enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

HOW TO SETUP UP CSIRT AND SOC

GOOD PRACTICE GUIDE

DECEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For queries in relation to this study, please use: csirt-relations@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Edgars Taurins, ENISA.
Activities supporting this study were conducted under contract with NRD Cyber Security.

ACKNOWLEDGEMENTS

Study was performed with the input from Informal Expert Group on EU Member States Incident Response Development.

LEGAL NOTICE

Copyright notice

ISBN 978-92-9204-410-7 - DOI 10.2824/056764

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This publication provides results-driven guidance for those who are interested in establishing a computer security incident response team (CSIRT) or security operations centre (SOC), and guidance on possible improvements for different types of CSIRTs and SOCs that exist currently.

The content of this report is based on an analysis of current publications on the establishment of CSIRTs (the analysis is summarised in Annex B); a field questionnaire (Annex A), which was completed by 40 CSIRTs and SOCs; and the authors' experiences in establishing and improving CSIRTs as part of numerous projects carried out in Europe, Asia, Africa and South America.

A results-driven approach is taken throughout the publication to provide guidance on the different stages involved in the establishment of a CSIRT or SOC organisation:

- Assessment for readiness
- Design
- Implementation
- Operations
- Improvement.

The reader will receive practical guidance on what to focus on during the individual phases of establishment and improvement.

Up to July 2020, ENISA had published 61 reports and 21 translated versions of reports supporting CSIRTs on its website ([1]). ENISA's training package ([2]) provides online training materials, training courses and exercise materials for cybersecurity specialists, based on the 'Train the Trainer' philosophy. This document aims to enhance ENISA's existing body of knowledge on the establishment of CSIRTs.

[1] https://www.enisa.europa.eu/publications#c8=CSIRTs
[2] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/

1. INTRODUCTION

1.1 CONTEXT OF THE WORK

Cybersecurity threats are increasing and becoming more complex. One of the most effective ways to counter these threats is by creating a global ecosystem of computer security incident response teams (CSIRTs) and security operations centres (SOCs) that can communicate, share information and respond to cyberthreats effectively. This can be facilitated by providing relevant frameworks and increasing the number of CSIRTs and SOCs around the world and the maturity of existing CSIRTs and SOCs.

A more mature ecosystem of CSIRTs and SOCs enables better cooperation and collective actions to respond to cyber security threats

In Europe, ENISA is assisting Member States with their incident response capabilities by providing them with various resources, such as documents, tools, materials and guidance. For example, ENISA hosts a European CSIRT inventory – an interactive map on ENISA's website that gives an overview of publicly listed CSIRTs in Europe. In addition, the *Study on CSIRT landscape and IR capabilities in Europe 2025*[3] looks at the overall status of CSIRTs' incident handling and response capabilities, while the *EU Member States incident response development status report*[4] provides an insight into the NIS Directive[5] (Directive (EU) 2016/1148 on security of network and information systems) sectoral incident response capabilities. ENISA has also carried out work in the field of national and governmental CSIRTs' capabilities and incident response capabilities, including providing training material covering some aspects of the development of CSIRTs.

To provide additional resources, a decision was made to publish guidelines and produce an interactive online information repository to guide the establishment of different types of CSIRTs and SOCs by building on the existing work of ENISA, especially in the areas of maturity and training.

1.2 OBJECTIVES OF THE WORK

This publication provides results-driven guidance for those who are interested in establishing a CSIRT or SOC or modernising a CSIRT or SOC in a structured way.

A results-driven approach is taken throughout the publication to provide guidance on the different stages involved in the establishment of a CSIRT organisation: assessment for readiness, design, implementation, operation and improvement.

The expectation is that the reader will use this publication as a practical guide during the individual phases involved in the establishment of CSIRTs. Readers may be stakeholders of CSIRTs that are to be established.

This report aims to encourage the establishment of CSIRTs and SOCs and provide practical techniques to ensure that the establishment and improvement process is effective.

[3] https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025
[4] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

1.3 OVERVIEW OF THE METHODOLOGY

Existing documents on CSIRT establishment focus on activities to do, without elaborating much on the resulting outcome. This publication aims to build a recurring process of improvement and related deliverables during the growth and development of a CSIRT. It was designed in a way that provides guidance for all CSIRTs no matter what development stage they are in or their current maturity.

To achieve this result data gathering methods such as analysis of current publications on the establishment of CSIRTs (the analysis is summarised in Annex B); a field questionnaire aimed at established CSIRTs and SOCs (Annex A); and the authors' and reviewers' practical experience in establishing and improving CSIRTs, were used. The objective was to make this publication as close to real life as possible. For this reason citations from various CSIRT teams as well as realistic costing and timing were included.

FIRST.org CSIRT Services Framework, as well as SIM3 assessment model are referred to as companions in the process because they are widely respected when defining an initial service catalogue for new CSIRT teams and for the assessment and development of CSIRT maturity.

1.4 DEFINITIONS OF CSIRT AND SOC

The most common terms used to describe the teams responsible for incident response handling are CSIRT, CERT([6]), and SOC.

1.4.1 Computer security incident response teams

The term CSIRT, or computer security incident response team, was established in the 1990s. CSIRTs are also known as CIRTs (Computer incident response teams), CERTs (Computer emergency response teams), SIRTs (Security incident response teams) among others. National teams may also be called national cyber security centres (NCSCs), which by law are usually assigned the CSIRT role as well as providing additional services for the nation (e.g. handling a country's information classification schemes). Each team chooses its name based on the preference of the organisation.

CSIRT has become a generic name for a team that provides a set of services: information and cybersecurity incident handling (core service), security monitoring, vulnerability management, situational awareness and cybersecurity knowledge management.

In simpler terms, a CSIRT[7] is a team that is assigned to handle computer security (thus, often, cybersecurity) incidents. Often this includes additional responsibilities, from detection to analysis, and even hands-on fixing, as well as different situational awareness, knowledge transfer and vulnerability management activities. Over the years, the role of a CSIRT has evolved from providing incident monitoring and handling services to coordinating and communicating with different stakeholders, countries and specific sectors.

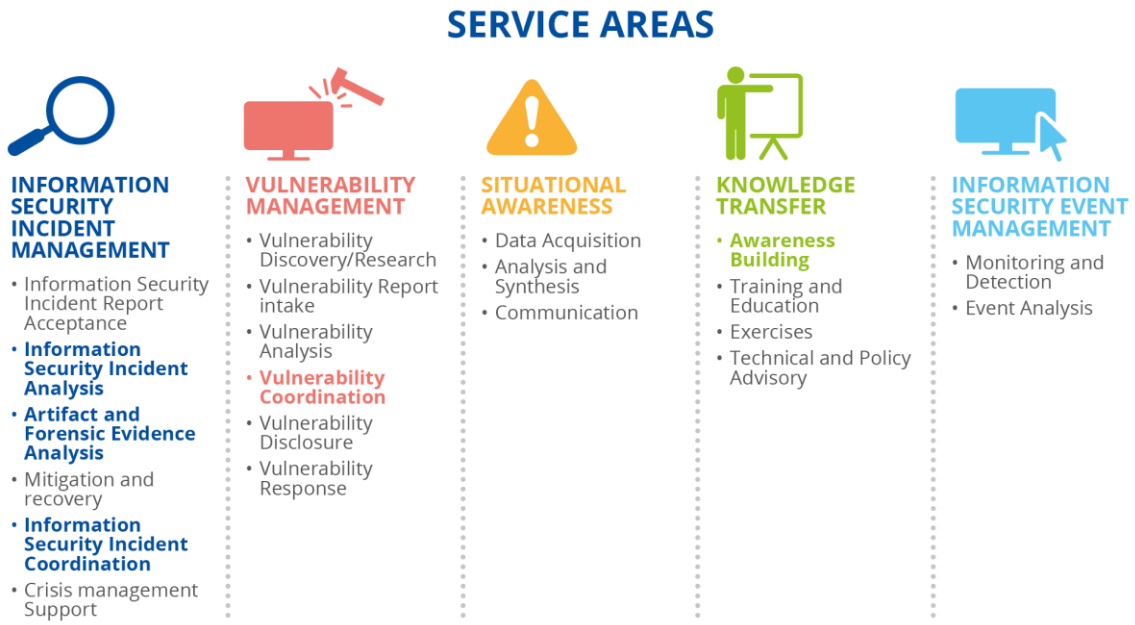
Currently, FIRST.org hosts and continuously improves a CSIRT Services Framework ([8]), which is a high-level document that describes the activities carried out by CSIRTs. These activities are organised into five main service areas, which are further split into services, functions and sub-functions. A CSIRT can choose which of the services and functions are relevant to their mandate and organise them into their own services structure. Although this framework does not define a SOC framework, services from some of the areas can also be applicable to SOC

[6] CERT, or computer emergency response team, is the oldest term and has been trademarked by the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU).
[7] See CSIRT definition for example at "Baseline capabilities for national / governmental CERTs" https://www.enisa.europa.eu/publications/baseline-capabilities-for-national-governmental-certs
[8] https://www.first.org/standards/frameworks/csirts/csirt_services_framework

teams. The CSIRT Services Framework is supported by ENISA, the International Telecommunications Union (ITU) and many other organisations.

Typically, a minimal set of services for CSIRTs usually includes those those in bold below in accordance with the FIRST services framework.

Figure 1: FIRST services framework – typical CSIRT services



1.4.2 Security operations centres

A SOC, or security operations centre, provides an incident detection service by observing technical events in networks and systems and can also be responsible for incident response and handling. In large enterprises, SOCs sometimes focus only on monitoring and detection services and then hand over incident handling to a separate CSIRT. In smaller organisations, CSIRTs and SOCs are often considered to be synonymous.

Typically, SOC teams operate from SOC rooms, where analysts sit at their workstations in front of a video wall that projects a summary of the current situation (Figure 2). SOC teams typically evolve from information technology (IT) security teams automating their work using security information and event management (SIEM) and other security automation and orchestration technology for security monitoring. SOC teams usually focus their key performance indicators (KPIs) around quality indicators – detection speed, detection breadth, coverage, false-positive rates – as well as incidents handled, the ratio of alerts/events/incidents, number of escalations and workload per incident.

'SOC is the first line, they receive all alerts, whereas IRT would only receive escalated alerts or be involved in the coordination. SOC is the responsibility of our members as we are a sector CERT'
(sectorial CSIRT)

Figure 2: Multi-State Information Sharing & Analysis Center (MS-ISAC) SOC room.
Source: MS-ISAC website (https://www.cisecurity.org/ms-isac/)

As well as operating physically, SOCs can consist of virtual and outsourced staff, or a hybrid model of internal and outsourced staff. It is common practice that, over time, SOCs alternate between outsourced and internal operations.

As both CSIRT and SOC organisations adhere to the same CSIRT Services framework, both CSIRTs and SOCs are referred to this report as CSIRTs.

Typically, a minimal set of services for SOCs usually includes those in bold below in accordance with the FIRST services framework.

Figure 3: First service framework – Typical SOC services

1.5 PREVIOUS ENISA WORK ON THE TOPIC OF CSIRTS

Up to July 2020, ENISA had published 61 reports and 21 translated versions of reports about CSIRTs on its website ([9]).

The foundational document on the establishment of a CSIRT is the *CSIRT Setting up Guide* ([10]), published in 2006. It was translated into more than 20 languages, including Chinese and Hindi. This 86-page publication covers the step-by-step process of creating a CSIRT and is still valid today.

'ENISA has excellent publications which are well organised and easy to read and understand'
(Unicom CSIRT)

ENISA's *Good Practice Guide for Incident Management* ([11]), published in 2010, provides guidelines for establishing incident handling management structures and capabilities; it can be used as a reference for establishment topics including incident handling processes and workflows.

ENISA's training package ([12]) provides online training materials, training courses and exercise materials for cybersecurity specialists, based on the 'Train the Trainer' philosophy.

ENISA has also published a body of knowledge for national and governmental CSIRTs on, for example, baseline capabilities ([13]) and maturity profiles ([14]), as well as a self-assessment tool.

