

JALAN IMPACT, 63000 CYBERJAYA, MALAYSIA

www.impact-alliance.org

08

**Fall**

 

**READINESS ASSESSMENT TO ESTABLISH NATIONAL CIRT FOR**

**<COUNTRY>**

Contents

[**Introduction 3**](#_Toc306370673)

[**Preamble 4**](#_Toc306370674)

[**SECTION 1 – Identifying Stakeholders 5**](#_Toc306370675)

[**SECTION 2 – Mission & Target 9**](#_Toc306370676)

[**SECTION 3 – Cybersecurity Initiatives within the Country 11**](#_Toc306370677)

[**SECTION 4 - Constituency 18**](#_Toc306370678)

[**SECTION 5 – Place in organisation / Reporting Structure 24**](#_Toc306370679)

[**SECTION 6 – Relationships with other CIRTs 28**](#_Toc306370680)

[**SECTION 7 – CIRT Services 30**](#_Toc306370681)

[**SECTION 8 – Financial Model 36**](#_Toc306370682)

[**SECTION 9 – Manpower Planning 39**](#_Toc306370683)

[**SECTION 10 – Research on Cybersecurity in the Country 42**](#_Toc306370684)

[**SECTION 11 – Physical Infrastructure 46**](#_Toc306370685)

[**SECTION 12 – Hardware & Software 52**](#_Toc306370686)

[**SECTION 13 – Performance Evaluation 54**](#_Toc306370687)

[**SECTION 14 – ICT Sustainability and Readiness of the Country 57**](#_Toc306370688)

[**SECTION 15 – Cybercrime Related Laws, Legislations and Frameworks 65**](#_Toc306370689)

[**SECTION 16 – Cyber / e-Government Frameworks 69**](#_Toc306370690)

[**SECTION 17 - Attestation 70**](#_Toc306370691)

[**APPENDIX A 71**](#_Toc306370692)

[**APPENDIX B 72**](#_Toc306370693)

[**APPENDIX C 73**](#_Toc306370694)

# Introduction

The primary objective of this questionnaire is to assist the assessor in the assessment of a country’s readiness to establish a Computer Incident Response Team (CIRT). Ideally this questionnaire should be used at the early stages when a country has obtained management support to form a National CIRT. This document is used as a basis to gather as much information as possible to assist the planning, development and implementation of CIRT.

Existing CIRTs looking to evaluate the completeness and comprehensiveness of their CIRTs can adopt this questionnaire as a standard framework for their assessment.

The questionnaire is divided into several sections and the assessor is advised to find answers to all the relevant questions in the sections.

# Preamble

**ITU-International Multilateral Partnership Against Cyber Threats (IMPACT)** is a strong advocate of National CIRTs (Computer Incident Response Teams) which provide a capability to identify, defend, respond and manage cyber threats and enhance cyberspace security in the sovereign country. This questionnaire is focused on providing ITU-IMPACT inputs to assess the readiness of the country to establish a National CIRT.

The areas covered in the questionnaire are:

* Current organisational structures to combat cyber threats
* Current legislative frameworks for addressing cybercrime.
* Current Capabilities – Human Resource / Technology
* Financial capability to operate a National CIRT

For a national CIRT in the set-up stage, this document is critical in providing valuable input on how to actually shape a national CIRT. All questions are designed to collect vital information in its respective areas and it is imperative that they are answered comprehensively to achieve the desired results.

# SECTION 1 – Identifying Stakeholders

 **Question 1.1**

**Which Government agencies and people will be involved at each level of the CIRT planning, implementation and operation?**

*(Guideline: List the agency names,**contact details, the names of the people, positions, phone numbers and email addresses)*

**Question 1.2**

**Who will be in charge of performing security or incident response functions within the CIRT?**

 *(Guideline: List down all their names, positions, phone numbers and email addresses)*

**Question 1.5**

**Please identify the benefits that the agencies will receive from the CIRT.**

**Question 1.6**

**Is there any security strategy/policy developed or initiated for the Critical Information**

**Infrastructure Protection (CIIP)? If yes, please list them below.** *(Guideline: There are 10 identified*

*categories of CNI. Please refer to Appendix B)*

**Question 1.6**

**Is there any security strategy/policy developed or initiated for the Critical Information Infrastructure Protection (CIIP)? If yes, please list them below.**

*(Guideline: There are 10 identified categories of CNI. Please refer to Appendix B)*

**Question 1.7**

**If the answer is "yes" for the above question, which Government agency leads the CIIP effort for policy development and operations?**

*(Identify how the effort is conducted - any trusted forum, how the input from participants are obtained and analyzed)*

**Question 1.8**

**Tick all the relevant agencies / ministries /sectors that are part of Critical Infrastructure (CI).**

|  |  |  |
| --- | --- | --- |
|  Finance |  Communication |  Transport |
|  Energy |  Water |  Emergency Services |
|  Food |  Public Safety |  Health |
|  Public Services |  |  |

