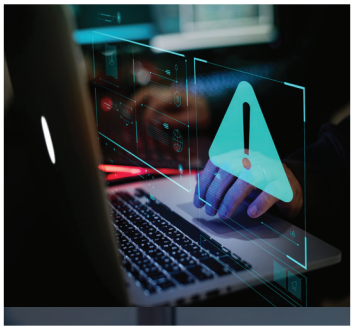
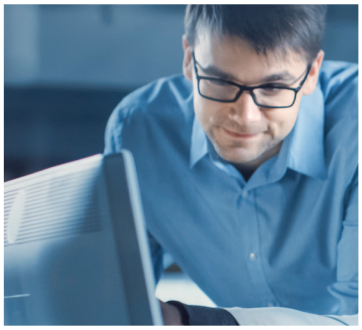
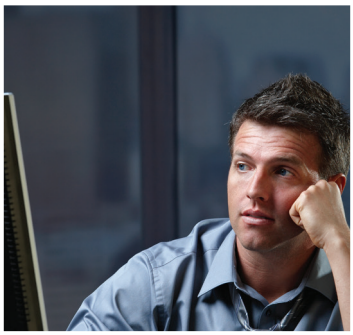
**ITU Publications**
Cybersecurity

International Telecommunication Union
Development Sector

# ITU cybersecurity programme: CIRT framework






# ITU cybersecurity programme: CIRT framework

## Disclaimer:

*The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ITU and of the Secretariat of ITU concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.*

*The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.*

*All reasonable precautions have been taken by ITU to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader.*

*The opinions, findings and conclusions expressed in this publication do not necessarily reflect the views of ITU or membership.*

**ISBN:**

978-92-61- 34941-7 (Electronic version)
978-92-61- 34951-6 (EPUB version)
978-92-61- 34961-5 (Mobi version)

**Please consider the environment before printing this report.**

# Table of contents

## List of figures

# 1 Executive summary

This report sets out how to establish a national CIRT and outlines cooperation mechanisms at the regional and international levels that identify, manage, and respond to cyberthreats.

Objective 2 of the Buenos Aires Action Plan is to support the ITU membership, in particular developing countries, in addressing the issues identified by WTDC-17 among others on establishing organizational structures, such as CIRTs, to identify, manage and respond to cyber threats, and cooperation mechanisms at the regional and international level. For this reason, Resolution 69 (rev. Buenos Aires, 2017) "Facilitating creation of national computer incident response teams, particularly for developing countries, and cooperation between them" was adopted at WTDC-17.

As lead facilitator for WSIS Action Line C5, ITU is responsible for assisting stakeholders in building confidence and security in the use of Information and Communication Technologies (ICTs) at national, regional and international levels.

In addition, ITU Resolution 130 (rev. Busan, 2014) on "Strengthening the role of ITU in building confidence and security in the use of information and communication technologies"; in particular instructs the Director of the Telecommunication Development Bureau (BDT) to support ITU Member States in their effort towards protection against cyber threats at national, regional and international levels, as appropriate, by establishing mechanisms, such as CIRTs, to identify, manage and respond to cyber threats, and cooperation mechanisms at the regional and international level.

WTDC-17 also calls on assisting Member States in establishing organizational structures, such as CIRTs, to identify, manage and respond to cyber threats, and cooperation mechanisms at the regional and international level. Governments are focusing increasingly on digital transformation and digital economy initiatives to ensure future prosperity, and information technologies have become so widely used that computer-related risks can no longer be separated from general business, health, and privacy risks, including protecting valuable national assets and securing cyberspace and critical information infrastructure.

It is essential to identify, create and coordination national centres that will monitor, warn, coordinate response and recovery efforts, and facilitate collaboration between government entities, the private sector, academia, and the international community when dealing with cybersecurity issues.

National and international collaboration to align capabilities and expertise are necessary to manage and raise awareness of potential incidents, and take remedial action, and governments have a key role in ensuring this cooperation. In addition, participation in international and regional professional associations of incident response teams facilitates trusted collaboration.

National computer incident response teams (CIRTs) not only protect critical infrastructure, but also assist in drafting national cybersecurity-related strategy as well as serving as central coordinators to further build and strengthen a national culture of cybersecurity.

The national CIRT plays a key role in detecting, managing, responding and preparing for cyber incidents. However, implementing an incident management mechanism requires funding, alignment to local requirements, human resources, processes, training, technological capability, government and private sector partnerships, and legal requirements.

Developing countries, with limited human, institutional and financial resources, face challenges in elaborating and implementing national policies and frameworks for cybersecurity and critical information infrastructure protection.

The establishment of a national CIRT, and the development of related processes, serves as a foundation for the development of the following activities:

- building a knowledge base that supports the country's implementation of a national cybersecurity strategy, as well as an approach for the protection of critical information infrastructures;
- supporting the building of a national culture and ecosystem of cybersecurity, and related awareness raising initiatives;
- supporting the development of related national cybersecurity platforms, such as e-government services, national identity and access management frameworks;
- further enabling the beneficiary country to develop and enhance its incident response and coordination capabilities.