In the past few years, ENISA has published a guidance document on CSIRT and law enforcement partnerships ([15]), including an analysis of partnership models, technical cooperation, electronic evidence analysis ([16]) and training modules. In addition, further information on how to choose a CSIRT cooperation model and the technical implementation of cooperation models is available from the ENISA website.

'Most of the publications and guidance from ENISA is relevant to our effective work. ENISA threat landscape is used to set our threat baseline every year'
(BGD e-GOV CIRT)

This report aims to enhance ENISA's existing body of knowledge on the establishment of CSIRTs. The content of this report is based on an analysis of previous publications on the establishment of CSIRTs (the analysis is summarised in Annex B); a field questionnaire (Annex A), which was completed by 40 CSIRTs and SOCs; and the authors' experiences in establishing and improving CSIRTs as part of numerous projects carried out in Europe, Asia, Africa and South America.

[9] https://www.enisa.europa.eu/publications#c8=CSIRTs
[10] https://www.enisa.europa.eu/publications/csirt-setting-up-guide
[11] https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[12] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/
[13] https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities
[14] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
[15] https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation
[16] https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders

2. GUIDELINES FOR ESTABLISHING CSIRTS

2.1 ORGANIZATION OF THE GUIDELINES

The guidelines for establishing CSIRTs are organised according to the different phases of the CSIRT establishment ([17]) process:

- Assessment for readiness
- Design
- Implementation
- Operations
- Improvement.

Figure 4: Lifecycle of CSIRT

The establishment of a new CSIRT starts with the 'assessment for readiness' phase, which begins with a discussion about the reasons and necessity for establishing a CSIRT and ends with the approval of an initial budget and shaping requirements for the design phase.

During the 'design' phase, detailed plans for the implementation phase are developed.

The 'implementation' phase covers organisational matters: governance, people, processes, services and technology.

In the 'operations' phase, a CSIRT delivers the CSIRT services.

Existing CSIRTs can follow the guidelines from the 'improvement' phase rather than from the 'assessment for readiness' phase.

During the 'improvement' phase, a CSIRT formulates requests for improvements, prioritises initiatives and receives an approved budged for following the 'design–implementation–operation–improvement' cycle.

[17] In this report 'establishment' refers to a CSIRT's path from a conceptual idea to a strong and mature CSIRT several years later or to advancing an existing CSIRT into further development stages.

These guidelines are organised based on the outcomes of each phase.

1. Assessment for Readiness

- Preliminary Mandate
- Governance Structure
- Identification of the CSIRT hosting organisation
- High-level roadmap and budget
- Detailed Requirements for the Design Stage

2. Design

- Approved Detailed Mandate
- CSIRT Services Plan
- CSIRT Processes and Workflows Plan
- CSIRT Organisation, Skills and Training Structure Plan
- CSIRT Facilities Plan
- CSIRT Technologies and Processes Automation Plan
- CSIRT Cooperation Plan
- CSIRT IT and Information Security Management Plan
- Detailed Requirements for the Implementation Stage

3. Implementation

- Approved and implemented organisational structure
- Hired and appointed people
- Executed training plan for the staff roles
- Prepared facilities
- Developed and Implemented detailed processes and procedures
- Implemented technology for the automation of processes
- Implemented IT and information security management procedures
- Trained people for CSIRT operations
- Signed relevant agreements with the constituency, stakeholders and partners
- CSIRT services Test run and Tuning of results
- CSIRT Launch Communication and Celebrations

4. Operation

- Measured KPIs
- Annual Operations Performance Review
- Annual Stakeholder Needs Review
- Approval Annual Budget
- Collected Requirements for Improvement

5. Improvement

- List of chosen Initaitves for improvement
- Detailed Requirements for Improvement for Design Stage
- Preliminary budget for Improvement

Figure 5: Summary of CSIRT establishment outcomes

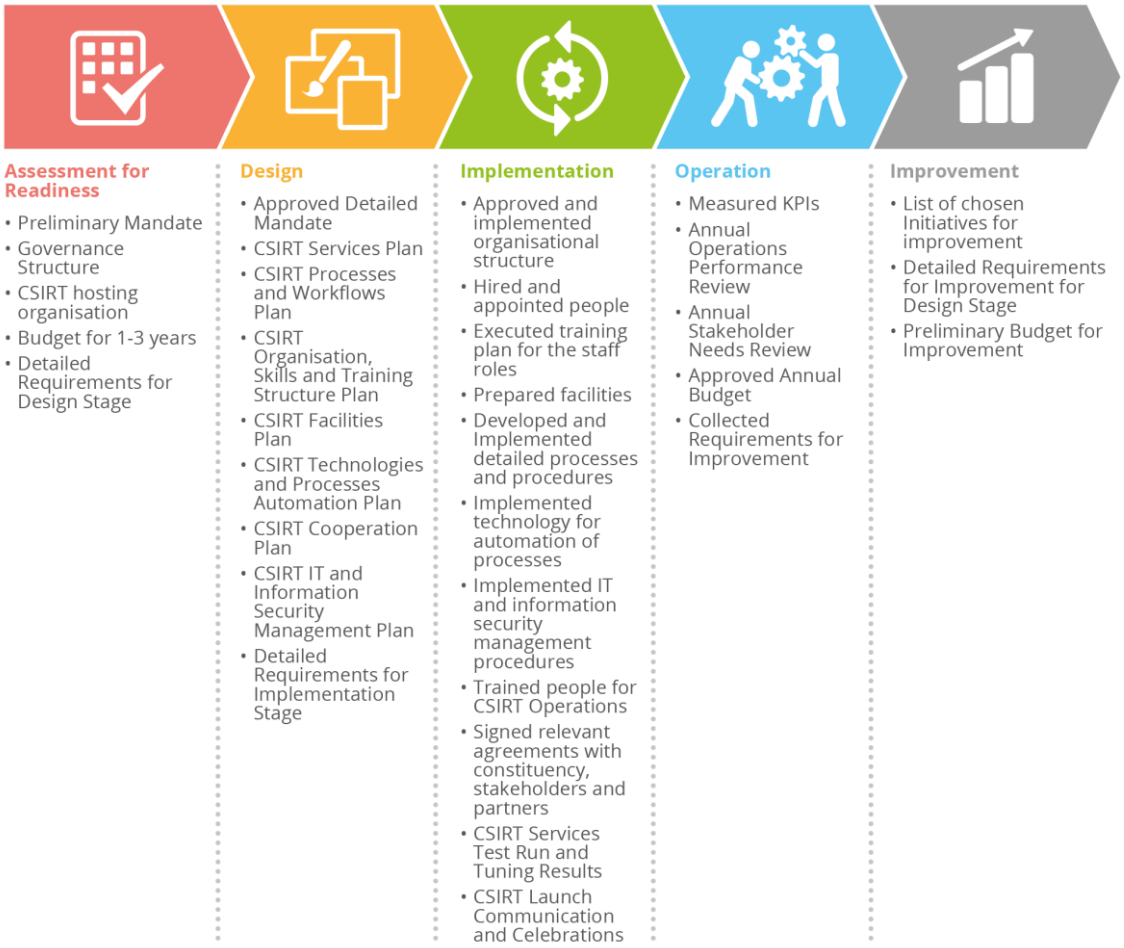


Figure 6: Sample of CSIRT establishment phases and required efforts

Figure 6 shows a timeline for CSIRT establishment, the expected internal and external resources needed, and the intensity of work required for the different roles involved in each phase.

The percentages in Figure 6 represent the workload/time required for the different roles. For example, '1 x Project manager 50 %' means that one project manager is required and that the required tasks will take up to 50 % of their maximum workload/time.

2.2 ASSESSMENT FOR READINESS

In the assessment for readiness phase, the following outcomes are expected.

- Preliminary mandate
- Governance structure
- Identification of the CSIRT hosting organisation
- High-level roadmap and budget
- Detailed requirements for the design stage

Figure 7: Implementation phases

2.2.1 Preliminary mandate

A CSIRT begins with a purpose – the initial idea and reasons why a CSIRT is needed. The establishment of a CSIRT must be justified.

The expectations of stakeholders and constituencies should be carefully considered before deciding to establish a CSIRT. In practice, this means considering the following aspects.

1. Identifying all major stakeholders and understanding their needs and expectations of a CSIRT. Depending on the stakeholder, their needs can include identification of incidents, security awareness, resolution of incidents and compliance with certain standards.
2. Identifying constituencies. This could be a small group of companies for a sectorial CSIRT, the residents of a city or even a whole country. Evaluating and meeting the needs and expectations of a specific constituency are extremely important for the success of a CSIRT.

A series of workshops should be planned with the main stakeholders and representatives of constituencies in order to obtain their support for the establishment of a CSIRT and to start a conversation about the real value that a CSIRT could bring. This can then be used as input for justifying the establishment of a CSIRT and for its mandate and budgeting.

Common justifications for establishing a CSIRT include:

1. The need to organise cybersecurity incident handing in a professional way to minimise the impact of incidents.
2. The need to have a professional team to respond to cybersecurity incidents using internationally accepted incident handling methods.
3. The need to be trusted by other CSIRTs around the world during incident investigations.
4. The need to have a coordinating team for cybersecurity incident handling, vulnerability handling, situational and security awareness rising and analysis of threats.

A team's purpose is determined in a CSIRT mandate, which must include the authority and responsibilities given to the team.

A mandate usually includes:

1. The authority given to a CSIRT to serve and act in a constituency.
2. The responsibilities of the CSIRT.
3. Requirements, objectives and tasks.

For a CSIRT with internal-only constituencies in an organisation or a managed security service provider (MSSP) set-up, the mandate is usually expressed in a single document of one of the following types:

1. An office order (in a government agency).
2. A decision or resolution by the board or executive management (in a private enterprise).

For sectoral or national CSIRTs, the mandate is usually expressed in at least two documents, namely:

1. A cybersecurity strategy, law or by-law, or government order assigning authority and overall responsibility (the only way to establish authority over a country's different organisations).
2. An office order of the CSIRT hosting organisation, outlining the detailed requirements, objectives and tasks and a list of services.

The following additional guidance on the mandate should also be followed.

1. The responsibilities of a CSIRT must be stated. Simply stating that a CSIRT is being established is not enough; the mandate should also indicate what its responsibilities are and why it is needed.
2. The responsibilities should indicate which overall constituency a CSIRT will serve, for example a CSIRT for the financial sector for cyberthreat management, threat information sharing and critical incident coordination, or a CSIRT for internal business divisions for cybersecurity monitoring and incident handling.
3. An authorised body must issue authority to a CSIRT. For sectoral or national CSIRTs this might be the national government, the parliament or a ministry.
4. An organisation or a business unit must be assigned to establish a CSIRT. Sometimes this might be a new organisation.

For national governments or sectoral regulators, the development of a mandate usually begins with drafting of a law, bill, cybersecurity strategy or cybersecurity plan.

For organisational CSIRTs, the development of a mandate usually begins after receiving approval to establish a CSIRT from the management board or C-level executives, starting with the purpose why it is being established.

An approved mandate of authority and responsibility usually indicates a person, unit or organisation that will lead the establishment of a CSIRT.

Examples of phrases typically used in mandate documents include the following.

1. Cybersecurity has become very important; thus, a CSIRT is being established to increase the resilience of information systems to cyberattacks; manage cyberthreats; work on lowering the costs of the impact of incidents by establishing strong incident management controls; improve know-how; foster collaboration between stakeholders; and ensure cyber situational awareness and cyber situational visibility.
2. A sectoral (national, organisational) CSIRT is being established by modernising the current IT security unit to provide effective cyber resilience, organise incident responses, enable cyber situational awareness and establish cyber information exchange channels with partner organisations.

For EU Member States, NIS Directive Annexes I and II present the requirements, tasks and mandatory constituencies of national CSIRTs; the high-level responsibility of CSIRTs is described as follows: 'responsible for risk and incident handling in accordance with a well-defined process'.

