



## **ADMINISTRATIVE AGREEMENT**

**Between**

**THE GOVERNMENT OF XXX** *represented by its Ministry of XXX*

**and**

**THE INTERNATIONAL TELECOMMUNICATION UNION**

Concerning

The Project of National CIRT Establishment

This Administrative Agreement is concluded

BETWEEN

**The Government of XXX** (hereinafter referred to as the “**Member State**”), represented by its Ministry of ,

AND

**The International Telecommunication Union** (hereinafter referred to as “**ITU**”), an intergovernmental organization and a specialized agency of the United Nations, having its headquarters located at Place des Nations, Geneva, Switzerland.

**WHEREAS** the Member State requests the cooperation of ITU to obtain specialized technical assistance on establishing a National Computer Incident Response Team Center (hereinafter referred to as the “CIRT Center”) which will operate in connection with the network of Computer Incident Response Team Centers (CIRTs) established within the framework of the collaboration by and between ITU and the International Multilateral Partnership Against Cyber-Threats (IMPACT);

**WHEREAS** ITU is willing to provide such technical assistance in accordance with the terms and conditions of this Agreement;

**CONSIDERING** that the role of Programme 2 of the Hyderabad Action Plan is to support the ITU Member States, in particular developing countries, in addressing the issues identified at the 2010 ITU World Telecommunication Development Conference (WTDC-10) among others on establishing organizational structures, such as CIRTs, to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level. Resolution 69 (WTDC-10) calls on “Creation of national computer incident response teams, particularly for developing countries, and cooperation between them”;

**NOW THEREFORE**, the Member State and ITU (hereinafter collectively referred to as the “Parties”) have agreed to enter into the present Administrative Agreement (hereinafter referred to as this “Agreement”).

## **Article 1**

### **Purpose and implementation of the Agreement**

- 1.1 This Agreement establishes the terms, conditions and procedures governing the technical assistance provided to the Member State by ITU in connection with the establishment of the CIRT Center, as described in the Project Document attached as Annex 1 to this Agreement (hereinafter referred to as “the Project”).
- 1.2 A separate project document will be established for each other project, if any, to be implemented in the framework of this Agreement, and each such project document shall form an integral part of this Agreement.

## **Article 2**

### **Responsibilities of the Parties**

#### **2.1 Responsibilities of ITU**

In accordance with its rules, regulations, policies and administrative and financial procedures, the ITU is responsible for providing assistance to the Member State as described in

this Agreement and in the Project Document attached hereto as Annex 1 (hereinafter referred to as the "Project Document"). ITU shall not be held responsible for any failure or delay in implementing the activities envisaged under this Agreement or the Project Document which is caused by the failure or delay of the Member State to fulfill its responsibilities and obligations in accordance with this Agreement or the Project Document.

## **2.2 Responsibilities of the Member State**

Notwithstanding the other provisions of this Agreement and those of the Project Document, the Member State is responsible for providing ITU with funds, local infrastructure, information, facilities, local staff and other resources necessary to enable proper execution of the activities described in this Agreement and the Project Document. The Member State is committed to keeping ITU duly informed of any measures taken for the implementation of this Agreement that may affect it.

### **Article 3 Financial Provisions**

- 3.1 The detailed estimated cost of the Project is provided in the Project Document.
- 3.2 The Member State will, for the purposes of the implementation of the Project, place at the disposal of ITU a contribution in cash the amount of which is contained in the Project Document hereinafter referred to as "the Contribution").
- 3.3 The Contribution will be deposited in Swiss Francs to the following account within thirty (30) days following the signature of the Project Document:

Account Name: International Telecommunication Union  
United Bank of Switzerland (UBS) SA  
Case Postale 2600  
CH - 1211 Genève 2 (Suisse)  
SWIFT Code: UBSWCHZH80A  
Account No. 240-C8108400.2  
IBAN: CH58 0024 0240 C810 8400 2  
Purpose: National CIRT Establishment Project in XXX

- 3.4 Under no circumstances shall ITU enter into any commitment regarding the implementation of the activities described in the Project Document (hereinafter referred to as the "Activities") before it has received the full Contribution from the Member State. ITU will not be liable for any failure or delays in the implementation of this Agreement or of the Project due to the lack of timely payment by the Member State of the Contribution.
- 3.5 ITU shall use the Contribution, as well as any and all interest earned by ITU on the Contribution, for the implementation of the Project.
- 3.6 The Contribution and the Activities financed therefrom shall be administered by ITU in accordance with the applicable ITU Rules, Regulations and procedures. Accordingly, personnel shall be engaged and administered, equipment, supplies and services shall be purchased, and contracts shall be entered into, in accordance with the provisions of such Rules, Regulations and procedures.