For questions regarding this framework, please contact cybersecurity@itu.int.

# 2 Scope of the ITU CIRT framework

The ITU CIRT framework is used in ITU engagements for beneficiary country assistance to establish a national CIRT that serves as a trusted central coordination point of contact for national cybersecurity policy, aimed at identifying, defending, responding and managing cyber threats. ITU assists the beneficiary country in assessing, building, and deploying the technical capabilities and related trainings necessary to establish its national CIRT.

### Framework objectives

The primary objectives of ITU CIRT framework are to:

- describe the ITU CIRT project approach; and
- present the structure and content of different project phases to clarify scope, responsibilities, and efforts.

The framework:

- enables a national (or sector) CIRT to serve as a trusted and central coordination point of contact for cybersecurity policy aimed at identifying, defending, responding to, and managing cyber threats.
- create a functioning national CIRT that is able to provide its constituents with a basic set of services such as incident handling, incident analysis, outreach/communication, and later with enhanced services including situation awareness and digital forensics.

### ITU CIRT project history

The ITU CIRT project has completed CIRT assessments for 81 countries. Each project starts with the CIRT assessment, and the initiative continues to assist with planning, implementation, and operation. ITU has established or enhanced:

- 14 national CIRTs in: Barbados, Burkina Faso, Cyprus (Governmental CIRT and National CSIRT), Ghana, Jamaica, Kenya, Montenegro, Tanzania, Trinidad and Tobago, Uganda, Zambia, State of Palestine, Gambia, and Botswana.
- CIRT implementations in progress in Bahamas, Burundi, and Malawi.
- CIRT enhancement in Barbados, and Kenya.

Continued collaboration with the newly established CIRT ensures that support remains available, and that institutions can continue to grow.

### Target audience

The main target audience for this framework includes:

- ITU Member States seeking support for the establishment of their national CIRT; and
- organizations around the world that wish to support the ITU CIRTs programme.

ITU Member States are constantly showing interest in the ITU CIRT programme. Thus, this framework document serves to explain the process of running a CIRT project with ITU.

CIRT projects are mostly government funded and cybersecurity capacity projects are occasionally supported by external donors.

## Usage of the framework

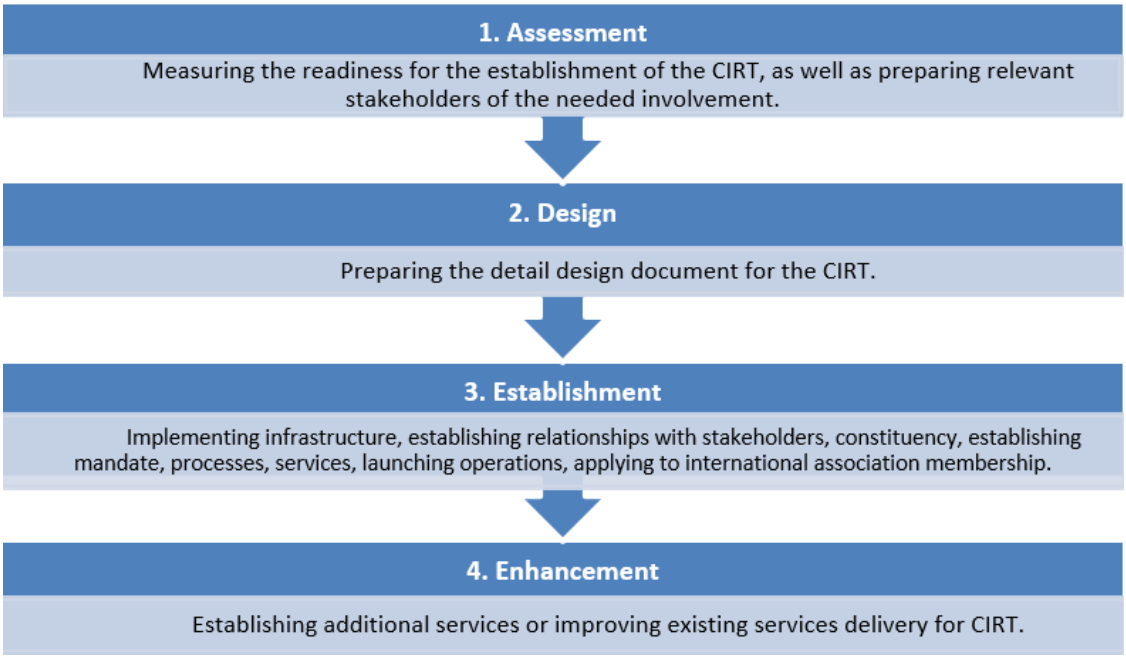
ITU CIRT framework is most applicable in the following instances:

- learn about ITU methodology for building national CIRTs;
- understand the effort needed by all parties to build a CIRT;
- get to know different phases of CIRT project life cycle; and
- familiarize with roles and responsibilities of stakeholders in CIRT projects.