Examples of mandates for the establishment of a CSIRT include:

- btCIRT ([18]) – national CIRT of Bhutan, established by government order.
- BGD e-GOV CIRT ([19]) – Bangladesh government sectorial CSIRT, established by office order.

Additional guidance on mandates and responsibilities can be found in ENISA's *Good Practice Guide for Incident Management* (2010), Section 5.4.

2.2.2 Governance structure

The governance structure defines the responsibilities of the CSIRT's stakeholders. It can be presented as a planning document or even as part of the mandate.

The governance structure document should provide answers to a number of questions.

1. Who will provide funding for the establishment and operations of a CSIRT and on what grounds?
2. Who will provide direction, monitoring and oversight of the CSIRT?
3. What types of agreements should the CSIRT have and with which stakeholders (e.g. law enforcement, intelligence agencies, international organisations, technology partners, academia)?
4. Who will the CSIRT report to, how often and in what form?

The owner of the CSIRT governance structure is usually the hosting organisation.

The governance structure is usually clarified during the workshops held to discuss the mandate with various stakeholders.

2.2.3 Identification of the CSIRT hosting organisation

The CSIRT hosting organisation is usually mentioned in the preliminary mandate. The hosting organisation might already exist or might need to be set up.

If a new hosting organisation is being established, the CSIRT budget can be approved only after the organisation is functional in terms of setting up management and legal processes, meaning that additional time will be required at this stage.

When choosing an organisation to host a CSIRT, the organisation's authority to deliver the services in accordance with the CSIRT's mandate must be evaluated.

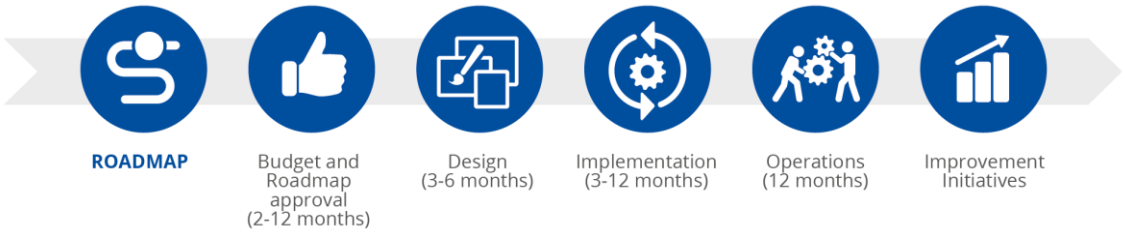
2.2.4 High-level roadmap and budget

After the mandate is defined, a high-level roadmap and budget must be approved.

The roadmap should include an expected timeline for the CSIRT establishment phases – design, implementation and operations – and further improvement initiatives.

[18] https://www.btcirt.bt/wp-content/uploads/2016/01/BtCIRT-Mandatep2.pdf
[19] https://www.cirt.gov.bd/wp-content/uploads/2016/08/Government-Mandate-of-BGD-e-GOV-CIRT.pdf

Figure 8: Roadmap example



Commonly, it takes 2–3 years from development of the preliminary mandate to initial mandate approval when a CSIRT becomes fully operational. This includes the following steps:

1. Budget approval, setting up of facilities, organisation establishment and initial hiring can take up to 1 year.
2. Design and implementation usually take 1–2 years, especially if the assistance of external consultants and technology has to be acquired through public tenders.

The budget for the initial year, which is spent on the establishment of the CSIRT and initial services, should cover at least:

1. Initial staff salaries – at least for the minimum required personnel (CSIRT manager, CSIRT establishment project manager, administrative assistant).
2. Facility establishment costs.
3. Salaries or consultancy service fees for creating the design stage results (legal processes, CSIRT-related expertise, technology deployment).
4. CSIRT skills acquisition recruitment and training.
5. Preliminary technology and licences.

'We operate 24/7'
(national CSIRT)

The budget should be adjusted according to the roadmap, mandate, stakeholder commitment and requirements for how quickly the CSIRT should be established.

The budget should be adjusted again once the design phase has finished and when the detailed plans are prepared for the implementation and operations phases. For example, if the budget is insufficient, some aspects can be moved to the further improvement phase in the roadmap.

The following notes provide indicative costings for 2020. Cost estimates are done for illustrative purposes only and does not depict any particular country.

1. In EU countries, a CSIRT staff member (including managers) costs on average EUR 40 000–60 000 per year.
2. Small CSIRT operations with three staff members (manager, two incident handlers) should budget around EUR 120 000–180 000 annually.
3. If a CSIRT is required to provide operations 24/7 for 365 days a year, it needs at least 12 additional employees (six teams of two staff members to cover 24/7, with each shift covering 8 hours). This will add EUR 480 000 annually to the budget.
4. CSIRTs typically employ the following numbers of staff: small – 3–7, medium – 10–15, large – 30–60, depending on the constituency size and mandate.
5. The cost of office rental is normally around EUR 3 000–4 000 per staff member per year.

6. It is common to spend EUR 3 000–10 000 on staff training per person per year. Attending conferences is highly recommended (one event per person per year).
7. Depending on the scope, consultancy services for the establishment of a CSIRT (design and implementation) can cost from EUR 75 000 to EUR 1 000 000 over a 1- to 3-year period.
8. It is common to spend EUR 100 000–300 000 on technology: hardware (at least two servers with virtualisation, backup solutions, firewalls, computers, printers), networking and specialised equipment for performing specific CSIRT operations (digital forensics, reverse engineering, vulnerability assessment, etc.). Using cloud services can be an effective way to limit initial investments in hardware, by allowing spending only on what is actually being used.
9. With regard to software components, CSIRTs might begin by using mostly open-source[20] solutions, using commercial tools only if there are no comparative alternatives or for their better effectiveness. In this case, the budget for software and software services should start at EUR 50 000. If CSIRTs are focusing on commercial technology, the budget should be increased; however, focusing on commercial technology can result in higher productivity, i.e. fewer staff members are required.

The initial amounts in the budget and the time period over which the budget should be spent may change over time. Design phase activities will be bound by the approved budget available.

The approved budget will impact the final detailed mandate, as an organisation can achieve the anticipated results only when a sufficient budget is made available. The discrepancy between the detailed mandate and the budget is a common reason why CSIRTs do not fulfil their mandate.

It may take 3 years for a CSIRT to become operational, so the budget should reflect the expected intensity of the CSIRT establishment process.

2.2.5 Detailed requirements for the design stage

The design phase activities will be based on the requirements and constraints of the CSIRT, such as:

1. The agreed mandate.
2. The roadmap and budget.
3. The people, competences and resources allocated to the design phase.

These must be validated and approved.

When external consultancy work is involved, the detailed requirements are often expressed as the consultancy project terms of reference (ToR) for a competitive tender (request for information (RFI)/request for proposal (RFP)).

When preparing the ToR for such work, it is relevant to include:

1. The mandate definition of the CSIRT.
2. A clear statement of the expected results.
3. The expected delivery plan.
4. The experience required from the consultants from delivering similar activities.

'We buy some specific services from vendors on behalf of the whole sector, e.g. TI for specific geographical regions/actors; sandboxes, takedown of domains, etc.' *(sectorial CSIRT)*

[20] When using Open source solutions CSIRT needs to take into consideration who is managing and updating particular solution

2.3 DESIGN

The design phase prerequisites are all of the outcomes from the assessment for readiness phase.

The design phase recommendations are aligned with SIM3 (security incident management maturity model which estimates how well a team governs, documents, performs and measures their function), covering all four areas – organisation, human, tools and processes – in sequence, as presented below. This guidance does not provide specific advice on how to reach the maturity levels, as this information can be found in the SIM3 assessment tools from ENISA ([21]) or the Open CSIRT Foundation ([22]).

In the design phase, the following outcomes are expected, in the form of either separate approved documents or one approved document.

1. Approved detailed mandate
2. CSIRT services plan
3. CSIRT processes and workflows plan
4. CSIRT organisation, skills and training structure plan
5. CSIRT facilities plan
6. CSIRT technologies and processes automation plan
7. CSIRT cooperation plan
8. CSIRT IT and information security management plan
9. Detailed requirements for the implementation stage

In addition, the resulting design structure is often published in RFC 2350 format ([23]) – this is the de facto format for the formal presentation of a CSIRT, covering the team name, contact information, the time zone, PGP (pretty good privacy) keys, the mandate (charter), policies and services, etc. It is good practice for a CSIRT to publish the RFC 2350 document on its own website.

2.3.1 Approved detailed mandate

The design phase is based on the requirements of the CSIRT mandate, which might still be in final discussions or might include some broad overarching statements. In this phase it must be ensured that final approval has been granted (e.g. the mandate has been signed by the minister, or board of directors, or executive) and that the mandate is clear and easy to understand and sets out:

1. The authority given to a CSIRT to serve and act in its constituency.
2. The responsibilities of the CSIRT.
3. The requirements, objectives and tasks.

The approval of the mandate, together with the budget constraints and the initial roadmap for establishment of the CSIRT, allows for successful preparation of the design.

A detailed mandate might indicate how to name a CSIRT, as described below.

1. The name of the organisation should reflect the mandate, ensuring that it is clearly formulated and includes the role of the CSIRT.
2. The type of constituency covered is often reflected in the name; for example, national CSIRTs are often named using the two-letter country code and the CSIRT/CIRT/CERT

[21] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey
[22] https://sim3-check.opencsirt.org/
[23] https://tools.ietf.org/html/rfc2350

abbreviation, joined by a dash, a dot or some other symbol, e.g. CERT-LV, CERT-MU, SK-CERT. The sector is often included too in a shortened form; for example, the financial sector would be FinCIRT or FS-CSIRT, with the country additionally named using the two-letter country code, e.g. EG (EG-FinCIRT).

3. Often, a name is chosen based on a short company or organisation name and adding CSIRT, for example Adidas CSIRT, CSIRT BNP Paribas.
4. A CSIRT is often referred to as a CIRT, CERT or SIRT. Such organisations must provide an incident handling (response) service.
5. The SOC name is usually used for organisations that monitor operations for the security of networks and data centres, for example NestleSOC, TDC SOC. Recently, names such as iSOC ([24]) and gSOC ([25]) have also been used.
6. When the primary function of an incident response team is to handle the vulnerabilities of the products of a certain company, it is usually referred to as a PSIRT ([26]), for example Adobe PSIRT, NVIDIA PSIRT, Fujitsu PSIRT. Separate guidance on PSIRTs has been created by FIRST.org ([27]).
7. Examples of existing team names are available on the FIRST.org ([28]), Trusted Introducer ([29]) and ENISA CSIRTs Map[30].
8. If the chosen name includes the CERT abbreviation, a request for approval must be submitted to the CERT trademark owner SEI ([31]) (the SEI policy may be amended in the future).

2.3.2 CSIRT services plan

The CSIRT services plan explains which services a CSIRT organisation will provide to a constituency to fulfil the roles and responsibilities defined in the mandate and adhere to the roadmap and budget constraints.

Figure 9: FIRST services framework

[24] An iSOC is an integrated SOC, for example in the energy sector, combining an operational technology (OT) SOC and an IT SOC.
[25] A gSOC is a global or government SOC.
[26] A PSIRT is a product security incident response team.
[27] https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1
[28] https://www.first.org/members/teams/
[29] https://www.trusted-introducer.org/directory/teams.html
[30] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map
[31] https://www.sei.cmu.edu/education-outreach/license-sei-materials/authorization-to-use-cert-mark/

The following guidelines are provided for preparation of the CSIRT services plan.