**Question 1.9**

**Are there any other relevant ministries/agencies/sectors as a part of Critical Infrastructure (CI).**

**Question 1.10**

**Do the stakeholders/CI follow any standards or policies?**

# SECTION 2 – Mission & Target

 **Question 2.1**

**Why does your country need a CIRT?**

*(Guideline: Clearly state the objectives of establishing a CIRT)*

 **Question 2.2**

**What are the expectations of the Government from this CIRT establishment (the primary target)?**

*(Guideline: A clearly defined expectation will help to determine the vision and missions, both the short-term and long-term goals of the CIRT. Lack of a clear understanding of goals and objectives will result in needless expend of effort and resources)*

**Question 2.3**

**Would the CIRT be allowed to react to a situation or incident?**

*(Guideline: A clearly defined expectation will help to determine the vision and missions of the CIRT. This will also allow for better understanding of correct priorities to ensure that they respond to the most important activity / threats.)*

**Question 2.4**

**Is the CIRT going to be a part of a bigger organisation?**

*(Guideline: If it is, the mission statement of the CIRT Must complement the missions of the organisation. Meet the policy makers of the parent organisation to obtain more information on its mission & vision.)*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

**Question 2.5**

**If the answer is "yes" please provide information about the organisation***.*

*(Guideline: If it is, the mission statement of the CIRT must complement the missions of the organisation. Meet the policy makers of the parent organisation to obtain more information on its mission & vision.)*

# SECTION 3 – Cybersecurity Initiatives within the Country

**Question 3.1**

**Were there any attempt to establish a security incident management organisation or a CIRT-like team by either the Government or private sector?**

*(Guideline: This question is connected to the next two questions.)*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

**Question 3.2**

**If the answer is “yes” for the above question, which organisation was or is responsible and list the contact details (it can be Government or private sector)? Please get any documentation from the project.**

*(Guideline: This is important to understand the previous incident management initiatives. It is also important to meet the people / organisation involved to get a better understanding by interviewing them. It is also advisable to meet the private-based CIRTs (if any) such as run by MNCs, to understand how they operate in the country. The documentation should cover all the policies, procedures, processes and so on.)*

**Question 3.2.1**

**From the Question 3.2 - Is this organisation a private entity or Government funded organisation? Please describe its incorporation. Are there any cooperation agreements between the organisation and any Governmental agencies on information sharing and incident management?**

**Question 3.3**

**If the answer is “yes” for the above questions and it was discontinued or delayed, what are the reasons for discontinuing/delaying? What is the status of the project and when it was stopped? Please provide any documentation related to the project if possible.**

*(Guideline: This is important to understand the reasons for discontinuing the project. The reasons could be lack of resources, political, environmental, economic, etc.)*

**Question 3.4**

**Have any cybersecurity incidents been reported in the past?**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

**Question 3.4.1**

**If yes, please provide some of the details of the incidents and what was done to respond to the incidents.**

*(Guideline: The incidents may have been reported to any organisation within the country or outside the country. This information is important to understand the trend and the level of awareness on cybersecurity among the people of the country)*

**Question 3.5**

**How many ISPs are there in the country? If circumstance permits, can your organisation arrange to meet the key personnel from all these ISPs (or at least the two biggest ISP’s).**

*(Guideline: To understand their roles in cybersecurity and their initiatives in security incident management. Also to understand their expectations from the CIRT)*

**Question 3.6**

**(At the ISP) Have the ISPs experienced or detected any cyber incidents recently?**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

**Question 3.6.1**

**Please provide additional information if above question's answer is "yes".**

*(Guideline: What was the nature of the cyber incidents and what were the steps taken to mitigate and contain the attacks.)*

Question 3.7

Does your country have a long-term cybersecurity strategy or plan? If yes could you elaborate in brief.

(such as a National Cybersecurity Strategy or Policy)

Question 3.8

If there are some cybersecurity initiatives in progress, or cybersecurity strategies/policies in place do you think there might be some overlapping areas of responsibility in their scopes?

Question 3.9

Are there any programs or subjects offered or conducted in schools and other educational institutions or youth establishments that promote the safe use of the Internet to children and young people? If yes provide more details.

Question 3.10

Has there been any awareness campaigns related to cybercrime, cybersecurity, child online protection, or similar activities in your country? Please share the campaign activities and success stories if any?

**Question 3.11**

**What are the main priorities in your country? Use the table below to rate them.**

*(1-highest, 2-medium and 3-low priorities)*

|  |  |  |
| --- | --- | --- |
| 3.11.1 | Development of cybercrime policy and legislation |  |
| 3.11.2 | Human Capacity Building and Trainings in the areas legislation and technical expertise on cybersecurity |  |
| 3.11.3 | Public awareness on online security for citizens, children, youth and small as well as medium businesses |  |
| 3.11.4 | Better coordination at the National level on cybersecurity among various stakeholders |  |
| 3.11.5 | Better coordination and cooperation at the international level |  |
| 3.11.6 | If you think that there are other priorities please list them below |  |

# SECTION 4 - Constituency

Question 4.1

What type of services will the CIRT be providing to its constituents?