# 3 Framework structure and phases

National CIRT rollouts have several phases that are defined by project objectives, resources and commitment. Figure 1 sets out four phases: assessment, design, establishment, and enhancement. These phases are customizable depending on detailed requirements.

## Figure 1: CIRT framework phased approach




Source: ITU

Typically, countries run project phases to define project scope and prepare the budget (assessment phase), to execute the budget and initiate operations (design and establishment phases), and to improve existing operations (enhancement).

## 3.1 Phase 1: Assessment

**Description**: The assessment phase ensures that project expectations are discussed and aligned with stakeholders such as project requirements, feasibility and finance, including government interest and motivation to create and mandate a national CIRT.

**Preconditions:** A government request for assistance to create a national CIRT.

**Outcome**: An assessment report that presents the way-forward and launch requirements for a national CIRT.

### Scope and methodology

The primary objective of assessment phase is to assist the country in the assessment of its readiness to implement a national CIRT. The assessment phase is implemented as a workshop with relevant CIRT stakeholders in the country, and the precondition that must be met for

this phase is a confirmed willingness from the country's responsible agency supported by the development of a national CIRT mandate.

The outcome and deliverable of the assessment phase is a report that contains key issues, key findings and analyses, recommendations, and a phased implementation plan for setting up the national CIRT. The report is prepared by ITU experts and delivered within three months of the on-site assessment.

## Figure 2: The assessment phase


Source: ITU

During preparation and onsite workshop, the following activities are undertaken in addition to the data collected while working with the national counterparts and in close collaboration with the relevant ministries:

1. Preparation for onside assessment (pre-workshop):
    - Studies and analyses of the country's current cybersecurity status and needs are conducted. Information is analyzed from ITU Global Cybersecurity Index, as well as from public sources. ITU sends a questionnaire to collect mission preparation data.
    - A study of institutional and organizational requirements is carried out, as well as preparation of the national CIRT set-up.
2. During the onsite assessment workshop:
    - A series of interactions and discussions are held with relevant stakeholders to assess the level of readiness for the creation of a national CIRT.
    - Training on key concepts of a national CIRT are carried out including operation and maintenance, coordination of CIRTs with all relevant national agencies, and requirements for international cooperation.
3. The assessment and workshop report: this provides key findings and recommendations indicating the best way forward to establish a national CIRT.

The assessment phase assigns project managers from both ITU and the country to ensure that the phase progresses smoothly.

### Assessment workshop

The assessment workshop consists of:

- An introduction and stakeholder survey.

- Sensitization: presenting national CIRT value, structure, operational models.
- Assessment discussions: assessor team records all findings needed to establish the "as-is" state of the facility and the personnel. These findings will be recorded on a confidential checklist, and completed via meetings, trainings, interview sessions, and one-to-one discussions.
- A verbal report: this will be provided at the closing meeting to brief officials on the findings, and to offer preliminary recommendations.

Each stakeholder organization should provide one to two participants to attend the assessment workshop, including:

- relevant ministry representatives;
- policy makers (parliamentarians);
- judiciary system;
- regulatory bodies;
- national security agencies;
- military establishment (or those currently responsible for information security and/or IT and ICT management);
- law enforcement agencies;
- critical infrastructure providers (water, energy, transport, etc.);
- central monetary agency and banks (most relevant public and commercial);
- telecommunication operators and Internet service providers;
- academia and national research bodies;
- local industry (private sector) involved in security initiatives.

The profiles of the participants must include technical, managerial, and national policy experts.

### Results of the assessment phase

The assessment phase written report must include the following content:

1. evaluation of the country's cybersecurity posture;
2. a high-level approach for the implementation of the CIRT including the resources needed; and
3. suggested project financing mechanisms.

## 3.2 Phase 2: Design

**Description**: For a national CIRT to become fully operational, the details agreed upon in the design phase must allow experts to set up and implement the CIRT including systems, processes, and skills transfer.

**Preconditions**: Following the assessment report, ITU and the country sign the Project Document and Cooperation Agreement and the country transfers the necessary funds to ITU.