- 3.7 As per the explicit demand of the Member State, for the purposes of this Agreement and the Project, ITU will, in particular, use the Contribution for the services to be provided by IMPACT.
- 3.8 All financial accounts and statements with respect to the Contribution and the Project shall be expressed in Swiss Francs.
- 3.9 ITU shall establish separate accounting records for the usage of the Contribution. The Contribution shall be subject to the internal and external auditing procedures laid down in the Financial Rules, Regulations and procedures of the ITU.
- 3.10 ITU shall apply an administrative overhead service charge of 7.5% on all expenditures incurred with the funds of the Contribution.
- 3.11 Any funds remaining unused after the completion of the Activities shall be returned to the Member State or used in a manner decided by mutual written agreement between the Parties.
- 3.12 ITU shall provide the Member State with a final expenditure report for the Project, in accordance with ITU's accounting and reporting procedures and within six (6) months after the closure of account of the year within which the Project and the Activities financed by the Contribution are completed in full.

#### **Article 4 Entry into Force and Duration**

This Agreement shall come into effect upon the date of its signature by both Parties. Its provisions shall remain applicable until all obligations and rights of the Parties have been fulfilled in accordance with the terms and conditions of this Agreement.

#### **Article 5 Amendment and Termination of the Agreement**

- 5.1 This Agreement may be extended or modified by written amendment agreed to, and signed by, both Parties. Any such amendment shall be annexed to this Agreement and shall form an integral part hereof.
- 5.2 This Agreement may be terminated by either Party by giving a notice to the other Party. The termination shall be effective thirty (30) calendar days after receipt of notice by the Party to whom it is addressed.
- 5.3 In case of termination of this Agreement for whatever reason, ITU shall take all necessary steps to bring the Project to a close in a prompt and orderly manner, and shall make every reasonable effort to keep the expenditures for this purpose to a minimum. ITU shall not undertake any forward commitment from the date on which a written notice of termination has been sent or received by it. Any cost incurred by ITU, as well as the remuneration due to ITU for services rendered under this Agreement and the Project Document, in each case, up to the effective date of such termination shall be paid from the relevant Project Budget. Should there be any remaining funds from the Contribution after the closure of the Project and termination of this Agreement, Article 3.11 will apply.
- 5.4 Notwithstanding its termination, the provisions of this Agreement shall survive to the extent necessary to permit an orderly liquidation of obligations between the Parties.

## **Article 6 Representation and addresses of the Parties**

6.1 Any notice to be given to either Party with respect to this Agreement shall be considered as effectively given, if delivered or sent by letter (with acknowledgement of receipt) or by fax or email addressed to either Party at the address mentioned below. Any such notice shall become effective on the day of its receipt by the Party to which it is addressed. The address of either Party may be changed by appropriate notice to the other Party.

6.2 Any notice to the Member State shall be addressed to:

Ministry of

Attn: Mr.

Address

Tel:

Fax:

Email:

6.3 Any notice to ITU shall be addressed to:

International Telecommunication Union  
Attn: Mr. Mario Maniewicz  
Telecommunication Development Bureau (BDT)  
Place des Nations  
CH-1211 Geneva 20, Switzerland  
Tel: +41 22 730 5421  
Fax: +41 22 730 5484  
Email: [mario.maniewicz@itu.int](mailto:mario.maniewicz@itu.int)

## **Article 7 Force Majeure**

7.1 In the event of a Force Majeure - i.e. an event outside the control of, and which could not be reasonably foreseen by, either Party exercising due care and diligence - which may result in delays or otherwise hinder successful completion of the Project(s) under implementation in the framework of this Agreement, such an event shall be notified in writing within ten (10) working days by the Party encountering it to the other Party.

7.2 As soon as possible after receipt of such a notification, the Parties shall consult each other to establish the existence of Force Majeure and determine its impact on the successful completion of any of the Project(s) in course of implementation.

7.3 The Parties shall also decide on the necessity of termination of this Agreement or of one or more of the Project(s) under implementation. In the case of termination, the relevant provisions of Article 5.3 shall apply.

## **Article 8 Confidentiality**

The Parties agree to treat with the utmost confidentiality all documents, information and/or data obtained in the course of the execution of this Agreement.

