NATIONAL CYBERSECURITY STRATEGY - SUDAN

DECEMBER 2012

Document Review & Approval
This document was authored by Abdulla Al-Attas, GRC Analyst from IMPACT and to be reviewed by <Reviewer name>, <Department Name> from IMPACT with the approval of Anuj Singh, Director GRC from IMPACT and Marco Obiso, Cybersecurity Coordinator from ITU

Table of Contents

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 (CNI) are now at risk over the Internet.

Overall reliance on the Internet continues to increase, 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, analyse, and respond to cyber-attacks across different business sectors and national borders. The Internet itself has become a critical infrastructure to many nations, businesses and people that must also be protected.

Internationally, awareness is developing rapidly of the challenges associated with society's dependence on Information and Communications Technology (ICT). This dependency has arguably become the defining feature of a modern, interconnected and knowledge-based society and economy. The machinery of government, the Critical National Infrastructure (CNI) and the provision of essential services such as water, gas, electricity, communications and banking are all ICT-dependent to a large degree. With this dependency can come vulnerability to aggressors, criminals and even the merely mischievous; Public and media attention is frequently drawn to tales of hacking and espionage and there is persistent interest in and concern about the rapid growth of cyber-crime such as banking fraud and identity theft.

Most countries have a national security body often the Computer Incident Response Teams (CIRT)'s which serve as a focal point for securing cyberspace and the line of defence to protect the country's classified information 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 when dealing with cybersecurity issues. The level of Readiness of a national CIRT needs to be constantly evaluated to help ensure the protection of the nation's Critical Information Infrastructures and thus ensure the overall plan on the country's approach to cybersecurity related issues are initiated.

For countries which are starting to develop their own National Cybersecurity Strategy, it is often difficult to identify best practices and good examples. Many of these countries may not have the same resources as the industrialized nations and cannot build complex and comprehensive organizations; rather, they can only focus on implementing only the most urgent measures. By concentrating on top priorities, cooperation between various stakeholders, flexibility and adaptability, relatively inexpensive solutions can be developed to meet country-specific needs. As the structure of the National Cybersecurity Strategy has to be designed in relation to its essential tasks, identifying the main duties and responsibilities is vital.

PROJECT OBJECTIVES

The main objective of this project is to assist the partner country in enhancing its National Cybersecurity Strategy through key areas that been prioritized by the respective country. The following are the area of concern:

- Critical National Information Infrastructure Protection (CNIIP).
- CIRT Readiness Assessments
- CIRT Implementation (Phase 2)
    a) Network Security Monitoring (IDS and Honeynets).
    b) Enhancing Digital Forensic Capabilities.

By studying, evaluating and implementing the above key areas ITU-IMPACT will assist the partner countries in strengthening its National Cybersecurity Strategy to defend against cyber threats. Based on the analysis which will be carried out through various means as discussed in the assessment approach section, some key recommendations will be made to the country intended to make its National Cybersecurity Strategy resilient and effective. The assessment exercise will evaluate the readiness of the partner country and its approach for ensuring cyberspace incidents, intrusion attempts, and emergencies are appropriately detected, channelled and managed to levels consistent with international standards and good practices.

The project also aims to identify an acceptable national level framework on cybersecurity that can be used as a reference by the member states for protecting the assets that are of national interest and security.

The final outcome and deliverable for each key area will be a report which will contain key issues, key findings and analysis, benchmarks and recommendations. The report will be prepared and submitted to ITU within 10 days after the experts have completed the project.

PROJECT SCOPE AND APPROACH

1.1. CNIIP Project Scope

This CNIIP assessment mission will be carried out during the predetermined time period agreed by all parties. Under the direction of the ITU, and in cooperation with the national counterparts and in close collaboration with the relevant Ministries/Agencies of the member state, ITU/IMPACT experts will undertake the following activities on-site and off-site:

- Study and identify the country's current critical information infrastructure on the national as well as sectorial level.
- Assist in identifying the risks to that respective critical national information infrastructure.
- Evaluate the current, processes, organizational bodies and other establishments, if any put in place as the national cyber security framework.
- Address the immediate concerns by carrying out a gap analysis with each identified critical sector and how best they can contribute in CNIIP plan.
- Taking all CNI sectors into confidence create a roadmap for establishing a centralised platform, such as a CIRT, which manages the critical information infrastructure of the country at a national level.
- Raising awareness of cyber security and its implications in various sectors of the country's critical information infrastructure via conducting a workshop.
- Suggesting a necessary framework for establishing policies, procedures and institutional arrangements (mechanisms)
- Building capacity amongst critical information agencies, researchers and information security professionals within the country or on a regional level.
- Assist the country in developing Self-Reliance at cybersecurity front
- Suggest the country on evaluating and improving the mechanisms in place continuously once established

1.2. CNIIP Assessment Approach

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 Experts will start its off-site activities by obtaining a copy (through e-mail) of all actual policies and procedures related to the country CIIP framework/policy and how it will deter threat, mitigate vulnerability and minimize consequences effecting the CIIP. The Experts will prepare a questionnaire which is attuned with the CIIP assessment objectives and scope. The Experts will plan and prepare a list of all the required documents to review from the current structure of the CIIP during the on-site assessment.

There are two main methodologies in which this assessment and workshop can be take place:

- All identified CNII sector representatives are assembled at one place where a 5 day workshop is run in collaboration with the host country authorities. Educating and discussing with the representatives all CNIIP plans and implementations.

- All identified CNII sector representative are assembled at one place for the initial one or two days only to make them aware of this assessment, its requirements and other modalities and then for the remaining days individual sectors are studied and analysed.