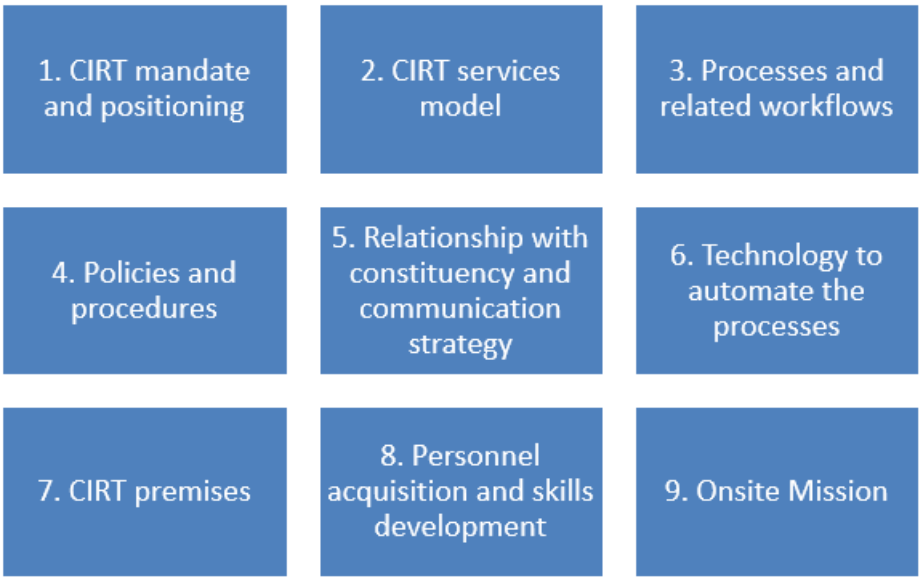
**Outcome**: CIRT Design Document is approved including associated implementation processes and tools.

### Scope and methodology

The design phase focuses on preparing and approving the CIRT Design Document. The CIRT design structure is based on the information provided in the CIRT assessment report. This

requires regular remote consultation sessions with the CIRT project manager, along with associated experts, to gather the design details and includes a detailed design presentation before the CIRT Design Document is signed-off.

## Figure 3: Design phase review




Source: ITU

During the design phase the following areas are reviewed:

1. CIRT mandate and positioning: these CIRT governance tools provide direction to the team, and include:
    - questionnaire responses review;
    - CIRT mission and vision;
    - reporting structure, authority, and organization.
2. CIRT services model: this provides the CIRT output structure, and include:
    - review of questionnaire responses;
    - interaction with the country where necessary;

Define the CIRT core services according to the FIRST CSIRT Services Framework[1]

3. Processes and related workflows: this element provides methods to deliver the CIRT services while providing internal support and includes identifying and documenting:
    - existing processes (if any);
    - specific processes (according to the services identified, e.g. incident handling, etc.);
    - general purpose processes (e.g. recruitment);
    - workflows (as necessary).
4. Policies and procedures: this element presents the methods of execution of the processes, including identifying and documenting:

[1] https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf

- existing procedures (if any);
- general purpose policies and procedures (data classification, retention, data life cycle, etc.);
- specific procedures (according to the services identified).

5. Relationship with constituency and communication strategy: this element describes interactions with constituencies and stakeholders, and defines:

   - constituencies;
   - interactions with the constituency;
   - roles and responsibilities for the interaction;
   - communication approach and strategy.

6. Technology to automate the processes: these are required to run effective operations, including:

   - network design;
   - general purpose infrastructure (phones, faxes, shredders, projectors, coffee machines, etc.);
   - hardware and software components such as datacentre, network, servers to run CIRT virtual machines, workstations for staff, all licences, and devices for physical access control.

7. CIRT premises: this element plans for a physical CIRT team, including identifying and defining:

   - physical location requirement (different rooms, secure zoning, etc.);
   - plans and disposition of rooms;
   - general purpose equipment such as air conditioning, datacentre, etc.

8. Personnel acquisition and skills development: these are needed when a new CIRT team is established, requiring new skillsets, including identifying and defining:

   - organizational structure;
   - skillsets for staff;
   - staff profiles;
   - training requirements.

9. Onsite Mission: this requires five working days for local activities, presentation and validation of design, as well as fine-tuning activities. The related activities include:

   - meetings with the key players and the CIRT constituency;
   - questionnaire responses review and gap-filling where necessary;
   - CIRT Design Document updates in line with discussions held on-site;
   - CIRT Design Document content and approach validation for implementation;
   - project timeline of all stakeholder actions (country and ITU);
   - wrap-up after visit;
   - final report delivery;
   - review and publication production process.