1. CSIRT should take a look at the latest version of the FIRST.org CSIRT Services Framework ([32]). This document is now available in several languages. This document presents the conceptual CSIRT services map, as presented below.
2. Choose which service areas (out of five) and which exact services the CSIRT should provide to fulfil the specific mandate stipulations.
3. Select and adjust the names of the service areas as the names provided in the CSIRT Services Framework may be too detailed initially. For example, when looking at the information security event management service area for SOCs, one might decide to consolidate both services (monitoring and detection and event analysis) into one entity and to rename the service area as security monitoring. Similarly, within the information security incident management service area, one might choose to include two services: incident handling service and artefact analysis.
4. Validate the list of resulting services to ensure that all of the mandate requirements are covered and that it does not include more services than the mandate requires. The resources of CSIRTs are limited; therefore, it is reasonable to concentrate on what is mandatory to ensure the provision of good-quality services for which proper authority has been provided.

The list of chosen CSIRT services should be listed in a CSIRT services catalogue. ITIL (information technology infrastructure library) methodology may be of value to organise the delivery of services. It is important to clearly understand the distinction between the different meanings of the word 'incident' – in CSIRTs, 'incident handling' is the name of the service, while in ITIL methodology 'incident' means a disturbance to service delivery, i.e. that the service cannot be delivered, with the 'incident' being closed when the service is recovered.

Realistically, CSIRTs must ensure that good-quality services are delivered and, if these services are disrupted, they are rapidly recovered. For example, if a CSIRT IT system fails, this could be recovered using an internal IT support process according to ITIL[33] principles.

On activities: 'incident response, monitoring sensor network, dispatching notifications, constituency building, awareness raising and education, training and cyber exercises' (national CSIRT)

2.3.3 CSIRT processes and workflows plan

CSIRT processes are needed to implement and support agreed CSIRT services.

Typically, each type of service delivery is implemented using at least one process. More than one process may be required to deliver a service if, for example, service provisioning requires several working groups to be involved, or specific intermediate goals must be reached.

Some processes may be established as supportive processes, for example, an IT support process for maintaining and updating CSIRT IT infrastructure. This process can be handled using ITIL methodology, using a separate IT services catalogue (not to be confused with a CSIRT services catalogue).

The interrelationships between the identified processes should be analysed and documented. For example, the output from the security monitoring process is an identified incident that is handed over to the incident handling process as input; the artefact analysis process can be initiated from the incident handling process when needed.

[32] https://www.first.org/standards/frameworks/
[33] https://www.axelos.com/best-practice-solutions/itil

Each process consists of one or more workflows, represented by workflow diagrams, depicting each step from the start until the final phase of activity. In addition, it is common to provide a tabular description of each step.

An example of a security incident handling workflow diagram, taken from ENISA's *Good Practice Guide for Incident Management* (2010), is provided below.

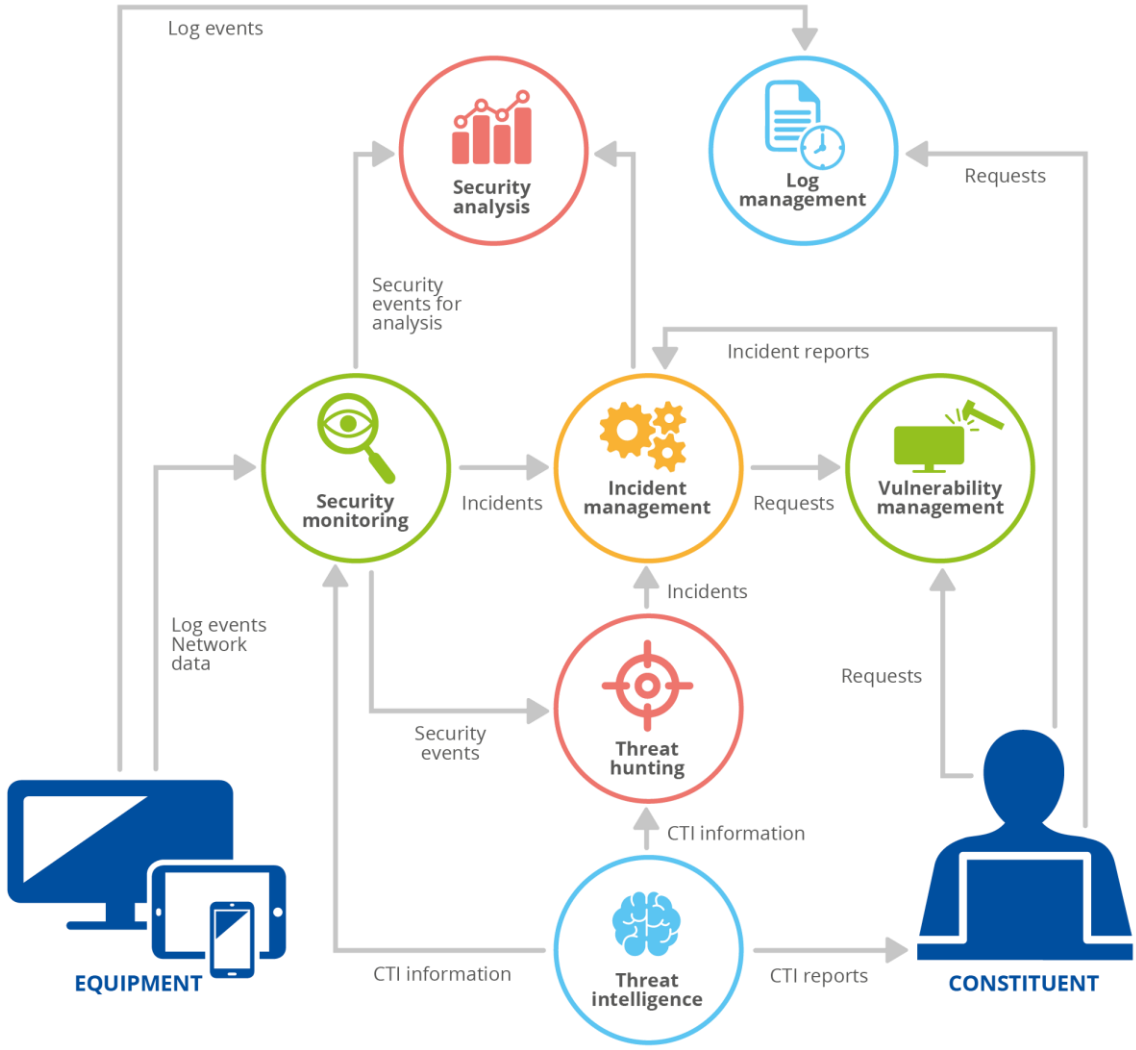
Figure 10: Incident handling workflow example

An example of an interrelationship diagram for different services and processes is presented in Figure 11.

When designing processes and workflows, the human parameters of SIM3, the ENISA CSIRT maturity assessment model ([34]) and the SOC capability and maturity model (SOC-CMM) ([35]) might be relevant tools for validating their completeness and coverage.

[34] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity
[35] https://www.soc-cmm.com/

Figure 11: Services/processes interrelationship diagram for an internal CSIRT



Examples of security incident handling and security monitoring processes, which are used for implementing security incident management and security monitoring services, are provided in Tables 1 and 2, respectively. Process definitions are adapted to the needs of CSIRTs.

Table 1: Examples of security incident handling processes

Process name	Security incident management
Description	Security incident management covers incident report registration, triage, incident resolving and incident closing
Process owner	Security incident manager
Purpose	To ensure that every incident detected is handled according to defined quality requirements and that response activities are carried out to mitigate any incidents, followed by actions to improve security measures; and to increase the maturity of the constituent's security processes so that it is more resilient to cyberthreats in the future
Service input/triggers	1. Events detected by security monitoring service activities 2. Incident reports registered by:

Process name	Security incident management
	2.1. Phone 2.2. E-mail 2.3. Online web form 2.4. Service desk self-service interface
Service output/deliverables	1. Assistance to constituents to mitigate security incidents 2. Provision of guidelines for improving the security of the constituent's infrastructure
Service activities	1. Triage of the security incident 2. Analysis of the security incident 3. Guide the containment of the security incident 4. Guide eradication and recovery after the incident 5. Close the incident 6. Lessons learned

The process is then usually constructed as a workflow diagram.

Figure 12: A simple security incident management process workflow diagram

Table 2: Examples of security incident monitoring processes

Process name	Security monitoring
Description	Event data from the security monitoring infrastructure are processed and analysed for incident detection
Process owner	Security monitoring manager
Purpose	To detect malicious and suspicious activities in a timely manner
Service input/triggers	1. Events detected by the security monitoring infrastructure 2. Alerts from the threat intelligence platform
Service output/deliverables	1. Provide alerts to constituents about security incidents 2. Register incidents in the security incident management process 3. Data for threat hunting process activities
Service activities	1. Observe alerts 2. Register incidents 3. Escalate incidents to the incident handling team

Figure 13: A simple security monitoring process workflow diagram

Example guidelines for intrusion incident handling are presented in Table 3.

Table 3: Example guidelines for intrusion incident handling

Section	Description
Containment guidelines	**Objective:** Advise the constituency and coordinate its efforts and participate in investigations of critical incidents 1. Advise the constituency to involve law enforcement authorities in the investigation 2. For incidents with a high level of criticality, consider sending the CSIRT to conduct an investigation in place or ask for logs to be shared and conduct the investigation at the CSIRT's premises. Share the findings with the constituency 3. Advise the constituency to: 3.1. Analyse logs 3.2. Find out the incident root cause 3.3. Assess for damage 3.4. Block malicious IP and DNS addresses 3.5. Implement quick workarounds 4. Evaluate the risk to other infrastructures and share anonymised incident details with the constituency 5. Look for recent similar incidents, evaluate the situation and, if necessary, raise the criticality level. Inform management about suspicious repeated intrusions
Mitigation guidelines	**Objective:** Help the constituency to find and fix the root cause of the incident, preserving any forensic evidence 1. Advise the constituency to: 1.1. Apply patches 1.2. Replace outdated and unsupported systems 1.3. Implement permanent workarounds 1.4. Implement best security practices 2. For high criticality incidents, request detailed investigation reports or offer resources to ensure proper incident analysis
Recovery guidelines	**Objective:** Support constituencies when returning to normal operations after the incident and lift temporary preventive measures 1. In the case of a high criticality incident, conduct a security assessment to evaluate the effectiveness of mitigation measures 2. Organise seminars for security personnel and explain common intrusion methods and mitigation strategies 3. Once a year conduct a technical cybersecurity exercise or training in a real-life environment

2.3.4 CSIRT organisation, skills and training structure plan

The CSIRT processes are run by CSIRT staff, who are organised into particular organisational structures.

Figure 14: Example of a small CSIRT structure

Smaller CSIRTs of up to five to seven people are mostly organised as one unit run by a unit manager (Figure 15). In this case, staff roles may be based on the NIST NICE framework's Cyber Defence Incident Responder work roles (PR-CIR-001) ([36]).

Staff training: 'TRANSITS I and II for all plus internal policies/procedures to use tools and communicate with rest of the team' *(ISP CSIRT)*

Figure 15: Example of organisational units for a bigger CSIRT

For larger CSIRT organisations of over 10 people, the structural units should be designed according to the services structure or the activities run or other organisational practices (Figure 16). Again, the NIST NICE[37] roles may serve as a starting point for defining staff roles.

[36] https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Cyber+Defense+Incident+Responder
[37] National Institute of Standards and Technology National Initiative for Cybersecurity Education https://www.nist.gov/itl/applied-cybersecurity/nice

It should be noted that 24/7 shift work can become very expensive, as six teams are required to cover the 8-hour shifts, including holidays. Thus, CSIRTs often use one of following operating procedures:

1. Operate only during normal business hours.
2. Have someone on duty to monitor calls or emergency escalations.
3. Outsource night and weekend registration monitoring to an external party for initial triage.
4. Rely on existing 24/7 network operations centre operations to process initial calls according to typical basic standard operating procedures (SOPs) and call experts if needed if a duty phone is in operation.

ENISA has developed around 50 training courses on CSIRT-related topics, which are provided for free on their website ([38]). These training materials cover technical and operational aspects, setting up a CSIRT, legal and cooperation aspects, and guidance on, for example, proactive training for CSIRTs and training methodologies. All of the training materials are licensed under a Creative Commons BY-NC-SA 4.0 license, i.e. they are open for use by anyone under attribution to ENISA. However, the training materials are non-commercial and thus are most useful for internal training delivered by CSIRT senior staff members.