(Guideline: There are 3 types: i.e. unbounded, bounded and hybrid. Unbounded: provide services to anyone requesting it (public). Bounded: bound by some constraints such as just for the funding source / just for the Government agencies. Hybrid: Combination of both)

Question 4.2

If the services are bounded, who are the prospective recipients of the services?

(Guideline: This should also match the stakeholders identified earlier.)

Question 4.3

If the services are hybrid, who are the prospective recipients?

Question 4.4

What will be the criteria used to bind the services.

(Guideline: Some CIRTs bound their services by domain name, geographical, political, technical or contractual)

Question 4.5

If the services are hybrid, how does the CIRT plan to draw the line between bound and unbounded services?

(Guideline: This is important to avoid confusion and overlapping of services. It is also important to protect sensitive data from being disclosed to unauthorized parties. Check if the Government has an information classification policy in place and get the documents)

Question 4.6

Will the CIRT extend its services to corporate or non-Governmental organisations/agencies?

(Guideline: This is important to avoid confusion and overlapping of services. It is also important to protect sensitive data from being disclosed to unauthorized parties.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 4.6.1

If the above answer is yes, please provide additional information.

(Guideline: This is important to avoid confusion and overlapping of services. Also important to protect sensitive data from being disclosed to unauthorized parties. Which organisations?)

Question 4.7

Will the CIRT advertise its constituency?

(Announce its members and those receiving services).

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 4.7.1

Please provide additional information, if the above answer is "yes".

(Guideline: Some CIRTs don’t advertise their constituency due to privacy and proprietary information but this poses a problem because given an incident, the external sites will not know the constituency the organisation falls under.)

Question 4.8

Will the CIRT with National Responsibility permit the constituents to have overlapping service offerings at their CIRTs?

(Guideline: Overlapping CIRTs may create confusion and duplication of effort during a remediation exercise but it can be managed by drawing a separation of duties line.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 4.8.1

Please provide additional information to your answer.

(Guideline: Overlapping CIRTs may create confusion and duplication of effort during a remediation exercise but it can be managed by drawing a separation of duties line.)

Question 4.9

What is the level of authority between the CIRT and its constituency?

(Guideline: There are 3 levels of authorities; i.e. full, shared and none. Explain each and every type of authorities to the interviewee)

Question 4.10

List down all the constituents for each authority above.

Question 4.11

What is the CIRT’s plan to promote its services to the constituents? Is there a method for the Government to promote its services?

(Guideline: a CIRT’s goal should be to promote itself and its services as widely as possible to ensure that its declared constituency is aware of the team and the offered services. Examples: publish in press, announce in Government events and Government newsletters, billboards, faxing memos to Government office, events, email campaigns, etc)

Question 4.12

If there is a Government method to promote the public services, how effective is the method and Is there a mechanism to evaluate the effectiveness?

Question 4.13

Determine the groups or organisations or sector that the CIRT will initially serve?

(Guideline: Initial group can be such as only Government agencies. Name the agencies, list the number of computers & internet capacities, mission & vision, identify e-commerce capabilities, types of systems in use and etc)

Question 4.14

Are any of the constituent’s IT services being outsourced to 3rd party vendors?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 4.14.1

Please provide additional information.

(Guideline: If yes, please define the business nature of the 3rd party vendors and their contact details.)

# SECTION 5 – Place in organisation / Reporting Structure

Question 5.1

To be provided during the onsite assessment or emailed to the country's focal point for this exercise as soon as possible: Please provide overarching organisational chart and the reporting structure within the ministry or Government agency in which the CIRT will be placed.

(Guideline: As a function not by names - the org chart.)

Question 5.2

Will the CIRT be located as a functioning organisation in a Government agency or as a separate organisation (or will it be a part of an organisation)?

(Guideline: For example, a national-level CIRT may function within the Government, as a separate national entity, or as a part of another organisation. A CIRT cannot be placed within its system administration department or IT department because it will fail due to the clear mismatch in responsibility. Provide or sketch the organisation chart.)

Question 5.3

Will the CIRT be a part of the existing security or information security team or organisation?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 5.3.1

If the answer above is “yes”, is there a risk assessment practice in place for the computing, networking and communications equipments?

(Guideline: Risk assessment is important because the parts of the organisation that host the computing, networking, and communications equipment (on which data resides) clearly carry technical risk.)

Question 5.4

If the CIRT will be part of an existing security or information security team. If yes, who will own the shared data?

(Guideline: It is critical to determine the ownership of the data so that proper policies and access rights are assigned to relevant users.)

Question 5.5

Which Government agency will the CIRT be reporting to? Please provide the contact details of the key personnel from the organisation.

(Guideline: Name the organisation and contact details (phone numbers and assigned email addresses) of the key role, - it is preferable to have contact information assigned to a role rather than a person – if the person changes roles/posts then the new appointee responsible for the role is reachable immediately.)

