policy of the vendor. Timelines for remediation 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 remediation.*

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

Multi-Party Stakeholder	Relationship to Self	Stake in Coordination
Upstream Vendors	OEM supplier provides technology.	To provide a remedy it is recommended upstream vendors manage their downstream stakeholders (see Service Area 1.4).
Downstream Vendors	Receives technology from upstream vendor.	To be notified to apply the security remedy. It is recommended that downstream vendors define and engage with upstream vendors communities and partners (see Function 1.3.1).

Table 1: Example of Multi-Party Coordination

Sub-function 5.2.2.1 Report Receipt

PSIRT vendor acknowledges receipt of the vulnerability report from vendor or coordinator.

Sub-function 5.2.2.2 Affected Vendor Identification

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

Sub-function 5.2.2.3 Vulnerability Information Sharing

PSIRT vendor or coordinator shares vulnerability information across the different vendors.

Sub-function 5.2.2.4 Remedy Release Planning

PSIRT vendor or coordinator partners with vendors on the timing and availability of remediations, and how the downstream vendors may receive the remedy.

Sub-function 5.2.2.5 Remedy Validation

PSIRT vendor or coordinator validates with vendors that the security remediation addresses the vulnerability.

Sub-function 5.2.2.6 Disclosure Coordination

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 remediation is released, there should be appropriate disclosures to ensure that stakeholders and vendors are properly notified of the remedy. 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 remediations.*

***Outcome**: Clarity regarding what remedies have been made to the code and where to find them.*

Function 5.3.1 Release Notes

Release notes, including readme and change history, should include CVE reference(s) for the remedy. Release notes should clearly communicate how the vulnerability was addressed.

***Purpose**: Provide indication of remedies included in the updated code.*

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

Sub-function 5.3.1.1 Release Note Disclosure

Define what vulnerabilities should be disclosed in the release notes.

Sub-function 5.3.1.2 Release Note Review

Define the review process.

Sub-function 5.3.1.3 Release Note Approvals

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 Advisory Template

Define a standardized security advisory template. Include title, summary, CVE(s), supported product impact and status, acknowledgement, references and revision history.

Sub-function 5.3.2.2 Advisory Delivery Method

Determine the mechanism to deliver the security advisory including, but not limited to web document, RSS feed, or subscription.

Sub-function 5.3.2.3 Advisory Formatting

In order for stakeholders and constituents to consume advisories using automation tools, consider publishing advisories in a machine-readable format such as the Common Security Advisory Framework [13](CSAF).

Sub-function 5.3.2.4 Advisory Triggers

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 remedied (breach scenario).

Sub-function 5.3.2.5 CVE Assignment

Determine the process for assigning a CVE ID to the vulnerability.

Sub-function 5.3.2.6 Finder Acknowledgement

Determine if the finder would like public acknowledgment or credit.

Sub-function 5.3.2.7 Disclosure Planning

Define review process such as who are the stakeholders and when should the disclosure be crafted.

Sub-function 5.3.2.8 Advisory Review Process

Conduct review process with defined stakeholders.

Function 5.3.3 Knowledge Base Articles

Vendor should have a mechanism to publish knowledge base articles which may accompany certain security remedies 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 Knowledge Base Article Disclosure

Define what vulnerabilities should be disclosed in a knowledge base article.

Sub-function 5.3.3.2 Knowledge Base Article Review

Define the review process.

Sub-function 5.3.3.3 Knowledge Base Article Approvals

[13] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf

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 FAQs 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 the media asking questions on day of advisory publication, enabling the message to be controlled.*

Sub-function 5.3.4.1 Internal Stakeholder Engagement

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, remediation timeline, affected products or services.

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

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

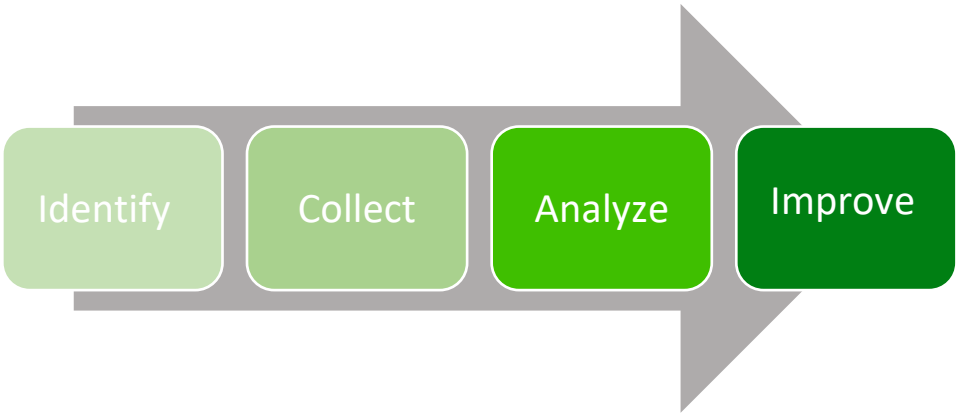


Figure 20: Vulnerability Metrics Process

Function 5.4.1 Operational Reports

Operational reports may provide additional information on the volume of disclosures posted as well as the number of page views. These reports should 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 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 the team to have a technical resource assigned.