## **Article 9 Default by ITU**

The Member State shall notify ITU, by registered letter with acknowledgement of receipt, if it considers in good faith that ITU is not discharging its obligations under this Agreement, stating the reasons therefor. In the event that ITU does not respond to such notice within fifteen (15) working days of its receipt, the Member State may deem this Agreement terminated. In this event, the provisions of Article 5.3 above shall apply.

#### **Article 10 Settlement of Disputes**

Any dispute arising from or in connection with this Agreement or the Project Document shall be settled directly by negotiation between the Parties or by such other means as the Parties agree to in writing.

#### **Article 11 Rights and obligation of the Parties**

The rights and obligations of each Party shall be limited to the terms and conditions of this Agreement and the Project Document.

#### **Article 12 Privileges, Immunities and Facilities**

- 12.1 ITU is an intergovernmental organization and a United Nations specialized agency and, as such, enjoys the privileges, immunities and facilities derived from this status, as recognized by the applicable international agreements and by relevant national laws.
- 12.2 Nothing in or relating to this Agreement shall be deemed a waiver, express or implied, of any privileges, immunities and facilities of the ITU or any of its officials.

#### **Article 13 Entire Agreement, Annexes**

The terms and conditions stated in this Agreement and the Project Document represent the entire agreement between the Member State and ITU with respect to the subject matter hereof and thereof, and supersedes all prior agreements, arrangements, communications, negotiations, proposals or other understanding, whether written or oral, between the Parties with respect to such subject matter. This Agreement and the Project Document contain all covenants, stipulations and provisions agreed by the Parties. No agent or representative of either Party has authority to make, and the Parties shall not be bound by or be liable for, any statement, representation, promise or agreement not set forth herein. All Annexes attached to this Agreement form an integral part hereof.

#### **Article 14 Assignment**

Neither Party shall in any way assign this Agreement or transfer all or part of its rights or obligations hereunder to any third person or entity without the prior written agreement of the other Party.

**IN WITNESS THEREOF**, the undersigned, being duly authorized representatives of the Parties have signed this Agreement in two (2) original copies, in the English language.

**For the Government of XXX**

**For the International  
Telecommunication Union**

---

**XXX**  
Minister  
Ministry of

---

**Mr. Brahima Sanou**  
Director  
Telecommunication Development Bureau  
(BDT)

Place: \_\_\_\_\_

Date: \_\_\_\_\_

Place: \_\_\_\_\_

Date: \_\_\_\_\_



**Project Number:**  
**Project Title:** National CIRT Establishment  
**Project Short Title:** XXX  
**Start Date:** XX 2013  
**Estimated End Date:** XX 2013  
**Government Coop. Agency:** Ministry of  
**Beneficiary Country:** XXX  
**ITU Project Manager:** Marco Obiso

#### SUMMARY OF CONTRIBUTIONS

##### A) Project Budget (in CHF)

External Services	93,564
Mission Expenses	<u>34,960</u>

Subtotal	<u>128,524</u>
----------	----------------

AOS (7.5%) on in-cash contribution	9,639
------------------------------------	-------

<b>Grand Total:</b>	<b>138,163</b>
---------------------	----------------

##### B) Cost Sharing

- ITU (in kind) estimated at CHF 25'000 in human resources
- Ghana in cash contribution of CHF 138,163

#### Brief Description:

The main goal of the project is to assist the government of XXX to establish its national Computer Incident Response Team (CIRT) to serve as a trusted, central coordination point of contact for cybersecurity; aimed at identifying, defending, responding and managing cyber threats.

ITU will assist the government of XXX in building and deploying the technical capabilities and related trainings necessary to establish its national CIRT. Thus it is expected to lead to development of national cybersecurity capacity while moving forward on enhancing regional and international collaboration.

For the	Signature	Date	Name/Title
ITU:	_____	_____	Mr. Brahim Sanou Director of BDT
Government of XXX:	_____	_____	H.E. . Minister, Ministry of



## **1. Background & Context**

### **1.1 General Introduction**

Many countries and governments are using the dynamic and inter-connected environment of today's networked information systems to improve communications, provide control, protect information, and encourage competitiveness. Computers have become such an integral part of daily activities that computer-related risks cannot be separated from general business, health, and privacy risks. Valuable country assets and critical national infrastructures are now at risk over the Internet.

Overall reliance on the Internet continues to increase<sup>1</sup>. Unfortunately, in this dynamic, distributed, and interconnected environment, cyber attacks occur rapidly and can spread across the globe in minutes without regard to borders, geography, or national jurisdiction. As a result, there is a growing need to be able to communicate, coordinate, analyze, and respond to cyber attacks across different business sectors and national borders. The Internet itself has become a critical infrastructure<sup>2</sup> to many nations, businesses and people that must also be protected.