Question 5.6

Is it possible that the CIRT could ever come under any political influences?

(Guideline: This is important to determine the level of authority the CIRT will be given and the sustainability of the CIRT in the event of political turmoil. It is also important to determine if the CIRT’s SOP can be changed during political issues. Sometimes due to some political influences, non-CIRT assignments are imposed that take staff away from their primary CIRT functions and inhibit effective performance of normal services.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 5.7

Is there a Government dictated method for information and document dissemination?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 5.7.1

If yes, explain the method and security control used in the method.

(Guideline: This is important to determine and evaluate the type of security control imposed for information and document dissemination. You may need to collect the necessary documents on the policies and procedures.)

# SECTION 6 – Relationships with other CIRTs

Question 6.1

Will the CIRT serve other CIRTs within the country in the future?

(Guideline: For example serving the military CIRT, campus CIRTs, CIIP CIRTs, private CIRTs and so on.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 6.2

If “yes” to above question, will the CIRT become the central coordination point to all the CIRTs

within the country?

(Guideline: For example within the U.S. military, the U.S. Army, Air Force, and Navy (ACERT/CC, AFCERT, and NAVCIRT, respectively), serve their own constituencies; while the U.S. Department of Defence DOD-CERT coordinates across all the U.S. military teams. Coordinating CIRTs usually request that they be informed of all activity in order for them to obtain an overall view of the level of activity in their domain and alert other teams to look for additional or related activity.)

Question 6.3

In the absence of a CIRT, has there been any initiative to reach CIRT’s/ Cybersecurity agencies/ International organisations in other countries. (If yes, please list the agencies).

# SECTION 7 – CIRT Services

Question 7.1

Are there any incident response capabilities available in the country?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 7.1.1

If above answer is "yes", please provide more information.

(Guideline: Please provide information on the mechanisms they serve their constituency, the modus operandi, the means by which incidents are being reported, the documentations etc.)

Question 7.2

What kind of services will the National CIRT extend to its constituency?

(Guideline: There are 3 kinds; reactive, proactive and security quality management.) Please refer to Appendix A for the details.)

Question 7.3

Is there a current need for forensics and artefact handling of the acquired data?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 7.3.1

If yes, explain why. This is important to determine the technical resources needed

Question 7.4

Is there a plan for the National CIRT to provide on-site incident response services?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 7.4.1

If yes, explain why

Question 7.5

Is the CIRT planning to provide security audit services to its constituents?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 7.5.1

Please name some of possible security audit services that National CIRT would be good to offer to its constituents?

(Guideline: Security audits such as infrastructure review, best practice review, vulnerability assessment, penetration testing, code review, architecture review, etc. This is also to determine the required resources and skill sets for the services.)

Question 7.6

Will there be a configuration and maintenance of security tools, applications and infrastructure

services?

(Guideline: This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CIRT constituency or the CIRT itself.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 7.6.1

Please elaborate the above answer

Question 7.7

Will the CIRT’s services include development of any new, constituent-specific tools that are required or desired by the constituency or by the CIRT itself?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 7.7.1

Please elaborate the above answer.

(Guideline: This can include, for example, developing security patches for customized software used by the constituency.)

Question 7.8

Will there be an intrusion detection service offered to the constituents? Or security event correlation or monitoring?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 7.8.1

Please elaborate on above answer.

(Guideline: Such as review of existing IDS logs.)

Question 7.9

What are the other types of quality-related services that will be provided by the CIRT?

(Guideline: Check relevant answers.)

|  |  |  |
| --- | --- | --- |
| a. | Risk Analysis |  |
| b. | Business Continuity Management / Disaster Recovery Planning |  |
| c. | Security Consulting |  |
| d. | Security Awareness Building |  |
| e. | Education or Training |  |
| f. | Product Evaluation or Certification |  |

Question 7.9.1

What services do you expect to deliver in addition from CIRT to the constituencies?

# SECTION 8 – Financial Model

Question 8.1

Are (Will) there (be) available funds for the CIRT project?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 8.1.1

Please elaborate your answer for the above question in more details. For example, how many funders are available and what is the background of the funders?

(Guideline: List all possible funders’ details including their background. It is important to take note whether the project is state funded or federal Government funded.) If the answer is “no” for the above question, please provide at least a possibility to get funds elsewhere?

Question 8.1.1.1

If answers to above questions are "yes", what is the estimated amount of the budget available? If there are multiple funders, list all of them with their respective committed funding.

(Guideline: This is important to determine the scale of the CIRT and its sustainability. State the amount in US Dollars.)

Question 8.2

Is there any revenue expected from the National CIRT?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 8.2.1

Please provide additional information on the above answer.

(Guideline: Perhaps by subscription fees from the constituency or constant funding from the Government.)

Question 8.3

Is there a framework for sustaining the CIRT operations in the future? If yes please elaborate.

# SECTION 9 – Manpower Planning

Question 9.1

What is the headcount that would possibly be available for the National CIRT to start up its operations?

