International Telecommunication Union

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

ITU-IMPACT MISSION PROGRAMME TO

CIRT READINESS ASSESSMENT

JALAN IMPACT, 63000 CYBERJAYA, MALAYSIA
www.impact-alliance.org

Contents

Overview

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfill all the descriptions of duties as stipulated in the Project Scope below. The National CIRT will provide a capability to identify, respond and manage cyber threats and at the same time will enhance the cybersecurity posture of the sovereign country.

The final outcome and deliverable of this mission will be a report which will contain key issues, key findings and analyses, recommendations and a phased implementation plan for setting up the National CIRTs. The report will be prepared and submitted to ITU within 4 weeks after the Experts have completed the on-site assessment and returned to base.

Collectively, with the integration of best practices and processes, experienced people and robust technology, it is believed that the National CIRTs can play the role of maintaining round-the-clock vigilance to defend critical national infrastructure/assets against cyber-attacks, and also serve as a critical cyber-nerve center in analysing threat information; which can extend towards alerting public and private sector agencies pre-emptively in enhancing their security awareness, assist in remediation of identified vulnerabilities, and improving overall security posture.

ITU-IMPACT Experts

There will be 2 Experts assigned to carry out this assessment exercise. Both of them are knowledgeable in the field of Cybersecurity and CIRT, and also in the use of the applicable international standards and best practices involved.

The identified experts for this mission are:

Anuj Singh
Director, Global Response Centre
IMPACT
anuj.singh@impact-alliance.org

Jairam Ramesh
Manager, Security Assurance
IMPACT
jairam.ramesh@impact-alliance.org

(NOTE: a presence of an ITU representative is always recommended. ITU HQ and the Regional Office would coordinate to make sure an ITU Professional is present)

Project Details

Scope

The mission will be carried out from **[Dates]** excluding travel dates. Under the direction of the ITU, in cooperation with the national counterparts and in close collaboration with the relevant Ministries of the respective countries, the Experts will undertake the following activities on-site and off-site:

a) Study and analyse the countries' current cybersecurity status and needs.
b) Provide high-level recommendations to improve the cybersecurity posture of the countries.
c) Study and suggest institutional and organisational requirements, and arrangements for setting-up National CIRTs.
d) Capacity building program for the CIRTs.
e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
i) Design specifications for hardware and software for the CIRTs.
j) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU; and,
k) Carry out any other duties in his/her specialty as may be assigned to him/her by ITU.

Assessment Approach

The ITU-IMPACT personnel assigned to carry out this assessment exercise are knowledgeable in the field of cybersecurity and CIRT, and also in the use of the applicable international standards and best practices involved. The scope of this assessment is limited to the job scope stipulated above and no attempt will be made to go beyond the scope.

The ITU-IMPACT team will start its on-site activities with a brief opening meeting to review this "Assessment Plan" and confirm the on-site schedule. If necessary this plan can be adjusted to suit the actual availability of the officials who will participate in the assessment. Following this meeting the team will undertake a brief tour of getting to know the area and other relevant personnel before starting the assessment process. The team will work together most of the time but may occasionally undertake short assessment sessions individually when this is required.

The team will record all findings needed to establish the "As-Is" state of the facility and the personnel. These findings will be recorded on a confidential checklist prepared by the team. The assessment methods will be meetings, trainings, interview sessions, and one to one or one too many discussions. A verbal report will be provided at the closing meeting to acquaint the officials with the findings and to offer preliminary recommendations.