It is important for each national government to create or identify a national organization to serve as a focal point for securing cyberspace and the protection of critical information infrastructure, and whose national mission includes watch, warning, response and recovery efforts, and the facilitation of collaboration between government entities, the private sector, academia, and the international community<sup>3</sup> when dealing with cybersecurity issues.

Therefore, collaboration at the national and international level is necessary to effectively align capabilities and expertise to manage incidents and raise awareness of potential incidents and steps toward remediation. Governments have the key role in ensuring coordination among these entities.

The establishment of a national CIRT is needed to help to ensure the protection of the nation's critical information infrastructures, to assist in drafting the overall plan on the country's approach to cybersecurity related issues, and to serve as a focal point for further building and implementing the national culture of cybersecurity.

### **1.2 Problem Statement**

The national CIRT has a key role to play in supporting the Government XXX in addressing cybersecurity related issues at the national level as this pertains to preparing for, detecting, managing, and responding to cyber incidents if and when they occur. However, implementing an incident

---

<sup>1</sup> <http://www.cert.org/archive/pdf/NationalCSIRTs.pdf>

<sup>2</sup> [http://www.itu.int/ITU-D/connect/flagship\\_initiatives/impact.html](http://www.itu.int/ITU-D/connect/flagship_initiatives/impact.html)

<sup>3</sup> <http://www.itu.int/md/D06-SG01-C-0249/en>

management mechanism requires consideration for funding, human resources, training, technological capability, government and private sector relationships, and legal requirements<sup>4</sup>.

Taking the foregoing into consideration, developing countries such as XXX, with limited human, institutional and financial resources face, particular challenges in elaborating and implementing national policies and frameworks for cybersecurity and critical information infrastructure protection.

### **1.3 Justification**

This project focuses on assisting the government of XXX to organize and equip itself to better respond to cyber-threats. It pays particular attention to improving cybersecurity in XXX to ensure better protection of XXX's ICT infrastructure, including critical information infrastructure, and the availability of dependent services provided to XXX's government agencies, citizens and businesses. Many of these services are part of daily life and have a direct impact on XXX's economic well-being and progress.

A national CIRT is a key component of a national approach to cybersecurity and is a solid building block onto which other cybersecurity related activities could be linked. The establishment of a national CIRT, and development of related processes on the national level, can also serve as a foundation for the development of the following activities in XXX:

- building a knowledgebase that supports XXX's development and implementation of a national cybersecurity strategy as well as a national approach for the protection of critical information infrastructures;
- supporting the building of a national culture of cybersecurity, and related awareness raising initiatives;
- supporting the development of related national cybersecurity platforms, for example: the national Public-Key Infra-structure (PKI), e-Government framework and approach, national identity and access management framework, combating SPAM, botnets, etc.;
- assisting in planning/development of a national strategy on child online protection;
- further enabling XXX to develop and enhance its national incident response and management capabilities.

---

<sup>4</sup> <http://www.itu.int/md/D06-SG01-C-0249/en>

#### 1.4 Relationship to BDT Programs/Activities

The objective of Programme 2 of the Hyderabad Action Plan is to support the ITU membership, in particular developing countries, in addressing the issues identified by WTDC-10 among others on *establishing organizational structures, such as computer incident response teams (CIRTs), to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level.*

For this reason, Resolution 69 “*Creation of national computer incident response teams, particularly for developing countries, and cooperation between them*” was adopted at WTDC-10.

As lead facilitator for WSIS Action Line C5<sup>5</sup>, ITU is responsible for assisting stakeholders in building confidence and security in the use of Information and Communication Technologies (ICTs)<sup>6</sup> at national, regional and international levels.

In addition, ITU Resolution 130 (Guadalajara, 2010) 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 to support Member States in their effort towards protection against cyberthreats at national, regional and international levels, as appropriate, by establishing mechanisms, such as CIRTs, to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level.**

WTDC-10 also calls on assisting Member States in establishing organizational structures, such as CIRTs, to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level.

In this framework, the Global Cybersecurity Agenda (GCA) was launched by the ITU Secretary-General as ITU’s framework for international multi-stakeholder cooperation towards a safer and more secure information society, and focuses on the following five work areas:

- Legal Measures
- Technical and Procedural Measures
- Organizational Structures
- Capacity Building
- International Cooperation

---

<sup>5</sup> <http://www.itu.int/osg/csd/cybersecurity/WSIS/>

<sup>6</sup> <http://www.itu.int/wsis/docs/geneva/official/poa.html>

Within the GCA's framework and as part of efforts to achieve global coordination and international cooperation on cybersecurity, in September 2008, ITU signed a Memorandum of Understanding with the International Multilateral Partnership against Cyber-Threats (IMPACT).