(Guideline: If the personnel are already identified, list the full names, positions, qualifications, experiences, contact numbers and email address. Our suggestion is to have a minimum of three personnel to start)

Question 9.2

From the above headcount state the number that will be dedicated for managerial positions and technical positions?

(Guideline: It is good to identify other manpower requirements if the CIRT will serve a big constituency such as legal executive and public relations. If the headcount is at minimum three, then one should be a manager)

Question 9.3

What are the skill sets of the identified / current technical staff?

(Guideline: List their experience, qualifications and competencies. If possible get their CVs – without personal data.)

Question 9.4

If the CIRT will be placed within an organisation, will the same employee hold two job descriptions?

(Guideline: Again, it is not advisable for a staff member / personnel to hold responsibilities outside of the CIRT role since this may create conflict of interest.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 9.5

Are there any computer security related trainings or education programs in the country?

(Guideline: List down all the training providers. This will assist in determining the training needs and the availability of such courses locally.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 9.5.1

List all the training providers in your country. This will assist in determining the training needs and the availability of such courses locally.

Question 9.6

List the cyber security training providers in your country or region.

Question 9.7

What are the personal skills of the identified staff (if identified) for the National CIRT establishment? (communication, leadership, technical, etc.)

Question 9.8

Are you familiar with the responsibilities of CIRT Manager, CIRT Analyst and/or CIRT Legal/PR Officer?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 9.9

Do you think that your country might need help in creating job descriptions of the team to be assigned or hired as a part of the National CIRT?

# SECTION 10 – Research on Cybersecurity in the Country

Question 10.1

Is there any research initiative within the country on cybersecurity?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 10.1.1

If the answer is “yes” to the above question, state the specific area of research?

(Guideline: Such as computer forensic, botnet analysis, honeynet, security management, security & psychology and etc.)

Question 10.2

Name the research centres or institutes which are active in these research areas?

 (Guideline: Name the universities / colleges / research centres and provide the contact details.)

Question 10.3

Who is funding the research initiatives?

(Guideline: Government sector or corporate sector.)

Question 10.4

What are the current achievements of the research groups so far?

(Guideline: Any achievements such as development of security tools and etc.)

Question 10.5

How have the achievements above benefitted the people/citizens and the Government of your country?

(Guideline: List them all with benefits and awards if any. If not available just answer with N/A.)

Question 10.6

With the current cybersecurity situation in the country, what is the research area that the Government needs to embark on immediately?

(Guideline: The area that is pressing at the moment.)

Question 10.7

Do you collaborate with other countries/partners/organisations on research in the area of cybersecurity?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 10.8

If yes, could you state the countries/partners/organisations you are collaborating with on research and which projects are you working on.

(Guideline: State the country/partner/organisation, the name of the project and status)

# SECTION 11 – Physical Infrastructure

Question 11.1

Do you think the National CIRT will have its own permanent premises?

(Guideline: This is to determine the physical security landscape of the CIRT.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 11.1.1

Please elaborate the above answer.

Question 11.2

If the National CIRT will be allocated its own permanent facility, what is the physical security

posture of the premise?

(Guideline: Physical security is important to safeguard the physical and information assets of the CIRT. Physical security measures are such as access control, CCTV, guards, fencing, gates etc.)

Question 11.3

If the CIRT is sharing / renting the premise, who is in-charge of the physical security of the CIRT’s part?

(Guideline: This is to determine who will be responsible for physical security.)

Question 11.4

What are the expected telecommunication facilities and infrastructure to be available at the premises?

(Guideline: This is important to cater for the sufficient bandwidth that will be needed to access respective cybersecurity portals and also to provide public access to the CIRT’s portal. This is also needed to determine if there is more than one provider for backup purposes, dual-homing and BCP.)

Question 11.5

Is there a BCM/DRP in place for the premise?

(Guideline: BCM/DRP is important in the event of disaster.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 11.5.1

Please provide additional information to your answer.

(Guideline: BCM/DRP is important in the event of disaster. BCM – Business Continuity Management. DRP – Disaster Recovery Plan)

Question 11.6

Are there plans to have data backup for the future/current National CIRT?

(Guideline: Including UPS & etc.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 11.6.1

Please provide elaborate with additional information.

(Guideline: Including UPS, HA, GenSet, etc.)

Question 11.7

To be provided during the workshop/interview sessions. Provide the over-arching network

diagram of the existing or future desired CIRT setup - if available

# SECTION 12 – Hardware & Software

Question 12.1

To establish a National CIRT there would be a need to purchase Hardware and Software. Are there any plans/funds available to acquire those?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 12.1.1

If the answer is “No”, what would be the plan to acquire Hardware and Operating System?

(Guideline: Basic hardware requirement for CIRT must be provided to establish a CIRT. If the CIRT hardware/software cannot be financed, what are the ways to acquire the necessary hardware/software.)

Question 12.2

What are the network components currently in place at the CIRT, if there is any CIRT established?

(Guideline: List down all the details of the network components such as the make, model, series & quantity.)