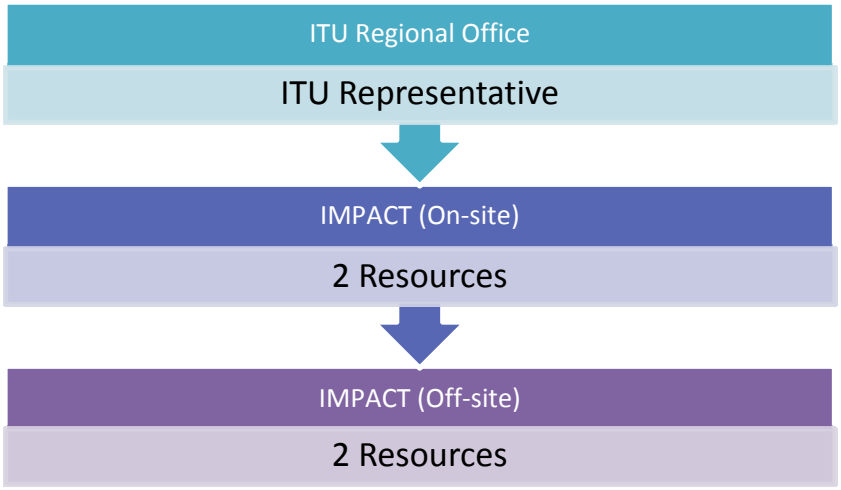
Phase 1: Initialisation & Planning Stage

Deliverables / Milestones	Estimated Effort
Visit [**Location**] to assess the participating country's readiness to implement CIRT and to collect and prepare all relevant documentation including: • Standard Operating Procedures, roles and responsibilities of CIRT • Detailed Terms of Reference for Chief Security Officer of CIRT • Areas of proactive and reactive response measures • Membership Policies for the proposed CIRT. • Policies to coordinate with internal agencies as well as international CIRTs taking into account policies for ITU IMPACT initiative on CIRT • Specifications for hardware and software for the proposed CIRT • Conduct a five day combined workshop to impart knowledge and skills for operation, maintenance and coordination of CIRT • Perform interviews, with the concerned representatives for each of the participating countries.	Onsite 5 + 1 days not including travel.

Phase 2: Reporting Stage

Deliverables / Milestones	Estimated Effort
Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU Regional Office for [**Location**].	56 days for 5 countries in total

Project Team Organisation



Project Financials

The project is [**conditional**] funded by ITU.

Project Risk Management

Initial Defines Risks	• Political risk - local political insurgencies • Internal risk • Schedule risk - unable to complete the on-site assignment within the stipulated days • Technical risk - Resources availability in the country
Project Assumptions	• Availability of resources for the mission • All documents & information are provided by these personnel • Conducive working environment with all facilities is provided (Please refer to Appendix B for Facilities Needed)
Project Constraints	• Time required to prepare
Project Interdependencies	• None
Issue and Change Management	• Will be administered

Proposed Countries

LIST OF ATTENDING COUNTRIES

Who should attend

A National CIRT is expected to coordinate on Cybersecurity Defence and Response with other bodies within the country and work with relevant governmental agencies to respond to any incidents at a National/agency level. It is important to meet up with key stakeholders to achieve initial consensus on the expectations, strategic direction, definitions, and responsibilities of the National CIRTs.

Who should attend?

- Representatives from Ministries
- Central monetary agency and local banks
- Telco's and ISPs
- Regulatory bodies
- National security agencies
- Academia and national research bodies
- Law enforcement agencies
- Policy makers
- Local private organizations involved in security initiatives

Programme Schedule

Day1

Time	Activity
TBD	- Depart from Kuala Lumpur International Airport

Day 2

Time	Activity
All Day	- Arrival at [**Location**] - Check in Hotel - Self administration - Preparation for the mission

Day 3

Time	Activity
09:00 – 09:30	- Speaker Engagement
09:30 – 10:40	- Ice Breaking & Program Overview Sessions - IMPACT Presentation - ITU-IMPACT Collaboration Presentation - Video presentation
10:40 – 11:00	- Break
11:00 – 12:30	- CIRT Introductory Training
	- Lunch
14:00 – 15:00	- Fundamentals of Computer Incident Handling Training
15:00 – 15:20	- Break
15:20 – 15:30	- Briefing Exercise 1
15:30 – 16:30	- Exercise 1 (Setting up your CIRT)
16:30 – 17:00	- Wrapping up Exercise 1