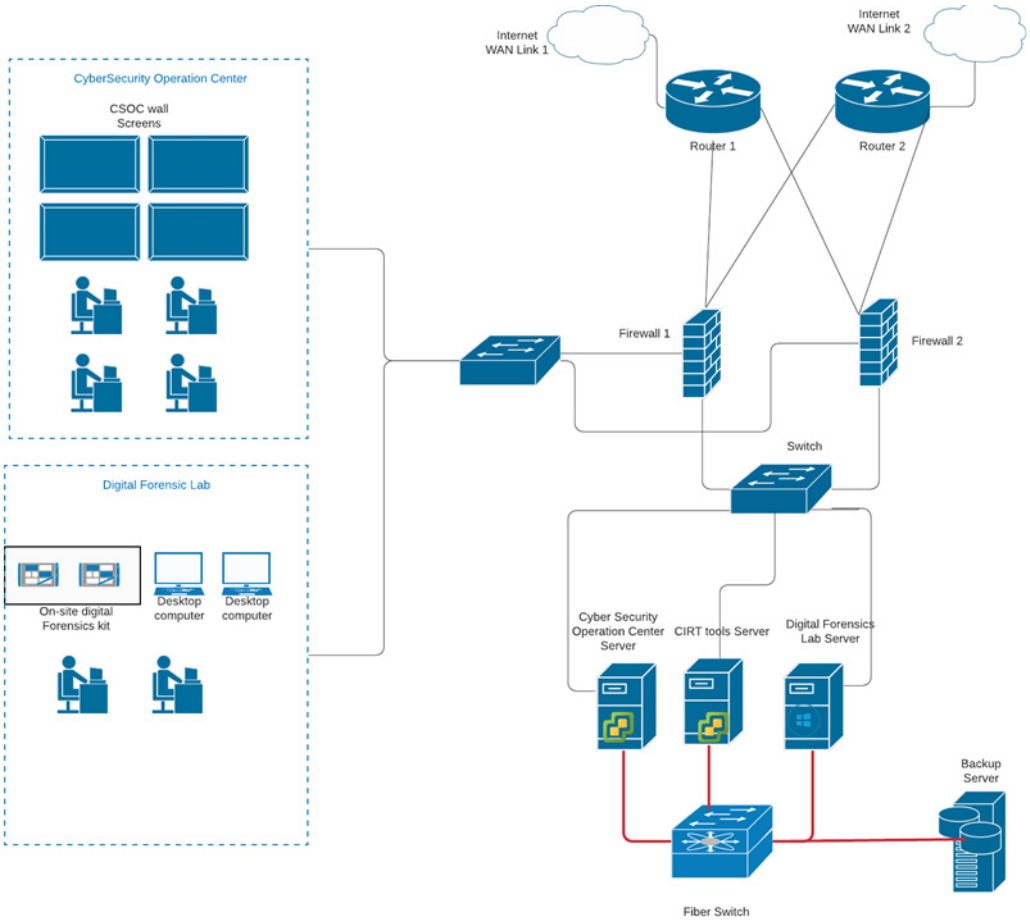
Additionally, human resources, premises, and hardware and software are essential components of a national CIRT that must be identified and assigned to the CIRT on a permanent basis, for which the following design plans must be validated: CIRT vision and mission; CIRT constituency; service catalogue; organizational model; training plan; technology; and premises.

It is recommended to have high-availability of two firewalls, two datacentres and user switches, and two servers throughout the CIRT:

- Firewall: connected to the Internet, and connected to at least four zones (DMZ, CIRT staff, CIRT servers, management);
- network switches for servers and users, as well as WiFi access point for guests and CIRT staff;
- servers to run virtual machines (it is recommended to have at least two servers with 32 cores, 128 GB RAM, and SSD storage for virtual machines) with power protection (UPS);
- backup server (with tapes, or alternative offline storage); and
- CIRT staff laptops or workstations with at least i5, 16 GB ram, 512 GB SSD, external monitors, and all utilities.

Figure 4 depicts the minimum physical infrastructure.

## Figure 4: Sample hardware schema




Source: ITU

### Results of the design phase

The CIRT Design Document sets out the results of activities and includes:

- project management content;
- list of workflows;
- processes map;
- list of policies and procedures;
- engagement strategy plan;
- networks design;
- list of necessary hardware and software equipment and tools;
- plans, schematics, etc.;
- profile templates;
- training plans.

## 3.3 Phase 3: Establishment

**Description**: During the establishment phase the operations of the CIRT are constructed.

**Preconditions:** ITU has assisted in the design and approval of the detailed CIRT Design Document.

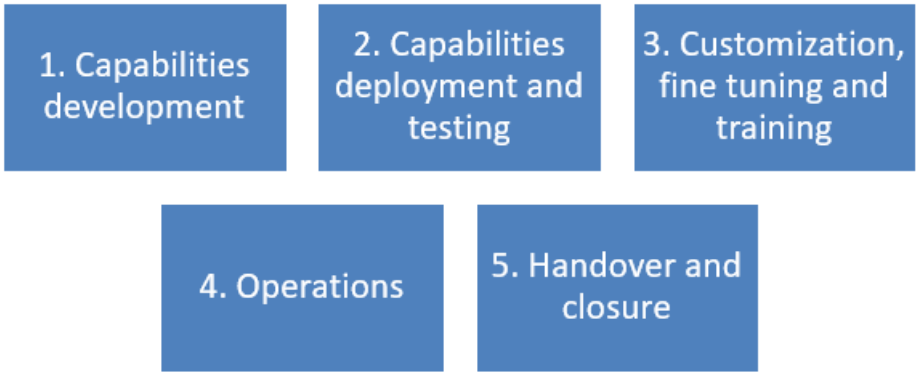
**Outcome:** Implementation and successful hand-over of the CIRT operations.