# SECTION 13 – Performance Evaluation

Question 13.1

Is there a mechanism or baseline currently in place for evaluating the work performance of Government staff, any KPI’s?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 13.1.1

If the answer is “yes” for the above question, what are the measurement criteria and quality assurance parameters used?

(Guideline: If there is a mechanism to evaluate performance, the same mechanism can be used to evaluate the performance of the CIRT staff. Collect documents related to the process flow of the performance evaluation.)

Question 13.2

Is there a mechanism in place currently for public sector to get feedback from Government constituents and the people of the country in general for the public service?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 13.2.1

Please provide additional information to the above.

(Guideline: This information can be used to adopt the same mechanism to gauge the CIRT constituent satisfaction. This is important to identify issues and areas for improvement. Collect necessary documents, policies and forms.)

Question 13.3

Are there any service level agreements (SLAs) currently in place for the public services? If yes, collect all the necessary documents such as agreements & forms.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 13.3.1

If yes, during the assessment provide the collected all the necessary documents such as agreements & forms. Please list some of the possible documents that will be provided during the assessment.

(Guideline: To study the way SLAs are implemented and the acceptance by the public or the Government constituents.)

Question 13.4

Will be the technical/financial review committee for the CIRT?

# SECTION 14 – ICT Sustainability and Readiness of the Country

Question 14.1

How affordable and widespread are ICT equipments / devices (e.g. personal computers, Internet access and software) for public, Government and private sector?

Question 14.2

Does the country have ICT industries developed to make hardware, software and offer services related to ICT?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 14.2.1

Please provide additional information to the above. Example: Is there sufficient expertise on ICT within the country or does it need to be imported?

Question 14.3

Are there any means where citizens, Government and private sector can discuss ICT and other ICT related issues?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 14.3.1

On the above, please describe some of those means available. Is it an online forum? Public Discussion? etc.

Question 14.4

Is the country a hub of discussion and forums for the ICT industry regionally and/or worldwide?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 14.4.1

Please provide additional information

Question 14.5

Is there infrastructure (technical, legal) for e-commerce to bloom in the country?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 14.5.1

Please provide additional information. (i.e. - Do you know the amount of electronic transactions?, who are the main e-commerce players)

Question 14.6

Does the country have indigenous e-commerce technology and services?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 14.6.1

Please provide additional information to the above. (i.e. Are these exported elsewhere in the region or wider?)

Question 14.7

Is there a forward-looking, progressive culture at the level of policy-makers, private sector, academia, citizens and the media in opening up access to ICTs and harnessing them? Or is there nervousness about the cultural and political impacts of ICTs?

Question 14.8

Is there adequate cooperation between public, private sector, academia, non-Governmental organisations (NGOs) and policy-makers to create a favourable climate for using ICTs?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 14.8.1

Please provide additional information by listing those organisations.

Question 14.9

Do you have any information on what would the level of foreign investments be in the country?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 14.10

Where is their investment focused in terms of region and industry?

Question 14.11

How many international players are active in the local private equity market?

Question 14.12

Are there stock markets for public listing?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 14.13

Do you think there are sufficient resources to invest in ICT infrastructure and education?

Question 14.13.1

Please elaborate on the above question

Question 14.14

Is there a domestic venture capital industry?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 14.15

Is that venture capital industry investing in the local market or abroad?

# SECTION 15 – Cybercrime Related Laws, Legislations and Frameworks

Question 15.1

Is cybercrime, computer crime or electronic crime growing problem in your country?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 15.1.1

If above answer is "YES", please share information on the types of crimes and some statistics if you have.

Question 15.2

Are there any cybercrime, computer crime or electronic laws in your country?

Question 15.3

If there is a law on the above mentioned areas, what is the applicability level of it? Has ever been used to prosecute the perpetrators? (please share with us some news, links or any other information you think it might be relevant)

Question 15.4

Please share if there is any part of the cyber, computer or electronic laws where the judges, lawyers or others have difficulties in understanding the digital evidence or digital forensics reports.

Question 15.5

If in your country there are no such laws, please state the possible reasons for not having them (in your opinion) (i.e. no local expertise, political reasons, monetary reasons, etc.)

Question 15.6

Is the possession of child pornographic or any other abusive child materials (in any format) a legal offence in your country? (videos, photos digital or printed, and any other format)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 15.6.1

Please provide additional information the above answers

Question 15.7

Does the organisation where you work or any of country’s Government agencies or regulatory bodies keep records of cybercriminals or suspected cybercriminals within the country?

(Guideline: This is to study and understand the local cybercrime scenario / activities.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 15.7.1

Please provide additional information.

(Guideline: This is to study and understand the local cybercrime scenario / activities.)

Question 15.8

Are there any cybercrime prevention authorities or units in your country?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 15.9

Are the Law Enforcement Agencies (LEA) in the country aware of the potential dangers of cyber crimes?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 15.10

Have the Law Enforcement Agencies participated in any training related to cyber crime?