## **2. Strategy**

### **2.1 Overall Project Objective**

The objective of this project is to assist the government of XXX in establishing and further developing its cybersecurity capabilities, including the establishment of a Computer Incident Response Team with national responsibility.

### **2.2 Project Strategy**

The overall strategy is to facilitate the process towards the establishment of a national cybersecurity strategy in XXX. As such the aim is to initially equip the government of XXX with a functioning national CIRT.

This project will:

- facilitate the establishment of watch-warning and incident response capabilities in XXX to better identify, respond to, and manage cyber-threats;
- assist XXX in identifying its national critical information infrastructure sectors and establishing a foundation on the national level to be able to further elaborate and implement a national cybersecurity strategy;
- build the national capacity and the transfer know-how to the government of XXX that are required in order to facilitate further development within the area of national critical information infrastructure protection, such as establishing sector CIRTs, etc.

## **3. Expected Results**

By implementing this project, the following primary and secondary results are expected:

### **3.1 Primary Expected Result:**

- A functioning national CIRT able to provide XXX's constituents with a basic set of services.

### **3.2 Secondary Expected Results:**

- Enhanced national expertise on cybersecurity and reduction of the human capacity gap in cybersecurity.
- Improved national preparedness on the identification, prevention, response, and resolution of cybersecurity incidents (preliminary assessment and post implementation assessment required).
- Utilization and operation of the CIRT by building an effective/efficient capable CIRT that is ready to respond to cyber attacks targeting the national critical information infrastructure. The national CIRT will be the trusted advisor to the government of XXX on matters concerning cybersecurity.
- National awareness training programmes are developed to result in improvements in cybersecurity procedures, to defend and protect infrastructures and government agencies.
- Increased ability to enact effective security measures and instill mature responses when such true threats occur.

#### **4. Performance Indicators**

Indicators are:

- National CIRT established and put into operation by the end of the project;
- At least three (3) government officials from XXX will be trained to manage the national CIRT;
- Drafting of roadmap on the building of a national culture of cybersecurity as a part of national cybersecurity strategy within the framework of national CIRT enhancements.

#### **5. Activities**

To meet the objectives of this project, a number of activities will be undertaken by the Parties.

##### **5.1 ITU Activities**

The project activities undertaken will be in synergy with Programme 2 of the Hyderabad Action Plan and ITU planned regional activities, to ensure effective implementation of the project.

ITU specific activities for the project include:

- Prepare terms of reference of the subcontractor (IMPACT) and contracting with such subcontractor as per the Administrative Agreement.

- Provide site assessment and preparation for project start.
- Provide and update project plan and roadmap with feasible dates throughout the project.
- Provide capacity building and training based on gaps in the areas identified during the project implementation.
- Customize training materials that meet XXX's goals on cybersecurity capacity building.
- Train experts – further developing of existing skills available in the country.
- Customize and develop processes to run CIRT operations.
- Customize CIRT software to meet XXX's needs and be in line with the relevant processes and strategy.
- Remote installation of CIRT software tools ,including the following:
  - A Public Portal
  - Request Tracker for Incident Response - (RTIR)
  - Mailing list
- Start the operation and conduct an assessment of the operations/implementation of the CIRT project for Quality Assurance.

## **5.2 Beneficiary Country Activities**

XXX's specific activities for the project include:

- Assisting site preparation for CIRT Installation.
- Procuring the recommended equipment - hardware/basic OS software configuration for the CIRT solution deployment.
- Assisting the project team in terms of logistics for training sessions.
- Preparing, together with the Project team the materials to conduct national awareness activities.
- Meeting the back-end requirements of the servers hosted the Public Portal, RTIR and Mailing List; such as operating system configurations, network configurations, or any other fine tuning related to the availability of these systems or ITU experts, IMPACT experts, or the intended end users of these systems. The foregoing will be the sole responsibility of XXX.