### Scope and methodology

The establishment phase focuses on building technical, process, services, organizational capabilities of the CIRT in accordance to approved CIRT Design Document and include the following activities:

- daily communication between ITU CIRT project manager and assigned local CIRT manager via email, messaging, and voice channels;
- installation of hardware by local IT team;
- remotely install and configure the required CIRT systems;
- handover, fine-tuning, and training;
- documenting implementation (documentation list is presented in outcome section);
- sign-off on handover of systems,
- complete documentation.

Figure 5: Aspects of establishment phase




Source: ITU

During the establishment phase the following aspects are covered:

1. Capabilities development: this involves the definition of:
    - processes and related workflows identified during the design phase;
    - policies and procedures identified during the design phase;
    - technology requirements and elaborating infrastructure plans (physical and logical), diagrams, etc.;
    - human resource needs including structure, organization, and training plans.
2. Capabilities deployment and testing: this consists of remote installation and testing of technology. The related activities are the following:
    - incident handling tracking system;
    - helpdesk, web site, mailing list software;
    - hardware and software, databases, data repositories, incident analysis tools, and data analysis tools.
3. Customization, fine-tuning and training: this covers the adjustment of automation technology to fit all developed use cases and workflows including:
    - fine tuning of IT infrastructure and related applications;
    - fine tuning of processes and workflows, policies and procedures and related documentation;
    - finalizing hardware configuration and software installation;
    - training on implemented processes and procedures, incident handling, infrastructure operations, administration of all tools, as well as detailed workflows for all delivered services.
4. Operations: this activity ensures ticketing and post deployment support (for a period of 6 month) and needs to be effective upon launch as many questions will arise.
5. Handover and closure: this stage closes the project, including:
    - final review of the documentation;
    - post deployment assessment and lesson learned;
    - project closure.

Note: The establishment service will only begin when certain assets are made available by the beneficiary country following the delivery of the design service. This includes three main components that must be identified and in place before the establishment service starts:

1. Human resources (CIRT staff);
2. Physical premises (staff offices, datacentres, CIRT operation room, etc.);
3. IT infrastructure (hardware and software), such as servers, end-user laptops and desktops, security and network appliances, office automation, etc. and related licences.

### Results of the establishment phase

The establishment phase results in the operational acceptance of the CIRT by the beneficiary country. This includes a trainings report and the documentation package:

- policy documents, flowcharts on the procedures;

- IT infrastructure plan and related documentation;
- operating manuals on the solutions deployed;
- standard operating procedures (SOP) documentation;
- training material;
- email and phone support according to the SLA agreed with the CIRT;
- user acceptance signoff (UAS signed);
- closure report.

## 3.4 Phase 4: Enhancement

**Description**: The enhancement phase covers improvements to new services based and aligned with the FIRST CSIRT Services Framework and better automation of existing services.

**Preconditions**: ITU agrees to expand services scope and improve operations.

**Outcome**: Strengthened and enhanced CIRT operations and successful handed-over.

### Scope and methodology

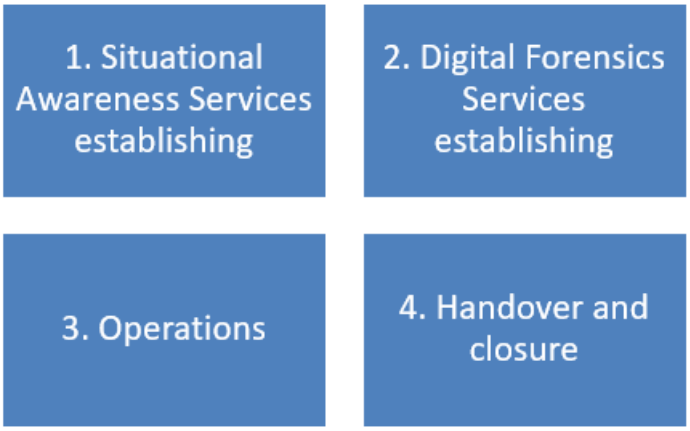
The enhancement phase focuses on improving the technology, process, services, and organizational capabilities of the national CIRT according to defined needs, including:

- agreement on objectives to be reached, and implementation methods;
- if needed, onsite expert visits;
- provisioning of additional hardware on site, installed by local IT team;
- remote installation and configuration of systems;
- onsite handover, fine-tuning and training;
- documentation of implementation;
- sign-off on handover of systems and documentation.