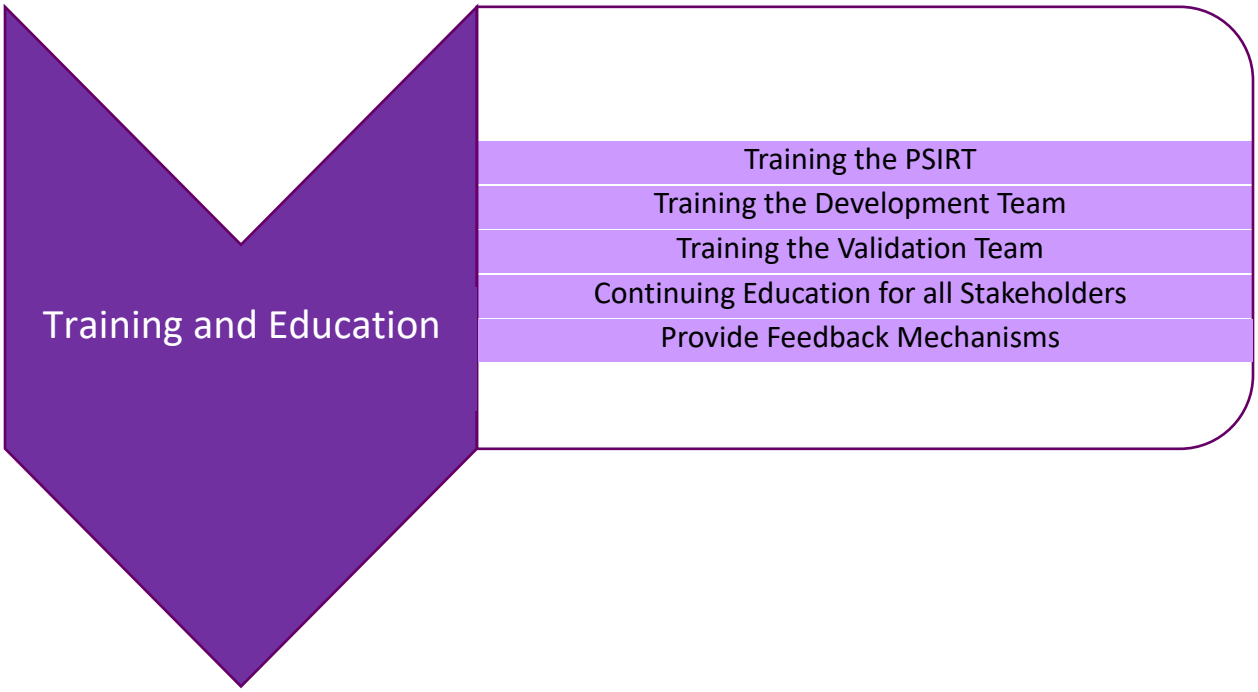
Sub-function 5.4.1.2 Number of CVEs Posted to NVD

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 towards proactive notification if the volume of stakeholders viewing your advisory is low.

Service Area 6



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. PSIRTs play 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 down 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 such as legal, communications, and development.

2) **Product Development** (Internal Engineering and Development): Developers require training in their specific areas 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 aspects such as 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 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 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 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

PSIRT staff need to be at the forefront of what is happening in the world of security including, but not limited to, what's trending, new exploits, and industry activities. 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.

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 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 staff have sufficient technical training to perform their duties.*

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 PSIRT staff are 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 follow 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 staff 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 staff will be sufficiently trained on internal processes so that they can perform their duties.*

Function 6.1.4 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 staff will be sufficiently trained and knowledgeable on tools so 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 it. 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 remedy. 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 that the vulnerabilities can be tracked and released in these components.*

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

Function 6.1.5 Tracking all Training Initiatives

PSIRTs 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 changes very rapidly, and hence the trainings and processes will need to be continually redefined.