## **6. Inputs/Contributions**

### **6.1 ITU:**

IN KIND CONTRIBUTION	Human resources and skills for project coordination and management - ITU will provide skills, care and diligence which are reasonably intended to ensure the success of the project, estimated at CHF 25'000.
-------------------------	---

**6.2 XXX:**

IN CASH CONTRIBUTION	CHF 138'163 (Details in Project Budget – see Annex 1).
IN KIND CONTRIBUTION	<ol style="list-style-type: none"> <li>1. Financial commitment on CIRT establishment and sustainability.</li> <li>2. Human resources to implement and run the entire project (minimum of 3 individuals).</li> <li>3. Facility (physical location and related infrastructure).</li> <li>4. Hardware and basic software (servers, clients, operating system, network, etc.).</li> </ol>

XXX will provide a project team comprising of its own staff (minimum of three (3) officials) to implement and coordinate the project on-site with ITU; mobilize local partners; host project team meetings; train the trainers, comprising CIRT manager and analysts; provide local logistics, including deployment of equipment and human resources; provide Internet connection, and computer hardware and software; and promote the project among stakeholders in the governmental agencies, etc.

XXX will oversee the involvement of required national entities and be responsible for the promotion of the project among the national media and local communities, with a view to getting stakeholders' continued involvement and to disseminating knowledge about the project and its importance. The stakeholders' involvement plays a key role in the overall success and effectiveness of the project.

**7. Risk Management**

- The primary risk for this project is that in-country activities may suffer delays due to unforeseen local events and circumstances. Getting the commitment from the government of XXX in the early stages of planning will minimize this risk.
- Another risk for the project is the possibility of inadequate human resources assigned to the project (by the government of XXX), which would increase the time for completion of the project. This risk will be reduced by the provision of appropriate site and country training courses by ITU.

- As a first step, ITU's BDT has already conducted a feasibility assessment for XXX on National CIRT Establishment in order to further manage the risk of potential project delays and or increased costs.

## **8. Project management**

The project will be implemented by the assigned ITU Project Manager in close coordination with XXX's Focal Point(s) and the Subcontractor (IMPACT).

ITU will supervise and administer overall implementation of the project in accordance with ITU rules, regulations and procedures.

## **9. Roles and Responsibilities**

### **9.1 International Telecommunication Union (ITU)**

#### **ITU will:**

- Provide staff resources for the coordination and management of the project and be responsible for the overall management of the project implementation, supervision, monitoring, coordination and evaluation.
- Provide its expertise and international experience to reasonably enable realization of the project objectives in an effective and efficient manner.
- Allocate the experts for the project as per Subcontractor's (IMPACT's) contract and terms of reference.
- Correspond with the relevant parties to make sure that project is successful.
- Provide advice and assistance to the project team, when it is required pre-, during and after project implementation.
- Provide the solution/software source code and related development documentation to XXX at no additional charge as a part of the project.
- Identify XXX's needs and assist in the development of a roadmap for the evolution of the National CIRT.
- Provide a roadmap for human capacity building and training needs for the development of the National CIRT services.
- Transfer the know-how to XXX on provided CIRT solutions, its daily operations and cybersecurity defense mechanisms and processes against some common attacks on national critical information infrastructure.



- Produce periodic project progress reports.
- Produce project closure report with financial statement at the completion of the project.

## 9.2 Beneficiary Country

### XXX will:

- Transfer the allocated funds to ITU and provide the project inputs/contributions listed under section 6.2.
- Provide physical as well as virtual access to the CIRT facility identified and allocated. Physical access for ITU-IMPACT experts to execute the onsite implementation part of the project and virtual in a sense for ITU-IMPACT experts to carry out the remote/offsite implementation part of the project.
- Purchase the recommended equipment hardware/software based on the accepted CIRT design and configure that hardware/software for CIRT solutions deployment by ITU-IMPACT experts remotely. All network or server related dependencies for installation of CIRT solutions by ITU-IMPACT experts have to be resolved by XXX's team members.
- Provide project facilities and resources where the project office can be located and training sessions can be conducted.
- Designate national counterparts (qualified technical personnel) that will assist in hosting project team, provide local logistics including deployment of equipment. The national counterparts designated by XXX will, in particular, assist ITU and the selected subcontractor by providing accurate information relevant to the project.
- Provide information required for carrying out the planned and agreed project activities.
- Provide human resources to efficiently operate the CIRT.
- Provide physical space, hardware and software facilities as required by the project nature and for the establishment of the CIRT.
- Provide administrative support (including 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.
- Collect cyber-attacks data, outline statistical trends, attack patterns, build intelligence on top of them and reach effective knowledge sharing.
- Commit necessary resources to keep the national CIRT facilities in operation after completion of the project.

- Issue all certificates, permits, licenses, exemptions, clearances and other instrument necessary to be obtained by ITU or its officials, or the project's Subcontractor or its personnel, in connection with the provision of services or goods to XXX under this project.