ENISA has developed around 50 free training courses on CSIRT topics, which are available at ENISA Trainings for Cybersecurity Specialists, see:

ENISA - Online training material

Similarly, FIRST.org provides an increasing number of training courses on its website education pages ([39]), under the same licence terms. Also GEANT provides training for CSIRTs TRANSITS I and TRANSITS II[40]

Suggested technical training courses and laboratories for incident handlers are provided in Tables 4 and 5.

Table 4: Suggested training courses for CSIRT incident handlers

Role/skills	Training course	Provider
Duty officer, incident handler		
Networking fundamentals	Internet History, Technology, and Security (https://www.coursera.org/learn/internet-history)	Coursera with the University of Michigan
Networks, ICT concepts, cybersecurity fundamentals	CSX fundamentals and additional practice (https://www.isaca.org/credentialing/cybersecurity/csx-fundamentals-certificate)	ISACA
	Security+ (https://certification.comptia.org/certifications/security)	CompTIA
	Systems Security Certified Practitioner (SSCP) (https://www.isc2.org/Certifications/SSCP)	(ISC)²
	Information Security Foundation (https://www.seco-institute.org/certifications/information-security-certification-track/information-security-foundation-online-course/) IT Security Foundation (https://www.seco-institute.org/certifications/it-security-certification-track/it-security-foundation-online-course/)	SECO Institute

[38] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material
[39] https://www.first.org/education/trainings
[40] https://www.geant.org/Services/Trust_identity_and_security/Pages/TRANSITS_Training.aspx

Role/skills	Training course	Provider
	IT Security Practitioner (https://www.seco-institute.org/certifications/it-security-certification-track/it-security-practitioner-online-course/)	
	SEC301: Introduction to Cyber Security (http://www.sans.org/course/intro-information-security)	SANS
Incident handling basics	TRANSITS I (https://tf-csirt.org/transits/transits-events/transits-i/)	GEANT
	Foundations of Incident Management (https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P139)	Software Engineering Institute
Networking fundamentals	Cisco Certified Networking Associate (CCNA) (https://learningnetwork.cisco.com/s/ccna)	Cisco
Technical practice of cybersecurity	ISACA CSX Cybersecurity Practitioner (CSX-P) (https://nexus.isaca.org/products/145)	ISACA
Senior incident handler		
Incident handling	Certified Incident Handler (ECIH) (https://www.eccouncil.org/Certification/ec-council-certified-incident-handler; http://iclass.eccouncil.org/?p=728)	EC-Council
	SOC Analyst (https://www.seco-institute.org/certifications/it-security-certification-track/soc-analyst-online-course/)	SECO Institute
	TRANSITS II (https://tf-csirt.org/transits/transits-events/transits-ii/)	GEANT
	SEC504: Hacker Tools, Techniques, Exploits and Incident Handling (https://www.sans.org/course/hacker-techniques-exploits-incident-handling)	SANS
Penetration testing	Certified Ethical Hacker (CEH) (https://www.eccouncil.org/Certification/certified-ethical-hacker; http://iclass.eccouncil.org/?p=719)	EC-Council
	SEC560: Network Penetration Testing and Ethical Hacking (http://www.sans.org/course/network-penetration-testing-ethical-hacking)	SANS
	Ethical Hacking Foundation (https://www.seco-institute.org/certifications/ethical-hacking-certification-track/ethical-hacking-foundation-online-course/)	SECO Institute
	Ethical Hacking Practitioner (https://www.seco-institute.org/certifications/ethical-hacking-certification-track/ethical-hacking-practitioner-online-course/)	
Security architecture	Certified Information Systems Security Professional (https://www.isc2.org/cissp/default.aspx)	(ISC)²
Incident handling manager		
Advanced incident handling	FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics (https://www.sans.org/course/advanced-incident-response-digital-forensics)	SANS
Advanced incident response	FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (https://www.sans.org/course/advanced-network-forensics-analysis)	SANS

Role/skills	Training course	Provider
	FOR578: Cyber Threat Intelligence (https://www.sans.org/course/cyber-threat-intelligence)	SANS
	Certified Threat Intelligence Analyst (https://www.eccouncil.org/programs/certified-threat-intelligence-analyst-ctia/)	EC-Council
	Diamond Model of Intrusion Analysis (https://school.threatintel.academy/collections)	Threat Intelligence Academy

Table 5: Suggested training laboratories for CSIRT incident handlers

Title	Description	Target group
iLabs CEH	iLabs CEH provides virtual machines preconfigured with vulnerabilities, exploits, tools and scripts. This is a cloud-based subscription service from EC-Council designed to deliver hands-on practice to information security professionals. The iLabs CEH portal enables a course participant to launch an entire range of target machines and access them remotely. This product consists of 6 months' access to the EC-Council virtual laboratory environment for certified ethical hackers. See https://store.eccouncil.org/product/ilabs-ceh and https://www.youtube.com/watch?v=iU_7zKypJZI for further information	Senior analyst
iLabs CTIA	See https://store.eccouncil.org/product/ilabs-ctia/ for further information	Senior analyst
ISACA CSX laboratories	Laboratory classes from ISACA on different technical topics. See https://nexus.isaca.org/products for further information	Analyst
Damn Vulnerable Web Application (DVWA)	DVWA is a PHP/MySQL web application that is vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and help teachers/students to teach/learn web application security in a classroom environment. See http://www.dvwa.co.uk/ for further information	Analyst
Investigation Theory	See https://www.networkdefense.io/library/the-analyst-mindset/110302/about/ for further information	Analyst
ELK for Security Analysis	See https://www.networkdefense.co/courses/elk/ for further information	Analyst

The training suggested for developing technical skills is not sufficient to enable the successful operation of a CSIRT. In addition, each CSIRT must develop comprehensive professional, leadership and operational skills during the implementation phase using the following means.

1. Knowledge transfer by implementation experts in the form of workshops, training, mentoring and post-implementation support.
2. Visits to other CSIRTs to learn about their operations. At least two to three visits to CSIRTs in other countries should be planned. Visits usually last for a few hours and are focused on sharing operational experience. Some CSIRTs carry out staff exchanges to build knowledge.

When hiring: 'Typically we ask for CISSP' *(CSIRT)*

All CSIRT staff members must develop professional competences, as described in the NIST NICE framework (where KSA stands for knowledge, skills, and abilities) (Table 6).

Table 6: Essential professional competences for CSIRT staff members

Competency	Description
Conflict management	KSAs that relate to managing and resolving conflicts, grievances, confrontations or disagreements in a constructive manner to minimise negative personal impacts; collaborates with others to encourage cooperation and teamwork
Critical thinking	KSAs that relate to the objective analysis of facts to form a judgment
Interpersonal skills	KSAs that relate to developing and maintaining effective relationships with others, and relating well to people from varied backgrounds and different situations; considering and responding appropriately to the needs, feelings and capabilities of subordinates, peers and seniors
Oral communication	KSAs that relate to the process of expressing information or ideas by word of mouth
Presenting effectively	KSAs that relate to activities in which someone shows, describes or explains something to an audience
Written communication	KSAs that relate to process of expressing information or ideas by word of mouth

CSIRT management and administrative staff must develop their leadership and operational competences, for example as indicated in the NIST NICE framework (Tables 7 and 8).

Table 7: Essential leadership competences for CSIRT management and administrative staff

Competency	Description
Project management	KSAs that relate to the principles, methods or tools for developing, scheduling, coordinating and managing projects and resources, including monitoring and inspecting costs, work and contractor performance
Strategic planning	KSAs that relate to formulating effective strategies consistent with the objective, vision and competitive strategy of the organisation and/or business unit
Teaching others	KSAs that relate to imparting knowledge of or giving information about or instruction in (a subject or skill)
Workforce management	KSAs that relate to the activities needed to maintain a productive workforce

Table 8: Essential operational competences for CSIRT management and administrative staff

Competency	Description
Business continuity	KSAs that relate to the planning and preparation carried out by a company to ensure it overcomes serious incidents or disasters and resumes its normal operations within a reasonably short time period
Client relationship management	KSAs that relate to the concepts, practices and techniques used to identify, engage in, influence and monitor relationships with individuals and groups connected to a work effort, including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative)
Contracting/procurement	KSAs that relate to various types of contracts, techniques for contracting or procurement, and contract negotiation and administration

Competency	Description
Data privacy and protection	KSAs that relate to the relationship between the collection, storage and dissemination of data while simultaneously protecting individuals' privacy
External awareness	KSAs that relate to identifying and understanding how internal and external issues (e.g. economic, political and social trends) impact the work of the organisation
Legal, government and jurisprudence	KSAs that relate to laws, regulations, policies and ethics that can impact organisational activities
Organisational awareness	KSAs that relate to understanding an organisation's mission and functions, its social and political structure and how programmes, policies, procedures, rules and regulations drive and impact the work and objectives of the organisation
Policy management	KSAs that relate to the process of creating, communicating and maintaining policies and procedures within an organisation
Process control	KSAs that relate to the active changing of a process based on the results of process monitoring
Risk management	KSAs that relate to the methods and tools used for risk assessment and mitigation of risk
Third-party oversight/acquisition management	KSAs that relate to the process of analysing and controlling risks presented to your company, data, operations and finances by parties other than your own company

All of these competences can be acquired through participation in locally provided academic or online courses or integrated programmes. For example, Coursera.org provides more than 1 000 courses on leadership.

2.3.5 CSIRT facilities plan

Secure facilities with separate workspaces and clear physical rules and regulations are essential for the efficient functioning of CSIRTs.

At a minimum the CSIRT facilities should include a data room to house any technology, an office room for incident handling staff, and a guest reception or meeting room.

To enable business continuity, the continuity of the CSIRT infrastructure should be ensured. To this end, redundant systems and backup working space should be available.

The following must be taken into consideration when planning facilities.

1. Physical security should be considered and proper access control and monitoring should be established. In addition, a risk assessment should be performed based on neighbouring facilities.
2. The data room must provide a level of physical and environmental security that is appropriate to the data that the CSIRT will possess and manage.
3. The office room for incident handling staff must provide an appropriate, convenient and secure working environment by ensuring the 'least required privilege' access for personnel.

CSIRTs must implement appropriate physical security measures, such as ensuring perimeter control of the premises and providing access controls for entry into the different rooms for reasons of confidentiality.

Additional sources of information on physical security requirements are the ISO 27001[41] standard from the International Organization for Standardization, Field Manual FM 3-19.30[42] and national regulations. Organisations should refer to their internal safety or physical security teams for further advice on implementation of security measures.

Larger CSIRTs may have separate zones for a digital forensics and incident response (DFIR) laboratory, security monitoring (a SOC room), a crisis room and a visitors' room.

Figure 16: Example layout of the internal rooms for a CSIRT

On tools: 'MISP for threat information sharing. Elastic to analyze data. matrix.org as internal communications platform. Gitlab for internal projects management. BBB for video conferencing. Commercial feeds and tools for specific tasks if no viable open source alternative exists.'
(national CSIRT)

2.3.6 CSIRT technologies and processes automation plan

A CSIRT's success depends heavily on the automation of its processes. Generic IT automation processes are used for workplaces and office work. There are also specific CSIRT processes related to automation.

A typical CSIRT should adhere to the following practices with regard to its technical infrastructure.

1. As an on-premises data centre solution, a CSIRT must have at least two virtualisation servers to ensure high availability and recovery. In case one fails, backups are performed on a third server using tapes or an alternative solution, located in a different room.
2. Network segmentation must ensure that data centre production systems, the LAN (local area network), the guest network, the laboratory and the DMZ (demilitarised zone) are separated accordingly via firewall rules.
3. CSIRTs and SOCs are often cautious about using cloud systems extensively, as shown by the survey responses. Cloud services are mandatory at least for SaaS (software-as-a-service) services, for example data feeds from external dataset providers or websites used for interaction. Use of cloud services often results in availability, cost and operational efficiencies, with less data governance. Depending on a CSIRT's data security needs and risk appetite, different cloud services may be utilised.