Standard offering for the enhancement phase establishes new services. The first two services below are well defined in the CIRT framework, and the remaining three services are custom-built for each client:

1. situation awareness service, utilizing threat intelligence and honeypot platforms, deployed locally;
2. digital forensics service, utilizing digital forensics platforms and training;
3. cybersecurity threat intelligence (CTI) service for detecting infected infrastructure, such as monitoring digital pollution;
4. security monitoring of government sector networks, for collective cyber defense of participating organizations;
5. improvement of other services, such as automation of alert publishing, vulnerability management, etc.

## Figure 6: Enhancement phase aspects are covered




Source: ITU

1. Situational awareness services: this establishes CIRT knowledge on what is happening in the monitored networks by deploying sensing nodes (honeypots) and collecting data from them centrally for analysis. The related activities are:

    - environment analysis:
        - determine hardware requirements;
        - outline operation requirements for technology activities;
        - develop a standard set of criteria and terminologies for categorizing and defining incidents, activities, and events;
        - prepare training materials and user guides for the deployment stage.
    - capabilities development:
        - procure sensor appliances;
        - install, configure and test the technology environment for CIRT operations;
        - prepare installation guides;
        - define procedures for network security monitoring, advanced incident handling, reporting;
        - define specific processes and workflows;
        - customize dashboard.
    - customization, fine-tuning and training:
        - conduct system integration tests;
        - deploy sensors at identified locations;
        - finalize hardware configuration and software installation;
        - customize and fine tune the deployment of the sensors and the dashboard;
        - delivery of training.

2. Digital forensics services: this provides artifact analysis capability for CIRT, which allows for better interaction with the constituency in which cybercrime is the cause of incidents. Service enables proper preservation of evidence and analysis. The related activities are:

    - environment analysis:
        - identify requirements and activities of the Digital Forensic Centre and prepare related guidelines, including reporting requirements, and processes;

- identify necessary toolkits to ensure a proper project execution based on best practices;
- identify clear roles and responsibilities for the operation and maintenance of the Digital Forensic Centre;
- identify digital forensics processes to be linked with current incident handling processes;
- prepare the plan based on the combination of best practices and country requirements assessment.

- capabilities development:
  - implement strategies and methods for building trusted relationships and collaborations with other partners or stakeholders;
  - finalize the installation of the Digital Forensic Centre lab tools;
  - prepare the training materials and user guides;
  - develop the standard set of criteria and consistent terminology for categorizing and defining incidents, activities, and events.

- customization, fine tuning and training:
  - integrate and finalize the digital forensic processes and workflow with the current CIRT processes and workflows;
  - finalize and conduct system integration tests;
  - conduct the capacity building programme.

3. Operations upon launch need to be supported for effective work, as many questions will arise. Activity is to ensure ticketing and post deployment support (for a period of six months).
4. Handover and closure stage are final closing of project. The related activities are the following:

- final review of the documentation;
- post deployment assessment and lesson learned;
- project closure.

### Results of the enhancement phase

The enhancement phase results in operational acceptance of new or enhanced CIRT services. This includes a trainings report and a documentation package:

- policy documents, flowcharts on the procedures;
- IT infrastructure plan and related documentation;
- operating manuals on the solutions deployed;
- standard operating procedures (SOP) documentation;
- training material;
- email and phone support according to the SLA agreed with the CIRT;
- user acceptance signoff (UAS signed);
- closure report.

# Annex: Risks, roles and responsibilities

## Risk management

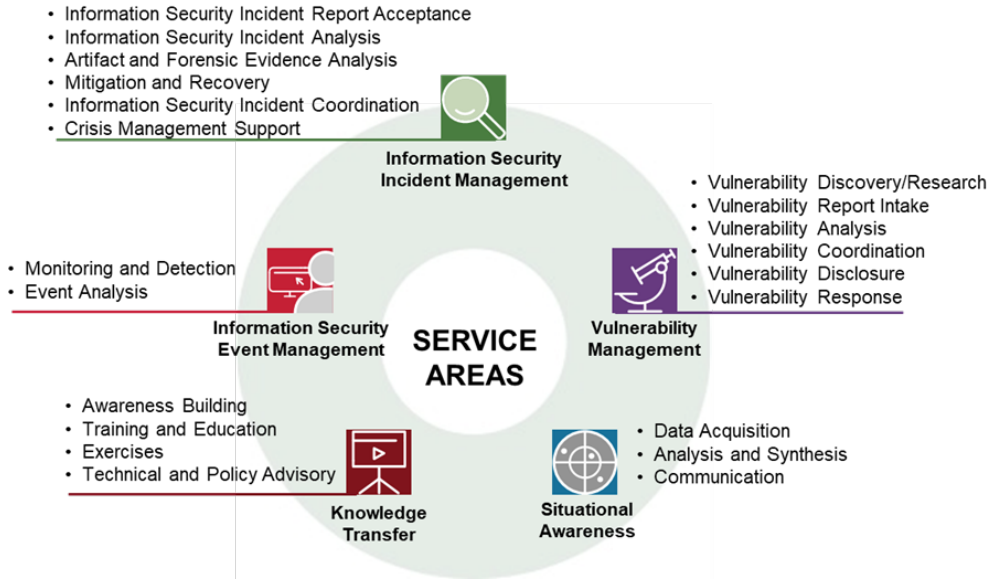
There are two main risks foreseen for CIRT framework projects:

1. In-country activities may suffer delays due to unforeseen and unanticipated local events or circumstances. Getting the commitment from the interested country in the early stages of planning will minimize this risk.
2. Human resources assigned to operate the national CIRT are not recruited in time (they need to be trained), which would delay the completion of the project. This risk is reduced by the commitment of the country to recruit staff with the appropriate profile before the training phase begins.

## FIRST CSIRT Services Framework

The FIRST CSIRT Services Framework is a high-level document describing in a structured way a collection of cyber security services and associated functions that CIRT/CSIRT/CERT and other teams providing incident management related services may provide.

The below figure displays the CSIRT Services Framework Service Areas and Services. Further information can be found on the FIRST website: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf




## Roles and responsibilities

ITU is responsible for the overall management of the project implementation, supervision, monitoring, coordination and evaluation during the different phases of the framework implementation. Specifically, ITU will:

- Perform the activities as per the expected project deliverables table.

- Provide staff resources for the coordination and management of the project, including planning, implementation, monitoring and evaluation of the project for the beneficiary country.
- Manage the recruitment of external experts (if necessary) and supervise their work.
- Manage the procurement process of hardware and services.
- Provide expertise and international experience to enable realization of the project objectives in an effective and efficient manner.
- Administer the project in accordance with applicable ITU rules, regulations and procedures. Accordingly, personnel will be engaged, administered, and contracted, in accordance with the provisions of such rules, regulations and procedures.
- Establish and maintain periodic contact and communication with the beneficiary country focal point(s) to ensure alignment of the delivery.
- Be responsible for administrative and logistic processes and procedures related to any on-site visits.
- Provide advice and assistance to the beneficiary country, when it is required, during and after project implementation.
- Produce quarterly project progress reports.

The beneficiary country takes the following responsibilities during the different phases of framework:

- Designate qualified technical personnel to work closely with the other stakeholders on the project implementation.
- Provide information required for carrying out the planned and agreed project activities.
- Provide necessary hardware and basic software (with appropriate licences).
- Provide human resources to efficiently operate the CIRT.
- Provide physical space, as required by the project nature and for the establishment of CIRT.
- Provide administrative support required, including with a view to issuing and delivering visas to the members of the project team and facilitating customs clearance of any necessary equipment, materials, etc. required during the project implementation and any other assistance that may be required for the successful project implementation.
- Designate national counterparts that will assist in hosting the project team, provide local logistics including deployment of equipment. The national counterparts designated by the beneficiary country will assist ITU by providing accurate information relevant to the project.

**Office of the Director**
**International Telecommunication Union (ITU)**
**Telecommunication Development Bureau (BDT)**
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

**Office of Deputy Director and Regional Presence**
**Field Operations Coordination Department (DDR)**
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

**Digital Networks and Society (DNS)**

Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

**Digital Knowledge Hub Department (DKH)**

Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

**Partnerships for Digital Development Department (PDD)**

Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

## Africa

### Ethiopia

**International Telecommunication Union (ITU) Regional Office**
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

### Cameroon

**Union internationale des télécommunications (UIT)**
**Bureau de zone**
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

### Senegal

**Union internationale des télécommunications (UIT)**
**Bureau de zone**
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

### Zimbabwe

**International Telecommunication Union (ITU) Area Office**
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

## Americas

### Brazil

**União Internacional de Telecomunicações (UIT)**
**Escritório Regional**
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

### Barbados

**International Telecommunication Union (ITU) Area Office**
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

### Chile

**Unión Internacional de Telecomunicaciones (UIT)**
**Oficina de Representación de Área**
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

### Honduras

**Unión Internacional de Telecomunicaciones (UIT)**
**Oficina de Representación de Área**
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: ituteguciglapa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

## Arab States

### Egypt

**International Telecommunication Union (ITU) Regional Office**
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

## Asia-Pacific

### Thailand

**International Telecommunication Union (ITU) Regional Office**
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailand

*Mailing address:*
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Email: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

### Indonesia

**International Telecommunication Union (ITU) Area Office**
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

*Mailing address:*
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Email: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 5521

## CIS

### Russian Federation

**International Telecommunication Union (ITU) Regional Office**
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Email: itumoscow@itu.int
Tel.: +7 495 926 6070

## Europe

### Switzerland

**International Telecommunication Union (ITU) Office for Europe**
Place des Nations
CH-1211 Geneva 20
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-34941-7

Published in Switzerland
Geneva, 2021
Photo credits: Shutterstock