## **10. Project's sustainability**

Cyberthreats are increasingly affecting the daily lives of ICT users therefore the national CIRT is considered to be a sustainable solution due to its capabilities against cyberthreats. Furthermore sustainability of the established national CIRT will be guaranteed by XXX. As described in section 9 of this project document, XXX commits itself to take necessary measures in order to keep the national CIRT in operation.

## **11. Monitoring and evaluation**

The Project Manager will prepare periodic progress reports, which will provide a summary of the achievements and activities as well as challenges faced in a given period.

ITU together with XXX will, at the end of the project, prepare a final report to assess the success of the project in terms of meeting its stated main objectives, expected outcomes and impacts on XXX's future development.

For the evaluation of the project, post-implementation feedback from XXX could be requested in order to provide useful lessons in planning and replicating similar implementation projects in future and customization of the training materials.

## **12. Budget**

The Budget is contained in Annex A.

## **13. Work Plan and CIRT Methodology Overview**

The Work Plan and the CIRT Methodology Overview are contained in Annex B.

**Annex A - Project Budget (cash contribution)**

Table 1 provides the overall estimated budget for this project by category of expenditures. The breakdown by category of expenditures is based on the best available information at this time and is subject to change during implementation of the project. In order to ensure the successful implementation of the project, the project manager will have the flexibility to shift funds between budget categories as necessary.