[41] https://www.iso.org/isoiec-27001-information-security.html
[42] https://www.wbdg.org/FFC/ARMYCOE/FIELDMAN/fm31930.pdf

Often, automation needs fall into the following areas:

1. ticketing systems for incident report registration and handling – typically, CSIRTs use RTIR, OTRS, ServiceNow and Jira, among other ticketing technologies.
2. data feed processing and routing – feed routers, threat intelligence platforms or dataset repositories are used.
3. alert and awareness bulletin publishing platforms – these include website portals, publishing platforms and social media channels.

'Automation makes the analysis of a big incident easier and more efficient. Automation helps with the daily tasks, allowing manpower to concentrate on malware analysis, forensic analysis and more training.' *(CSIRT-CY)*

2.3.7 CSIRT cooperation plan

A CSIRT's success depends heavily on implementing effective working partnerships with different stakeholders and the international CSIRT community.

After establishment, a CSIRT might not be known by all stakeholders and constituencies; thus, it must actively approach stakeholders and constituencies and build cooperation arrangements. Some of these cooperation initiatives will result in the signing of formal memorandums of understanding (MoUs) or partnership agreements, or in formal and informal memberships of associations and information sharing communities.

'Anyrun for sandboxing, Recorded Future for threat stream' *(MSSP SOC)*

Trust-based and long-lasting partnerships require planning, including clear objectives from each partnership and strategies for how to maintain the relationships.

The guidelines set out below should be followed.

1. A proactive approach to building partnerships with local and international law enforcement and intelligence agencies might help to handle cybercrime incidents or advanced persistent threats (APTs) more effectively in crisis situations.
2. Regional and national (if any) CSIRT initiatives for improving cooperation should be considered. The Trusted Introducer listed status ([43]) ([44])·is relatively easy to achieve for a CSIRT that is already operational and that has the support of other CSIRTs and participates in CSIRT-related events and conferences. CSIRTs should subsequently focus on attaining accredited status ([45]) or even certified status ([46]), The Trusted Introducer scheme is the only certification scheme currently available for CSIRTs and Trusted Introducer services are more focused to CSIRTs operating in Europe.
3. It is strongly advised that CSIRTs join the FIRST.org association as this is the major global association for CSIRTs.
4. Proactively approaching different ISAC([47])s for partnering and exploring the value of such partnerships is often a good way to determine what partnerships will be valuable.
5. The structure of MoUs and partnership agreements can usually be divided into three parts:
   a. the objectives of partnering – this can reflect the mandates of both parties;
   b. what each of the parties will be doing in relation to each other, for example invite each other to training sessions, share knowledge, participate in workshops and exercises, share indicators, respond to inquiries about collaboration on incidents;
   c. an initial action plan and timeline, to be executed after signing of the MoU or agreement, which includes a joint evaluation of the agreement and planning of the following year's activities.

[43] https://tf-csirt.org/membership/why-listed/
[44] https://www.trusted-introducer.org/processes/registration.html
[45] https://www.trusted-introducer.org/processes/accreditation.html
[46] https://www.trusted-introducer.org/processes/certification.html
[47] Information Sharing and Analysis Centres see https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

6. For cooperation to work, related activities, for example organising, travel, hosting, workshops and informal socialising, must have a dedicated budget as part of the annual budget.

2.3.8 CSIRT IT and information security management plan

CSIRTs should implement an IT and information security management plan or adopt and adapt the IT security framework from the hosting organisation.

It is recommended that CSIRTs adhere to industry good practices, for example ISO 27001-based information security management systems (ISMS).

The IT management plan might adhere to COBIT([48]) (control objectives for information and related technology) and ITIL principles and methods.

2.3.9 Detailed requirements for the implementation stage

The results of the design plans should be included in the requirements for implementation, explaining in more detail:

1. What the requirements are and how they should be implemented.
2. What precise outcomes should be achieved.

The detailed requirements might be included as ToR.

2.4 IMPLEMENTATION

The implementation phase focuses on rolling out all services, enabling processes, preparing detailed procedures and training staff members.

At the end of the implementation phase, the CSIRT is ready to deliver services to its constituency and start the operations phase.

In the implementation phase, the following outcomes are expected.

1. Approval and implementation of the organisational structure.
2. Hiring and appointing of staff.
3. Execution of a training plan for different staff roles.
4. Preparation of facilities.
5. Development and implementation of detailed processes and procedures.
6. Implementation of technology for the automation of processes.
7. Implementation of IT and information security management procedures.
8. Training of staff for CSIRT operations.
9. Signing of relevant agreements with the constituency, stakeholders and partners.
10. Test run of CSIRT services and tuning of results.
11. Launch of CSIRT communications and celebrations.

2.4.1 Approval and implementation of the organisational structure

For a CSIRT to become operational, the designed organisational structure must be approved and the different positions defined.

[48] https://www.isaca.org/resources/cobit

Sometimes this process can take months; thus, an organisation might begin work using an interim structure, to enable work to progress without it being dependent on the CSIRT establishment process.

For example, hiring can begin using an existing structure, with a clear plan of how resources will be moved later, or by adjusting the initial services plan if a smaller number of staff are available.

2.4.2 Hiring and appointing of staff

The new structure must be filled with competent and skilled staff. It is highly likely that only a few positions will be filled with current staff; thus, additional staff members must be hired.

Usually, there is a lot of interest from those wanting to work for a newly established CSIRT and gain professional experience; however, potential recruits often lack the required competences.

As for other positions, it is important to hire staff showing a determination and willingness to provide services in a professional manner.

'SEI has a number of open source tools on its github site. These include SiLK, Cyberticket Studio, Cyobstract, and others. We have a network situational awareness suite of tools: https://tools.netsa.cert.org/ We also use MISP'
(CERT/CC)

2.4.3 Execution of a training plan for different staff roles

All CSIRT staff must have the initial skills needed for their roles. To upskill staff, the designed training plan should support implementation of, and participation by staff members in, standard training sessions, conferences and workshops.

Additional training for CSIRT operations – processes, and SOPs – must also be run.

2.4.4 Preparation of facilities

CSIRT facilities must be prepared according to the approved plan, taking into account physical security and appropriate accesss rights.

Some teams choose to brand their facilities with logos and recognisable marks, whereas other teams, especially if hosted in a national security area, do not provide any markings on their buildings; the CSIRT is visible only inside the premises.

2.4.5 Development and implementation of detailed processes and procedures

Planned CSIRT processes are implemented in the form of established procedures.

Some of the typical activities that are repeated are defined in SOPs and automated using technology.

2.4.6 Implementation of technology for the automation of processes

Technology implementation is carried out by installing, configuring, documenting and testing technologies.

CSIRTs use open-source software extensively, often written or contributed by other CSIRT members.

2.4.7 Implementation of IT and information security management procedures

CSIRTs must define and implement detailed procedures for IT and information security management.

A common challenge is that core CSIRT services and processes are a priority in the implementation phase, while IT support and internal security management processes and procedures usually receive less attention initially. Thus, it is expected that these processes and procedures will require further improvements.

When a CSIRT is part of a larger organisation, the hosting organisation's IT processes and information security management system can be adopted into practice.

2.4.8 Training of staff for CSIRT operations

Extensive hands-on and theoretical knowledge transfer to CSIRT members with regard to implemented technologies and procedures is crucial for establishment success.

Knowledge transfer activities are usually run in the form of hands-on workshops, where all processes and procedures are explained and practised.

Further training can be carried out and identification of skills gaps achieved using crisis drills and blue–red–purple teaming exercises.

2.4.9 Signing of relevant agreements with the constituency, stakeholders and partners

During the execution of a CSIRT partnership plan, there might be a need for the implementation of additional policies and procedures.

FIRST.org and Trusted Introducer membership applications should be submitted as soon as they are ready and the requirements for functional and operational readiness have been fulfilled. It may take a few months for the membership applications to be approved.

The building up and maintenance of partnerships require active participation and communication and should be overseen by the CSIRT manager or, in case of larger CSIRTs, the partnership manager.

2.4.10 Test run of CSIRT services and tuning of results

Once the processes and technologies have been implemented it is important to run tests for at least a day and provide notifications of any deficiencies in processes and technologies in the test run report. Tuning actions should then be carried out, that is, adjustments should be made to processes, workflows and technology implementation as appropriate.

Irrespective of the initial preparations and planning, the results often reveal that some design presumptions were not correct and some implementation activities must be modified.

2.4.11 Launch of CSIRT communications and celebrations

Once implementation has been completed, the CSIRT's operations can begin. It is important to communicate properly about the new CSIRT services, the CSIRT's mode of operations, the practical value it will provide and the responsibilities of the constituency and the CSIRT.

Typically, this communication is aligned with a CSIRT launch celebration and press release.

The launch celebration usually includes a small presentation, a visit to the facilities by the constituency, stakeholders and journalists, and printed materials.

A successful launch can inspire and give positive momentum to the entire CSIRT.

Similarly, other improvements are worth celebrating in order to draw positive stakeholder attention to the CSIRT, for example inauguration of a CSIRT laboratory or cyber gym facilities, launch of an annual report or any other major event in the life of the CSIRT.

2.5 OPERATIONS

The operations phase focuses on effective and efficient delivery of services, i.e. executing the CSIRT mandate daily.

In the operations phase, the following outcomes are expected.

1. Measurement of KPIs.
2. Annual operations performance review.
3. Annual stakeholder needs review.
4. Approval of the annual budget.
5. Collection of improvement initiatives.

On KPIs:
'incident statistics, vulnerability management statistics (monthly and quarterly) including number of vulnerabilities detected and remediated (only critical and high for now)'
(university CSIRT)

2.5.1 Measurement of key performance indicators

KPIs are used for management and governance purposes and quality monitoring. Not all CSIRTs are KPI driven. It has been observed that many CSIRTs are overburdened and run their overall operations without a sharp focus on the quality management of CSIRT services.

The following guidelines are provided for the use of KPIs.

1. KPIs should be measured monthly. For mature organisations, weekly indicators might also be of relevance. Annual KPIs are usually the sum of monthly KPIs.
2. KPIs should be linked to service delivery, i.e. they should be linked to each service and should facilitate an understanding of whether or not a service is of a good quality and meets service objectives.
3. Some KPIs are used only for statistical analysis whereas others are used for implementing actions for improvement. For example, the number of incidents, analysed monthly, is useful for statistical analysis – bigger or smaller numbers rarely produce actions for improvement – whereas the number of visitors to the CSIRT website, where alerts and awareness information is shared, indicates trends of relevance, which might result in actions for improvement.

Examples of KPIs include:

1. The number of meetings with the constituency each month for awareness raising (target: at least one).
2. Incident handling service-level agreement (SLA) breaches for critical incidents (target: less than 5 %).
3. Number of monthly visitors to a website (target: an increase from the previous month).
4. Number of awareness-raising campaigns carried out (target: at least one every second month).
5. Trends in incident statistics (target: priority incidents must be handled according to SLAs).

On KPIs:
'Time to respond and mitigate ongoing DDoS incidents via e-mail (1.5 hours), respond and mitigate ongoing DDoS incidents (45 minutes)'
(ISP CSIRT)

2.5.2 Annual operations performance review

The management team of an operational CSIRT should conduct the annual CSIRT performance review, to identify successes to celebrate and areas for improvement.

During the internal phase of the review, staff skills and individual performances are assessed, CSIRT processes are checked, automation is evaluated and KPIs are analysed.

The review of operations is commonly presented in the CSIRT annual report..

2.5.3 Annual stakeholder needs review

It is good practice to set up an annual workshop or meeting with CSIRT stakeholders where the performance of the CSIRT and stakeholders' priorities for and expectations of the CSIRT are presented.

These priorities contribute to the planning of subsequent improvements for the CSIRT.