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

# SECTION 16 – Cyber / e-Government Frameworks

Question 16.1

Does your country have the eGovernment Framework? (Intention is to understand the current status, plans and strategies on bringing public services closer to the citizens and the businesses)

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** |  | **No** |

Question 16.1.1

Please provide information on current activities on broadband, connectivity of schools, connectivity of rural areas, etc.)

Question 16.2

Do you think that there is enough local expertise to embark on projects of such sizes? Please elaborate.

# SECTION 17 - Attestation

I ..................................................................................................................................... hereby attest that I have completed / compiled all the answers to the questions stated above to the best of my ability as a representative of ...........................................................................................................................................................................

...............................................................................................................................................................................

...............................................................................................................................................................................

Dated:

Name, Designation, Office Address

Location:

# APPENDIX A

List of Common CIRT Services

|  |  |  |
| --- | --- | --- |
| Reactive Services | Proactice Services | Security Quality Management Services |
| a) Alerts & Warningsb) Incident Handling* Incident analysis
* Incident response on-site
* Incident response

support* Incident respond

coordinationc) Vulnerability Handling* Vulnerability analysis
* Vulnerability response
* Vulnerability response coordination

d) Artefact Handling* Artefact analysis
* Artefact response
* Artefact response coordination
 | 1. **Announcements**
2. **Technology Watch**
3. **Security Audits or Assessments**
4. **Configuration & Maintenance of Security Tools, Applications & Infrastructure**
5. **Development of Security Tools**
6. **Intrusion Detection Services**
7. **Security-Related Information Dissemination**
 | 1. **Risk Analysis**
2. **Business Continuity &**

**Disaster Recovery Planning**1. **Security Consulting**
2. **Awareness Building**
3. **Education / Training**
4. **Product Evaluation /**

**Certification** |

# APPENDIX B

List of Critical National Infrastructures

|  |  |
| --- | --- |
| No | CNI Sectors |
| 1 | Finance |
| 2 | Communication |
| 3 | Transport |
| 4 | Energy |
| 5 | Water |
| 6 | Emergency Services |
| 7 | Food |
| 8 | Public Safety |
| 9 | Health |
| 10 | Public Service |