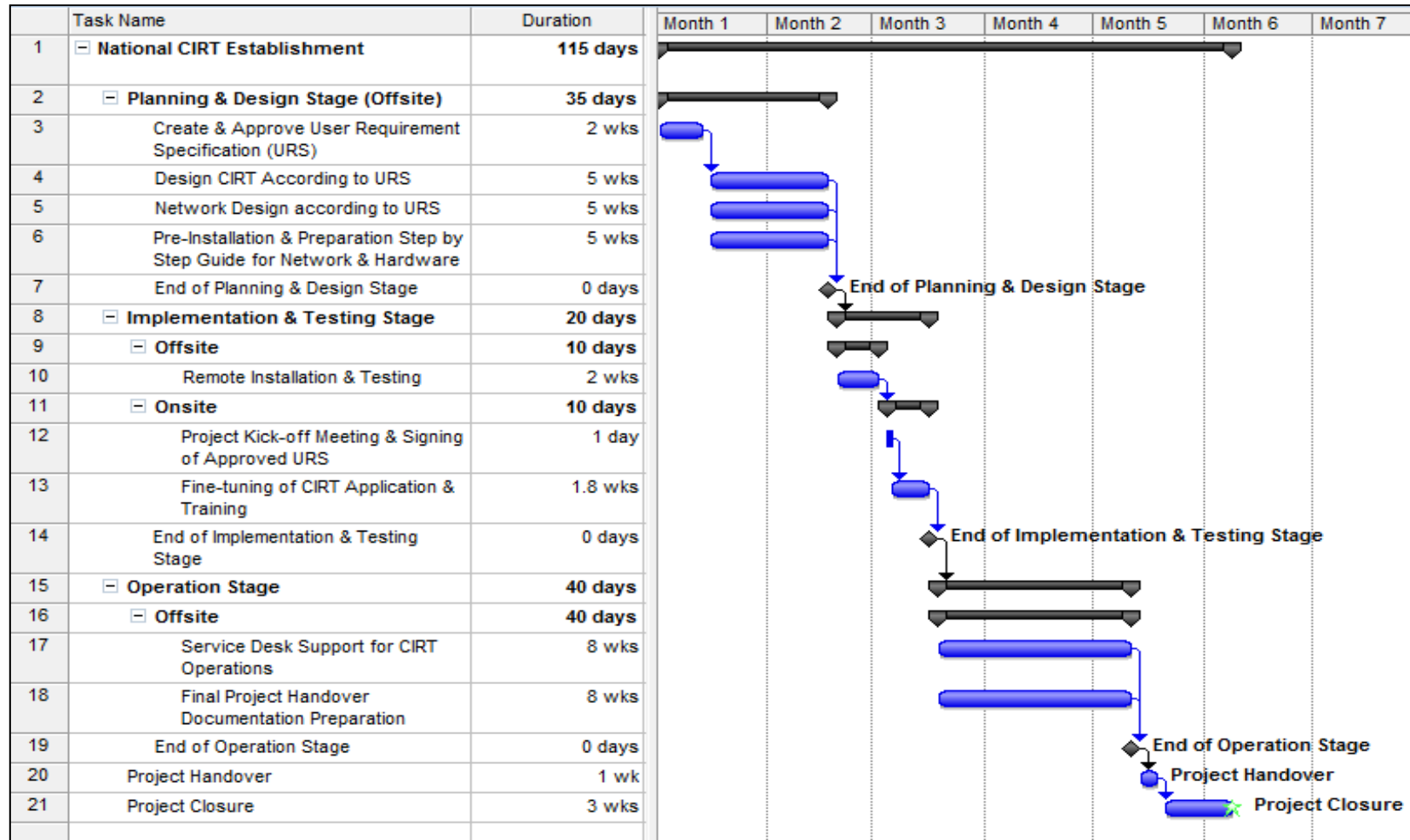
**Table 1- Project Budget in CHF**

<b>SPONSOR CLASSES</b>	<b>DESCRIPTION</b>	<b>ESTIMATES</b>
	<b>EXTERNAL SERVICES*</b>	
3310	Sub-contracts ITU-D	<b>93,564</b>
	<b>MISSION EXPENSES</b>	
3111	DSA-Staff	2,300
3112	Transportation –Staff	4,140
3113	Misc. Mission –Staff	920
3141	DSA-SSA Consulting	14,720
3142	Transportation – SSA Consulting	9,200
3143	Misc. Mission – SSA Consulting	3,680
	<b>Subtotal</b>	<b>34,960</b>
	<b>Total</b>	<b>128,524</b>
	<b>OTHER CHARGES</b>	
3730	AOS (7.5%)	<b>9,639</b>
	<b>GRAND TOTAL</b>	<b>138,163</b>

<b>* Details of External Services</b>	
<b>Description</b>	<b>Amount</b>
CIRT and CIRT Solutions Design and Development	12,512
Customisation of Training Materials + Training Activities	12,512
Customisation and Development of Processes	25,024
CIRT Solutions Fine Tuning and Customization	17,204
Installation of CIRT Solutions + Testing	6,256
Operations and Implementation assessment	6,256
Post implementation phone and e-mail Support (12 months)	13,800
<b>Inclusive of assessment, awareness, planning, design, implementation and support reporting, and server hardening.</b>	<b>93,564</b>

**Annex B. Work plan and CIRT Methodology Overview**

The table 2 below identifies the main tasks necessary for the successful implementation of this project, the expected timeframe for their completion and the CIRT Methodology Overview .



CIRT Methodology Overview			
Planning & Design	Implementation	Operations	Collaboration
<ul style="list-style-type: none"> <li>• Determine &amp; Confirm Constituency</li> <li>• Define &amp; Confirm Mission Statement</li> <li>• Determine CIRT Services</li> </ul>	<p>People:</p> <ul style="list-style-type: none"> <li>• Trainings</li> </ul>	<ul style="list-style-type: none"> <li>• Incident Handling Activities</li> <li>• Information Dissemination</li> </ul>	<ul style="list-style-type: none"> <li>• Cooperation Between Other CIRTs</li> </ul>
<ul style="list-style-type: none"> <li>• Determine Reporting Structure, Authority &amp; Organisation Model</li> <li>• Define CIRT Processes &amp; Workflow</li> <li>• Develop Policies, Procedures and Documentations</li> </ul>	<p>Process:</p> <ul style="list-style-type: none"> <li>• Finalised CIRT Processes &amp; Workflow</li> <li>• Finalised Policies, Procedures &amp; Documentations</li> </ul>	<ul style="list-style-type: none"> <li>• Managing CIRT Staff</li> <li>• Managing CIRT Infrastructure</li> <li>• Identify CIRT Media Spokesperson(s)</li> </ul>	
<ul style="list-style-type: none"> <li>• Identify Interactions with Key Parts of the Constituency</li> <li>• Define Roles and Responsibilities for Interactions</li> <li>• Determine Technology Requirements (HW, SW, Tools, etc.)</li> </ul>	<p>Technology:</p> <ul style="list-style-type: none"> <li>• Assess Infrastructure for the Constituency</li> <li>• Hardware &amp; Software Installation</li> </ul>	<ul style="list-style-type: none"> <li>• Disaster Recovery Plan</li> <li>• Quality Assurance Review</li> </ul>	
<ul style="list-style-type: none"> <li>• Human Resource Requirements</li> <li>• Capacity Building</li> <li>• Communications Approach</li> <li>• CIRT Facilities</li> </ul>	<p>Others:</p> <ul style="list-style-type: none"> <li>• Legal Issues</li> <li>• CIRT Announcement</li> </ul>		