2.5.4 Approval of the annual budget

As for any organisation, CSIRTs must develop and gain approval for their annual budget each year. The budget outlines which initiatives will receive additional funding.

The budget must be prepared in agreement with local laws, rules and regulations.

2.5.5 Collection of improvement initiatives

The internal annual review, stakeholder needs analysis and daily operations allow identification of CSIRT requirements that may need to be improved. These are analysed as part of the improvement phase.

Ideas for improvements may also come from the operations review. All improvement initiatives should be presented in a table, including justifications and explanations of need.

2.6 IMPROVEMENT

The improvement phase focuses on selecting and approving CSIRT enhancement initiatives. After approval, these initiatives are moved to the design, implementation and operations phases. Improvement process should be continuous during existence of CSIRT.

In the improvement phase, the following outcomes are expected.

1. List of improvement initiatives.
2. Detailed plans for improvement initiatives for the design stage.
3. Preliminary budget for improvement initiatives.

2.6.1 List of improvement initiatives

It is often difficult initially to execute the CSIRT mandate at an excellent level of quality because of a lack of skills, automation, processes and resources; thus, balancing improvement priorities is a common activity for CSIRTs.

Improvement initiatives come from the operations phase as areas requiring improvement; from a high-level roadmap; from additional guidance from stakeholders; or from the demands of CSIRT management to improve the maturity and capability of the CSIRT.

Guidance on maturity improvement is available from frameworks such as SIM3 and SOC-CMM and from ENISA, the Global Forum on Cyber Expertise (GFCE), the CERT Coordination Center (CERT/CC) and FIRST.org, among others.

With the knowledge of existing resources available for improvement initiatives, the management team of a CSIRT decides which initiatives to prioritise and approve and what resources to allocate, e.g. the budget and number of people. Examples of improvement initiatives for prioritisation are provided in Table 9.

Table 9: Examples of improvement initiatives for prioritisation

Initiative	Budget required[49] *(EUR)*	Duration *(months)*	Justification	Approved
Automation of incident detection	150 000	4	CSIRT requires automation of registration and routing of incidents from public sources and internal networks	Yes
Honeypot initiative	80 000	6	Honeypots provide visibility into who is attacking networks and how	Yes
Design, implementation and 1-year operation of an awareness service	75 000	3	Constituency lacks timely and focused awareness of contextual information; thus, it has limited resilience to social and technical attacks	Yes
ISO 27001 certification	50 000	8	CSIRT handles sensitive data and thus must ensure that internal information security processes are operating well	Yes
DFIR laboratory	250 000	12	Required for a few incidents	Postponed until the following year as the number of cases requiring digital forensic analysis is low
SOP development	60 000	4	Clear and detailed procedural instructions result in fewer errors in operations and faster learning for new personnel	Postponed until the following year because of lack of resources
Threat intelligence automation and commercial provider of information	60 000	3	Improve quality with regard to the detection and analysis of incidents	Postponed until the following year; unable to currently consume data properly because of lack of staff
Attaining SIM3 ENISA/Global CSIRT Maturity Framework (GCMF) intermediate level	40 000	5	Increased maturity allows the provision of better-quality services in a more streamlined and uniform way and a reduction in defect rates, and increases trust and the reputation of the CSIRT	Postponed until the following year as allocation of key internal expert resources is required to carry out the improvements

[49] Figures for illustrative purpose only.

2.6.2 Detailed plans for improvement initiatives for the design stage

After the improvement initiatives have been approved, the next step is to prepare detailed plans for the design stage.

In the case of external consultancy involvement, detailed requirements are often expressed as improvement project ToR in competitive tenders (RFI/RFP).

Requirements for the design stage outcomes must be specifically listed.

At this stage it is relevant to consider:

1. The objectives of the improvement initiatives.
2. The clearly stated expectations of any improvements.
3. The expected implementation plan.
4. The experience required of experts carrying out similar work.

2.6.3 Preliminary budget for improvement initiatives

The annual budget must incorporate any approved preliminary budget for improvement initiatives. This may be needed to cover the costs of internal staff, additional facilities, technology, external consultancy, administration, cooperation and marketing, and additional training.

The preliminary budget will guide resource and design constraints for the design phase activities during planning.

It is normal to expect that at least 15 % of the annual CSIRT budget will be spent on improvement initiatives for mature CSIRTs. For CSIRTs with a lower level of maturity, improvement initiatives usually make up at least 30 % of the CSIRT budget.

3. CONCLUSIONS

This report presents guidelines for the establishment of CSIRTs and SOCs using a phased outcomes-driven approach, including many examples from established CSIRTs of the different phases of implementation.

Establishment is a continuous process. It is possible to identify the beginning of the process; however, the end stage consists of a continuous improvement cycle – to better serve the constituency, be more effective in operations and respond better to stakeholder needs.

The authors hope that this publication will inspire better CSIRT and SOC project management and provide clearer descriptions of the intermediate steps involved in the establishment of CSIRTs and SOCs.

Some challenges related to the establishment of CSIRTs and SOCs are not covered in this report and require additional work.

1. This publication focuses on the establishment of a single CSIRT. However, a single CSIRT is usually part of an ecosystem of CSIRTs. Future research might focus on ecosystem buildout and value creation through partnerships and specialisation.
2. Sectorial CSIRTs are emerging in different sectors in many countries; however, there are currently too few data points and good practice guidelines available for guidance to be provided for different sector-specific CSIRTs.
3. There is too little relevant and practical guidance on blueprints for technology orchestration and automation of CSIRTs and SOCs.
4. The do-it-yourself approach to creating a CSIRT is still challenging because of the relevant expertise required, which is not easily available in many countries. It will be important to determine in the future how this can be overcome.

ENISA continues to support incident response teams by creating relevant content for CSIRTs..

4. GLOSSARY AND ACRONYMS

Please refer to ENISA glossaries and lists of acronyms:

- https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/glossary
- https://www.enisa.europa.eu/topics/csirts-in-europe/glossary
- https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary

5. BIBLIOGRAPHY

Carnegie Mellon University, 2016, *Create a CSIRT*, Software Engineering Institute, Pittsburgh, PA.

Cowley, C. and Pescatore, J., 2019, *Common and best practices for security operations centers: Results of the 2019 SOC survey*, SANS Institute.

ENISA, 2006, *A step-by-step approach on how to set up a CSIRT.* (https://www.enisa.europa.eu/publications/csirt-setting-up-guide)

FIRST, 2019, *Computer Security Incident Response Team (CSIRT) Services Framework* (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1).

IETF Internet Engineering Task Force, 1998, RFC 2350 for CSIRT establishments. (https://tools.ietf.org/html/rfc2350)

Internet Governance Forum, 2014, Best practice forum on establishing and supporting computer security incident response teams (CSIRTs) for internet security (https://www.intgovforum.org/multilingual/content/establishing-and-supporting-computer-incident-security-response-teams-csirts-for-internet).

MITRE, 2014, *Ten strategies of a world-class cybersecurity operations center*, MITRE, Bedford, MA.

Morgus, R., Skierka, I., Hohmann, M. and Maurer, T., 2015, *National CSIRTs and their role in computer security incident response*, New America and GPPi. (https://www.researchgate.net/publication/323358191_National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response)

National Cyber Security Centre, 2015, *CSIRT Maturity Kit*, National Cyber Security Centre, the Hague.

National Cyber Security Centre, 2017, *Building a SOC: Start Small*, National Cybersecurity Centre, the Hague.

Organization of American States, 2016, *Best Practices for Establishing a National CSIRT*, OAS, Washington, D.C.

Open CSIRT Foundation, 2008-2019, SIM3: Security Incident Management Maturity Model. (https://opencsirt.org/csirt-maturity/sim3-and-references/)

Skierka, I., Morgus, R., Hohmann, M. and Maurer, T., 2015, *CSIRT Basics for Policy-makers*, New America and GPPi. (https://www.researchgate.net/publication/323358187_CSIRT_Basics_for_Policy-Makers)

Telecommunications Development Sector (ITU-D), 2020, ITU CIRT framework, International Telecommunication Union, Geneva.

ThaiCERT, 2017, *Establishing a CSIRT*, Thailand Computer Emergency Response Team, Bangkok.

TNO, 2017, *GFCE global good practices: National computer security incident response teams (CSIRTs)*. (https://thegfce.org/wp-content/uploads/2020/06/NationalComputerSecurityIncidentResponseTeamsCSIRTs-1.pdf)

A ANNEX: QUESTIONNAIRE

Data collection using the questionnaire

The content of the report “Guidelines for establishing CSIRTs and SOCs” is based on the analysis of current publications on CSIRT establishment, the answers to this questionnaire and the authors’ experience in establishing and improvement CSIRTs over numerous projects in Europe, Asia, Africa and South America.

This field questionnaire (presented below) was published using the European Commission Questionnaire platform (the direct link to the questionnaire was https://ec.europa.eu/eusurvey/runner/HowtosetupCSIRTandSOC) and distributed to various CSIRTs and SOCs in different parts of the world, via sharing networks, as well as individually encouraging to participate. CSIRT and SOC teams were invited to fill it in via personal invitations as well as Trusted Introducer member and CIRTs Network communication.

During the set time for the questionnaire detailed responses were received from over 40 CSIRT and SOC teams from different geographic locations including various types of CSIRTs and SOCs (national, sectorial, internal to organization and other).

The questionnaire used

The objective of the questionnaire is to serve ENISA’s study on Guidelines to setup CSIRTs and SOCs. Responses are expected from at least 40 organizations and the received data will be processed and integrated with other methods of research. Some of the gathered data will be used in the ENISA CSIRT and SOC Setup Guidelines publication as a case study, an example, or statistically processed data.

The data is gathered in the European Commission Questionnaire platform, and will not be used, sold, or processed in any other way except for direct ENISA analysis, to serve its target:

“Since 2009, ENISA has carried out a considerable amount of work in CSIRT Capabilities and Maturity area, and this work contributes by shaping the role of ENISA in helping CSIRTs on their way to a higher maturity standard and advanced capabilities.”

To be filled by CSIRT or SOC team manager or assigned person.

You can answer only the questions you find relevant/interesting/on which you are willing to share your experience and expertise.

A.1 About your CSIRT/SOC team:

1.1. Team / Organization name: (text box)

1.2. Country: (text box)

1.3. Type of CSIRT or SOC: National / Sectorial / MSSP / Internal to organization (multichoice choosing)

1.4. Team size: (text box)

1.5. Constituency of the CSIRT or SOC: (text box)

1.6. Year of establishment: (text box)

1.7. Contact email and/or phone, for clarifications if any: (text box)

1.8. Permission of data usage: Anonymous (i.e. without any attribution to the team) / Can be attributed to your team, but need to receive a prior confirmation for exact data to be attributed / all data is ok to be used in ENISA research and possibly attributed to your team)

A.2 Terminology questions:

2.1. Does your organization operate a CSIRT or SOC, or both? (single choice)

2.2. If both, how are the roles split between CSIRT and SOC? (text box)

2.3. How do you perceive the difference between a CSIRT and a SOC as organizations? (text box)

A.3 CSIRT/SOC related knowledge questions:

3.1. Which publications do you use or find relevant to implement capability and maturity improvements for your organization? (text box)

3.2. What publications and guidance from ENISA content do you find are missing on CSIRT and SOC topics for your effective work? (text box)

3.3. If you conduct a Coordinating CSIRT role (i.e. your team coordinates incidents, which are happening outside your institution/enterprise), what activities do you regularly conduct under such role? (Text box)

3.4. If you conduct Internal or MSSP CSIRT/SOC role (i.e. you handle your own institution/enterprise incidents or work as contractual MSSP), what activities you regularly conduct under such a role? (Text box)

3.5. If you outsource some functions of CSIRT/SOC, what are they? What is the motivation to outsource? (text box)

3.6. What kind of regular reporting are you delivering (please describe to whom (no names needed but general target group, for example – energy sector), what kind of content, and how often? For example, annual report to the public with statistics of incidents, quarterly to ENISA on CII threats, weekly vulnerability statistics to CISO, etc.) (Text box)

3.7. Describe the information-sharing methods you have implemented in your operations (for example: website newsletters and alerts; provide customized MISP/IntelMQ based feed to CII subscribers; provide annual/quarterly statistics from internal/external sources on incidents/vulnerabilities and share it with constituency; have deployed PassiveDNS sensors and share resulting feed with passiveDNS community; contribute to FIRST.org MISP instance with OSINT and data from your investigations; deployed T-POT and share data with sicherheitstacho platform, etc.) (Text box)

3.8. Do you run your tools on premises, in cloud (public or private), or mixed? What are your future plans regarding this topic? What is your opinion about the industry trend on this topic? (text box)

3.9. Are orchestration and automation important objectives for your CSIRT/SOC? Do you currently or in future plans use SOAR-like tools?