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

Outcome: *PSIRT staff 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 [14]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 concerned 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. Document information such as who was the security architect, the development lead, and the testing lead so that the PSIRT can go back to those who know the most to assess risks and develop mitigations. This documentation should also include aspects such as: what are the third-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 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 aspects 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 should encourage the organization to have a group that focuses on this.

[14] https://www.microsoft.com/en-us/sdl/

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 also need to 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 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 timelines involved.*

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

Function 6.4.3 Training the Government Affairs and Compliance Team

Government affairs personnel 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 that PR can be involved if any external posting is 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 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 the vendor's website to make it easily visible to stakeholders. PSIRTs typically maintain a close relationship with support so they understand the kind of issues that are being reported by customers. Sometimes a finder might also be a customer, so handling the issue may move between support and PSIRT.

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

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

Service 6.5 Provide Feedback Mechanisms

Use information gained during the root cause analysis of the incident to educate those involved and prevent similar vulnerabilities in the future.

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

Outcome: *Higher-quality training will result in an improved experience for all stakeholders.*

Annex 1: Supporting Resources

[15]Architecture Content Framework

[16]ISO 31000:2009 Risk management – Principles and guidelines

ISO/IEC 27000/2018 Information technology – Security techniques – Information security management systems

[17]ISO/IEC 30111:2013 Information technology – Security techniques – Vulnerability handling processes

[18]ISO/IEC 29147:2014 Information technology – Security techniques – Vulnerability disclosure

[19]Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure

The Project Management Body of Knowledge (PMBBOK) Guide and Standards

[15] http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html

[16] https://www.iso.org/iso-31000-risk-management.html

[17] https://www.iso.org/obp/ui/#iso:std:53231:en

[18] https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en

[19] https://www.first.org/global/sigs/vulnerability-coordination/multiparty/FIRSTMultiparty-Vulnerability-Coordination-v1.0.pdf

Annex 2: Acknowledgements

- Barbara Cosgriff, MetLife
- Beverly Finch, Lenovo
- Carl Denis, Siemens
- Chris Robinson, Red Hat
- Jeff Hahn, Honeywell
- Jerry Bryant, Microsoft
- Josh Dembling, Hikvision
- Jean-Robert Hountomey, Brocade
- Kevin Ryan, NetApp
- Krassimir Tzvetanov, Fastly, Inc.
- Langley Rock, Red Hat
- Lisa Bradley, Nvidia
- Pete Allor, Honeywell
- Reshma Banerjee, Oracle
- Rupert Wimmer, Siemens
- Steve Brukbacher, Johnson Controls
- Tania Ward, Dell EMC
- Vic Chung, SAP

Annex 3: Tables and Illustrations

Annex 4: Pros and Cons of PSIRT Organizational Models

Model	Description	Pros	Cons
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 5: 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 is also generally 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 a 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 description 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 FIRST 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.

- **Common Vulnerability Exposures (CVE**) - [20]is a list of entries containing an identification number, a description, and at least one public reference for publicly known vulnerabilities. It serves as a standard identifier to reference vulnerabilities.

- **Common Vulnerability Scoring System (CVSS)** - [21]a numerical score that reflects a vulnerability's severity.

- **Common Weakness Enumeration (CWE)** - [22]a formal list of software weakness types created to:

  - serve as a common language for describing software security weakness in architecture, design, or code.
  - serve as a standard measuring stick for software security tools targeting these weaknesses.
  - provide a common baseline standard for weakness identification, mitigation, and prevention efforts.

- **Health Insurance Portability and Accountability Act (HIPPA)** - [23]a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health-care providers.

- **Key Performance Indicators** - [24]a measurable value that demonstrates how effectively a company is achieving key business objectives. Organizations use KPIs at multiple levels to evaluate their success at reaching targets.

- **Maturity** - how effectively an organization executes a particular capability within the mission and authorities of the organization. It is a level of proficiency attained either in executing specific functions actions or tasks, or in an aggregate of functions or services. The ability of an organization will be determined by the extent, quality of established policies and

[20] https://cve.mitre.org/
[21] https://www.first.org/cvss/
[22] https://cwe.mitre.org/about/index.html
[23] https://www.medicinenet.com/script/main/art.asp?articlekey=31785
[24] https://www.klipfolio.com/resources/articles/what-is-a-key-performance-indicator

documentation, and the ability to execute a set process.

- **Payment Card Industry Data Security Standard (PCI DSS)** - [25]an information-security standard that promotes the safety of cardholder data across the globe.

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

[25] https://www.pcisecuritystandards.org/pci_security/