# APPENDIX C

Questionnaire Checklist

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Question No** | **Answered** | **Needs to be Verified by** | **Unclear** | **Unable to answer** |
| **Self** | **Higher Official** | **ITU-IMPACT** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **2.1** |  |  |  |  |  |  |
| **2.2** |  |  |  |  |  |  |
| **2.3** |  |  |  |  |  |  |
| **2.4** |  |  |  |  |  |  |
| **2.5** |  |  |  |  |  |  |
| **3.1** |  |  |  |  |  |  |
| **3.2** |  |  |  |  |  |  |
| **3.2.1** |  |  |  |  |  |  |
| **3.3** |  |  |  |  |  |  |
| **3.4** |  |  |  |  |  |  |
| **3.4.1** |  |  |  |  |  |  |
| **3.5** |  |  |  |  |  |  |
| **3.6** |  |  |  |  |  |  |
| **3.6.1** |  |  |  |  |  |  |
| **3.7** |  |  |  |  |  |  |
| **3.8** |  |  |  |  |  |  |
| **3.9** |  |  |  |  |  |  |
| **3.10** |  |  |  |  |  |  |
| **3.11** |  |  |  |  |  |  |
| **4.1** |  |  |  |  |  |  |
| **4.2** |  |  |  |  |  |  |
| **4.3** |  |  |  |  |  |  |
| **4.4** |  |  |  |  |  |  |
| **4.5** |  |  |  |  |  |  |
| **4.6** |  |  |  |  |  |  |
| **4.6.1** |  |  |  |  |  |  |
| **4.7** |  |  |  |  |  |  |
| **4.7.1** |  |  |  |  |  |  |
| **4.8** |  |  |  |  |  |  |
| **4.8.1** |  |  |  |  |  |  |
| **4.9** |  |  |  |  |  |  |
| **4.10** |  |  |  |  |  |  |
| **4.11** |  |  |  |  |  |  |
| **4.13** |  |  |  |  |  |  |
| **4.14** |  |  |  |  |  |  |
| **4.14.1** |  |  |  |  |  |  |
| **5.1** |  |  |  |  |  |  |
| **5.2** |  |  |  |  |  |  |
| **5.3** |  |  |  |  |  |  |
| **5.3.1** |  |  |  |  |  |  |
| **5.4** |  |  |  |  |  |  |
| **5.5** |  |  |  |  |  |  |
| **5.6** |  |  |  |  |  |  |
| **5.7** |  |  |  |  |  |  |
| **5.7.1** |  |  |  |  |  |  |
| **6.1** |  |  |  |  |  |  |
| **6.2** |  |  |  |  |  |  |
| **6.3** |  |  |  |  |  |  |
| **7.1** |  |  |  |  |  |  |
| **7.1.1** |  |  |  |  |  |  |
| **7.2** |  |  |  |  |  |  |
| **7.3** |  |  |  |  |  |  |
| **7.3.1** |  |  |  |  |  |  |
| **7.4** |  |  |  |  |  |  |
| **7.4.1** |  |  |  |  |  |  |
| **7.5** |  |  |  |  |  |  |
| **7.5.1** |  |  |  |  |  |  |
| **7.6** |  |  |  |  |  |  |
| **7.6.1** |  |  |  |  |  |  |
| **7.7** |  |  |  |  |  |  |
| **7.7.1** |  |  |  |  |  |  |
| **7.8** |  |  |  |  |  |  |
| **7.8.1** |  |  |  |  |  |  |
| **7.9** |  |  |  |  |  |  |
| **7.10** |  |  |  |  |  |  |
| **8.1** |  |  |  |  |  |  |
| **8.1.1** |  |  |  |  |  |  |
| **8.1.1.1** |  |  |  |  |  |  |
| **8.2** |  |  |  |  |  |  |
| **8.2.1** |  |  |  |  |  |  |
| **8.3** |  |  |  |  |  |  |
| **9.1** |  |  |  |  |  |  |
| **9.2** |  |  |  |  |  |  |
| **9.3** |  |  |  |  |  |  |
| **9.4** |  |  |  |  |  |  |
| **9.5** |  |  |  |  |  |  |
| **9.5.1** |  |  |  |  |  |  |
| **9.6** |  |  |  |  |  |  |
| **9.7** |  |  |  |  |  |  |
| **9.8** |  |  |  |  |  |  |
| **9.9** |  |  |  |  |  |  |
| **10.1** |  |  |  |  |  |  |
| **10.1.1** |  |  |  |  |  |  |
| **10.2** |  |  |  |  |  |  |
| **10.3** |  |  |  |  |  |  |
| **10.4** |  |  |  |  |  |  |
| **10.5** |  |  |  |  |  |  |
| **10.6** |  |  |  |  |  |  |
| **10.7** |  |  |  |  |  |  |
| **11.1** |  |  |  |  |  |  |
| **11.1.1** |  |  |  |  |  |  |
| **11.2** |  |  |  |  |  |  |
| **11.3** |  |  |  |  |  |  |
| **11.4** |  |  |  |  |  |  |
| **11.5** |  |  |  |  |  |  |
| **11.5.1** |  |  |  |  |  |  |
| **11.6** |  |  |  |  |  |  |
| **11.6.1** |  |  |  |  |  |  |
| **11.7** |  |  |  |  |  |  |
| **12.1** |  |  |  |  |  |  |
| **12.1.1** |  |  |  |  |  |  |
| **12.2** |  |  |  |  |  |  |
| **13.1** |  |  |  |  |  |  |
| **13.1.1** |  |  |  |  |  |  |
| **13.2** |  |  |  |  |  |  |
| **13.2.1** |  |  |  |  |  |  |
| **13.3** |  |  |  |  |  |  |
| **13.3.1** |  |  |  |  |  |  |
| **13.4** |  |  |  |  |  |  |
| **14.1** |  |  |  |  |  |  |
| **14.2** |  |  |  |  |  |  |
| **14.2.1** |  |  |  |  |  |  |
| **14.3** |  |  |  |  |  |  |
| **14.3.1** |  |  |  |  |  |  |
| **14.4** |  |  |  |  |  |  |
| **14.4.1** |  |  |  |  |  |  |
| **14.5** |  |  |  |  |  |  |
| **14.5.1** |  |  |  |  |  |  |
| **14.6** |  |  |  |  |  |  |
| **14.6.1** |  |  |  |  |  |  |
| **14.7** |  |  |  |  |  |  |
| **14.8** |  |  |  |  |  |  |
| **14.8.1** |  |  |  |  |  |  |
| **14.9** |  |  |  |  |  |  |
| **14.10** |  |  |  |  |  |  |
| **14.11** |  |  |  |  |  |  |
| **14.12** |  |  |  |  |  |  |
| **14.13** |  |  |  |  |  |  |
| **14.13.1** |  |  |  |  |  |  |
| **14.14** |  |  |  |  |  |  |
| **14.15** |  |  |  |  |  |  |
| **15.1** |  |  |  |  |  |  |
| **15.1.1** |  |  |  |  |  |  |
| **15.2** |  |  |  |  |  |  |
| **15.3** |  |  |  |  |  |  |
| **15.4** |  |  |  |  |  |  |
| **15.5** |  |  |  |  |  |  |
| **15.6** |  |  |  |  |  |  |
| **15.6.1** |  |  |  |  |  |  |
| **15.7** |  |  |  |  |  |  |
| **15.7.1** |  |  |  |  |  |  |
| **15.8** |  |  |  |  |  |  |
| **15.9** |  |  |  |  |  |  |
| **15.10** |  |  |  |  |  |  |
| **16.1** |  |  |  |  |  |  |
| **16.1.1** |  |  |  |  |  |  |
| **16.2** |  |  |  |  |  |  |

END OF QUESTIONNAIRE