3.10. Do you operate 24/7? Do you see "follow-the-sun" as a solution (team spread in different time zones), at least for the future? (text box)

3.11. Which open-source tools and for what objective are you using? Which and for what reason would you advocate them to other CSIRT/SOCs as especially valuable? (text box)

3.12. Which commercial tools and for what objective you are using them? Which and for what reason you would advocate them to other CSIRT/SOCs as valuable? (text box)

3.13. What are the main KPIs and their target levels you have implemented for your CSIRT/SOC operations? (text box)

3.14. What were the main problems that you encountered when setting up your CSIRT or SOC? (text box)

3.15. What actions would you take (or would recommend) to avoid the mentioned problems when setting up a new CSIRT or SOC? (text box)

3.16. If you would have to establish a new CSIRT or SOC team in the same or a different organization, what activity priorities you would focus on? Please choose up to 5. (text box)

A.4 Staffing Roles:

4.1. How many formal roles have you defined in your CSIRT/SOC organization? What are they, and what is their short description? (text box)

4.2. What training for different roles (that you have defined earlier) do you recommend or consider before you consider the employee as a fully-prepared specialist at a specific role in your organization? (text box)

4.3. What are the ongoing training paths for the current staff (ex. ad-hoc, organised in a particular order, etc.) (text box)

4.4. What challenges do you face developing and arranging roles in your organization? (text box)

A.5 SIM3 and other CSIRT models related questions:

5.1. About SIM3 model usage in your CSIRT or SOC organization: we do not know or use the model/it is somewhat used as a reference/it is our development guiding and maturity improvement model/we use alternative model;

5.2. If you are using or planning to use SIM3 model in your organization: how has SIM3 created value for your organization so far? (text box)

5.3. Please list what CSIRT/SOC services have you defined, implemented, are providing and measuring for your constituency? (text box)

5.4. What Organizational and Personnel biggest challenges do you see for improving maturity of your CSIRT/SOC organisation? (text box)

5.5. Which CSIRT/SOC operational processes have you formally documented and implemented (e.g. Incident Prevention Process, Incident Detection Process, Incident Resolution Process, Audit/Feedback Process, etc.)? (text box)

6. B ANNEX: METHODOLOGY MAPPING

1. What CSIRTs methodology covers:					
Aspect / Source	1.National CSIRT	2.Critical Sector CSIRT / SOC	3.MSSP CSIRT / SOC	4.Organisation CSIRT / SOC	5.Terminology it uses (CSIRT/ CERT/SOC)
FRST	x	x	x	x	CSIRT
ENIS1	x	x	x	x	CSIRT
THAI	x	x	x	x	CSIRT
OAS	x				CSIRT
GPPI2	x				CSIRT
GPPI1	x	x		x	CSIRT
GFCE	x				CSIRT
CMU1				x	CSIRT
MITRE	x	x	x	x	SOC
SIM3	x	x	x	x	CSIRT
NL1	x	x	x	x	CSIRT
NL2				x	SOC
RFC				x	CSIRT
SANS1		x	x	x	SOC
IGF1		x	x	x	CSIRT
ITU	x				CIRT
Count	12	9	8	12	16

2. Phases of establishment CSIRT/SOC covered:					
Aspect / Source	**1.Assessment for readiness**	**2.Design**	**3.Implement**	**4.Operate**	**5.Improve**
FRST				x	
ENIS1		x	x	x	x
THAI	x	x	x	x	x
OAS		x	x		
GPPI2		x			
GPPI1		x		x	x
GFCE		x	x	x	x
CMU1	x	x	x	x	x
MITRE	x	x	x	x	x
SIM3	x	x		x	x
NL1		x	x	x	
NL2	x	x	x		x
RFC		x	x	x	
SANS1				x	
IGF1		x		x	
ITU	x	x	x		
Count	6	14	10	12	8

3. Covered SIM3 Parameters: 1.O "Organisation" Parameters										
Aspect / Source	O-1 : Mandate	O-2 : Constituency	O-3 : Authority	O-4 : Responsibility	O-5 : Service Description	O-7 : Service Level Description	O-8 : Incident Classification	O-9 : Integration In Existing CSIRT Systems	O-10 : Organisational Framework	O-11 : Security Policy
FRST					x					
ENIS1	x	x		x	x	x	x	x	x	x
THAI	x	x	x	x	x		x	x	x	x
OAS	x	x	x	x	x					x
GPPI2	x		x	x	x				x	
GPPI1	x				x			x		
GFCE	x	x	x	x	x			x		
CMU1	x	x	x	x	x				x	
MITRE	x	x	x	x	x			x		
SIM3	x	x	x	x	x	x	x	x	x	x
NL1					x		x	x	x	x
NL2	x		x		x				x	x
RFC	x	x	x	x	x	x	x	x	x	x
SANS1	x	x		x	x				x	
IGF1					x				x	x
ITU	x	x	x	x	x				x	x
Count	13	10	10	11	16	3	5	8	11	9

3. Covered SIM3 Parameters: 2.H "Human" Parameters							
Aspect / Source	H-1 : Code Of Conduct/ Practice/Ethics	H-2 : Personal Resilience	H-3 : Skillset Description	H-4 : Internal Training	H-5 : External Technical Training	H-6 : External Communication Training	H-7 : External Networking
FRST				x	x	x	
ENIS1	x	x	x	x	x		x
THAI	x	x	x	x	x		x
OAS		x	x		x		
GPPI2							x
GPPI1							
GFCE							
CMU1							
MITRE	x	x	x	x	x		x
SIM3	x	x	x	x	x	x	x
NL1	x	x	x	x	x	x	x
NL2			x				
RFC							
SANS1	x	x					
IGF1							
ITU				x			
Count	6	7	7	7	7	3	6

3. Covered SIM3 Parameters: 3.T "Tools" Parameters										
Aspect / Source	T-1 : IT Resources List	T-2 : Information Sources List	T-3 : Consolidated E-Mail System	T-4 : Incident Tracking System	T-5 : Resilient Phone	T-6 : Resilient E-Mail	T-7 : Resilient Internet Access	T-8 : Incident Prevention Toolset	T-9 : Incident Detection Toolset	T-10 : Incident Resolution Toolset
FRST										
ENIS1	x	x		x	x			x	x	
THAI	x	x	x	x	x	x	x			
OAS										
GPPI2										
GPPI1										
GFCE					x	x	x			
CMU1										
MITRE	x	x		x				x	x	x
SIM3	x	x	x	x	x	x	x	x	x	x
NL1	x		x	x						
NL2	x			x						
RFC						x				
SANS1									x	x
IGF1										
ITU			x	x		x	x		x	x
Count	6	4	4	7	4	5	4	3	5	4

3. Covered SIM3 Parameters: 4.P "Processes" Parameters																	
Aspect / Source	P-1 : Escalation To Governance Level	P-2 : Escalation To Press Function	P-3 : Escalation To Legal Function	P-4 : Incident Prevention Process	P-5 : Incident Detection Process	P-6 : Incident Resolution Process	P-7 : Specific Incident Processes	P-8 : Audit/Feedback Process	P-9 : Emergency Reachability Process	P-10 : Best Practice E-Mail And Web Presence	P-11: Secure Information Handling Process	P-12: Information Sources Process	P-13: Outreach Process	P-14: Reporting Process	P-15: Statistics Process	P-16: Meeting Process	P-17: Peer-To-Peer Process
FRST	x	x			x	x	x						x	x			
ENIS1		x		x	x	x		x	x	x	x	x	x	x			x
THAI						x		x	x		x			x			
OAS																	
GPPI2																	
GPPI1																	
GFCE											x		x				
CMU1																	
MITRE	x			x	x	x					x			x			
SIM3	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
NL1					x	x			x	x	x		x				
NL2								x			x						
RFC						x											
SANS1					x	x	x							x	x		
IGF1																	
ITU				x	x	x	x	x									
Count	3	3	1	4	7	9	4	5	4	3	7	2	5	6	2	1	2

4. Services of FIRST.org covered:																										
Aspect / Source	Service Area: Information Security Event Management	Service: Monitoring and detection	Service: Event analysis	Service Area: Information Security Incident Management	Service: Information security incident report acceptance	Service: Information security incident analysis	Service: Artifact and forensic evidence analysis	Service: Mitigation and recovery	Service: Information security incident coordination	Service: Crisis management support	Service Area: Vulnerability Management	Service: Vulnerability discovery / research	Service: Vulnerability report intake	Service: Vulnerability analysis	Service: Vulnerability coordination	Service: Vulnerability disclosure	Service: Vulnerability response8	Service Area: Situational Awareness	Service: Data acquisition	Service: Analysis and synthesis	Service: Communication	Service Area: Knowledge Transfer	Service: Awareness building	Service: Training and education	Service: Exercises	Service: Technical and policy advisory
FRST	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
ENIS1	x	x	x	x	x	x	x	x	x		x	x		x	x	x	x		x		x		x	x	x	x
THAI					x	x	x	x	x																	
OAS		x			x	x	x	x				x					x									x
GPPI2				x							x										x					x
GPPI1		x		x		x	x	x	x		x			x	x		x			x	x		x	x		x
GFCE				x														x			x	x	x	x	x	
CMU1																										
MITRE		x				x	x	x				x							x	x	x			x	x	x
SIM3																										
NL1		x				x		x													x		x	x	x	
NL2	x	x		x		x									x		x		x							x
RFC					x	x			x																	
SANS1	x	x	x																							
IGF1																										
ITU	x	x	x	x	x	x	x	x	x	x								x	x	x	x					
Count	5	9	4	7	6	10	7	8	6	2	4	4	1	3	4	2	5	3	5	4	8	2	5	6	5	7

The acronyms used in the methodology mapping diagram are explained in the following table.

Local Acronym	Title of Publication
FRST	Computer Security Incident Response Team (CSIRT) Services Framework, FIRST, 2019.
ENIS1	A Step-By-Step Approach On How To Set Up a CSIRT, European Union Agency for Network and Information Security, 2006.
THAI	Establishing a CSIRT, ThaiCERT, 2017.
OAS	Best Practices for Establishing a National CSIRT, The Organization of American States, 2016.
GPPI2	National CSIRTs and Their Role in Computer Security Incident Response, New America and GPPi, 2015.
GPPI1	CSIRT Basics for Policy-Makers, New America and GPPi, 2015.
GFCE	GFCE Global Good Practices: National Computer Security Incident Response Teams (CSIRTs), TNO, 2017.
CMU1	Create a CSIRT, Carnegie Mellon University, 2016.
MITRE	Ten Strategies of a World-Class Cybersecurity Operations Center, MITRE, 2014.
SIM3	SIM3: Security Incident Management Maturity Model, S-CURE bv and PRESECURE GmbH, 2015.
NL1	CSIRT Maturity Kit, National Cyber Security Centre, The Netherlands, 2015.
NL2	Building a SOC: start small, National Cyber Security Centre, The Netherlands, 2017.
RFC	RFC 2350 for CSIRT establishments, IETF, 1998.
SANS1	Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey, SANS, 2019.
IGF1	Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security, Internet Governance Forum, 2014.
ITU	ITU CIRT Framework, ITU-D, 2020.

TP02-20-935-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-410-7
DOI 10.2824/056764