Day 4

Time	Activity
09:00 – 10:30	- Video presentation - Steps of Incident Handling Training
10:30 – 10:50	- Break
10:50 – 11:00	- Briefing Exercise 2
11:00 – 12:30	- Exercise 2 (Triage, Prioritization and Basic Incident Handling)
12:30 – 14:00	- Lunch
14:00 – 14:30	- Video presentation - Wrapping up Exercise 2
14:30 – 14:40	- Briefing Exercise 3
14:40 – 15:40	- Exercise 3 (Incident Handling Procedure)
15:40 – 16:00	- Break
16:00 – 16:30	- Exercise 3 (ctd..)
16:30 – 17:00	- Wrapping up Exercise 3

Day 5

Time	Activity
09:00 – 10:30	- IMPACT GRC Portal, ESCAPE & CIRT Portal Walkthrough
10:30 – 10:50	- Break
10:50 – 11:00	- Briefing Exercise 4
11:00 – 12:30	- Exercise 4 (Vulnerability Handling)
12:30 – 14:00	- Lunch
14:00 – 14:30	- Video Presentation - Wrapping up Exercise 4
14:30 – 14:40	- Briefing Exercise 5
14:40 – 15:40	- Exercise 5 (Establishing external contacts)
15:40 – 16:00	- Break
16:00 – 16:30	- Exercise 5 (ctd..)
16:30 – 17:00	- Wrapping up Exercise 5

Day 6

Time	Activity
09:00 – 09:20	- Video Presentation - Cybersecurity Landscape
09:20 – 09:30	- Briefing Exercise 6
09:30 – 10:30	- Exercise 6 (Large Scale Incident Handling)
10:30 – 10:50	- Break
10:50 – 12:00	- Exercise 6 (ctd..)
12:00 – 12:30	- Wrapping up Exercise 6
12:30 – 14:00	- Lunch
14:00 – 14:10	- Briefing Exercise 7
14:10 – 16:30	- Exercise 7 (Operational CIRT) - Break
16:30 – 17:00	- Wrapping up Exercise 7

Day 7

Time	Activity
09:00 – 09:20	- Video Presentation - Warm up session
09:20 – 09:30	- Briefing Exercise 8
09:30 – 10:30	- Exercise 8 (Cooperation with Law Enforcement Agencies & COP)
10:30 – 10:50	- Break
10:50 – 12:00	- Exercise 8 (Ctd..)
12:00 – 12:30	- Wrapping up Exercise 8
12:30 – 14:00	- Lunch
14:00 – 14:10	- Briefing Exercise 9
14:10 – 16:30	- Exercise 9 (Incident Handling & Role Playing)
16:30 – 17:00	- Wrapping up Exercise 9
17:00 – 17:30	- Wrap up session

Day 8

Time	Activity
TBD	- Check-out from hotel - Depart from [**Location**]

Breakout Session (Detailed)

Day 4: Breakout Assessment Session:

1. ICT readiness of the country
2. Identifying stakeholders
3. Vision, mission and goals
4. Cybersecurity initiatives within the country

Day 5: Breakout Assessment Session:

1. Identifying constituencies
2. Place in organisation or reporting structure
3. Relationships with other CIRTs
4. Financial model

Day 6: Breakout Assessment Session:

1. Identifying CIRT services
2. Manpower planning
3. Physical infrastructure
4. Hardware and software

Day 7: Breakout Assessment Session:

1. Child Online Protection (COP)
2. Cybersecurity research initiatives
3. Training needs assessment
4. Cybersecurity legislative framework and policy

Toolkit (on-site)

Listed below are items that are required to be made available on-site to the Experts to complete the mission successfully. The organising team shall be responsible to make the items available. Should there be any issue in ensuring the availability of any of the items; the ITU/IMPACT Experts must be notified at least five (5) days before the departure of the Experts from Kuala Lumpur.

1. Participants are required to bring a notebook computer each
2. Conducive training / seminar room
3. Broadband Internet connection for all participants
4. LCD Projector
5. Projector screen
6. White board
7. Marker pens (multiple colours)
8. A4 papers for classroom exercises
9. Big-sized white papers for student presentations
10. Laser printer
11. Audio connectivity for laptops
12. Sufficient power for all participants.

END OF DOCUMENT