If necessary these plans can be adjusted to suit the actual availability of the relevant officials who will participate in the assessment. Following these meetings the team will undertake a brief tour of the areas (if applicable) and get to know relevant personnel from different CNII sectors before starting the assessment process. The team will work together most of the time but may occasionally undertake short assessment sessions with different CIIP sector when this is required.

The team will record all findings needed to establish the "As-Is" state of the country CIIP framework. These findings will be recorded on a confidential checklist prepared by the team. The assessment methods will be mainly meetings, interview sessions, site visits, questionnaires, and workshops.

Phase 1 – Off-site Assessment (7 Man days x 2 Experts)

Obtain a copy of CNIIP answered questionnaire that has been sent across and relevant documentation including;

- Best Practises, Guidelines, Policies and Procedures currently in place.
- Complete list of critical sectors organisations that the country has identified.
- Organizational chart that identifies organizations/people who are responsible for implementing and coordinating the CIIP framework
- Roles and responsibilities of critical sectors that have been identified.
- Current Partnership models and Policies being used at the international, national or sectorial level.
- List of Partners, Councils or any relevant agencies involved in CIIP implementation.
- Policies to coordinate with internal agencies as well as international agencies taking into account policies for ITU IMPACT initiative on CIRT and CIIP
- List of technical and procedural measures that assist in deterring threats, mitigating vulnerabilities and minimize consequential losses, and help in sharing of information between public-private sector partners.

Phase 2– On-site Assessment (5 Man days x 2 Experts)

- Assessment as per project scope.

Phase 3– Reporting (10 Man days x 2 Experts)

- Reporting in Electronic form
- Current state key issues, key findings & analyses of the country CNIIP
- Recommendations

2.1. CIRT Assessment Project Scope

The CIRT assessment project will be carried out during the predetermined time period agreed by all parties. Under the direction of the ITU, and in cooperation with the national counterparts and in close collaboration with the relevant Ministries/Agencies of the member state, ITU/IMPACT experts will undertake the following activities on-site and off-site:

- Study all current policies, procedures, and forms developed for computer incident, intrusion, or emergency response process.
- Review the risk assessment process employed to determine the computer incident, intrusion and/or emergency response processes.
- Evaluate the tools designed and used to prevent and detect computer incidents or intrusions.
- Check information security events.
- Capacity building programmes for Sudan-CERT.
- Check the roles and responsibilities of key positions that have been identified as necessary to respond to computer incident, intrusion, or emergency.
- Review and evaluate the computer incident, intrusion, emergency, or evidences reported to management.

2.2. CIRT Assessment Approach

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 Experts will start its off-site activities by obtaining a copy (through e-mail) of all actual policies and procedures, and compare them with all policies and procedures used to address computer incident, intrusions, or emergency responses process. The Experts will prepare a questionnaire which is attuned with the CIRT assessment objectives and scope. The Experts will plan and prepare a list of all the required documents to review from the current structure of the CIRT during the on-site assessment.

The Experts will then begin its on-site activities with a brief opening meeting to review the “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 the area and get to know 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, interview sessions, visits and photographing. A verbal report will be provided at the closing meeting to acquaint the officials with the findings and to offer preliminary recommendations.

Phase 1 – Off-site Assessment (7 Mandays x 2 Experts)

- Obtain a copy of all Sudan-CERT relevant documentation including;
  - Standard Operating Procedures, roles and responsibilities
  - Areas of proactive and reactive response measures

- complete inventory of the tools that have been purchased to prevent and/or detect a computer incident or intrusion
- organization chart that identifies positions/employees who are responsible for the computer incident, intrusion, or emergency process
- roles and responsibilities of key positions that have been identified as necessary to respond to computer incident, intrusion, or emergency
- Current Membership Policies.
- Policies to coordinate with internal agencies as well as international CIRTs taking into account policies for ITU IMPACT initiative on CIRT
- Current specifications for hardware and software

Phase 2– On-site Assessment (4 Mandays x 2 Experts)

- Assessment as per project scope.

Phase 3– Reporting (8 Mandays x 2 Experts)

- Reporting in Electronic form
  - Current state key issues, key findings & analyses of Sudan-CERT
  - Recommendations

3.1. CIRT Implementation (Phase 2) Project Scope

This project is to assist the Sudan-CERT in further developing its cybersecurity capabilities, to provide proactive services to the constituents, in terms Network Security Monitoring (NSM) and enhancing the incident response (Digital Forensic) to mitigate cyber threats within six (6) months from the date of the project kickoff meeting.

The CIRT implementation (Phase 2) project will be carried out during the predetermined time period agreed by all parties. Under the direction of the ITU, and in cooperation with the national counterparts and in close collaboration with the relevant Ministries/Agencies of the member state, ITU/IMPACT experts will undertake the following activities:

- To enhance the national CIRT capability, able to provide its constituents with reactive and proactive services.
- To train at least 3 staff from Sudan-CERT to mitigate, contaminate and analyze cyber incident.
- To raise human capability and capacity in the field of cybersecurity.
- To improve Sudan-CERT reactive and proactive services and on the identification, prevention, response and resolution of cybersecurity incidents at identified constituents of the CIRT.
- To expand the utilisation and operation of the CIRT by building an effective and efficient capable CIRT that is ready to respond to cyber threats.
- To assist the government of Zambia with the development of national security awareness programmes to improve cybersecurity posture of the identified constituents.
- To effectively implement security measures and apply effective responses when threats occur.
- To implement, review and test day-to-day operations on processes and workflow developed for the CIRT.
- To implement, review and test tools that are required for the operation of the CIRT.

Project Assumptions and Dependencies

The project assumes that the availability of resources for the project is always accessible. This includes human resources as well as the facilities needed for the smooth implementation of the project.

Due to the limited implementation time, this project is dependent on the suitable human resources assisting to complete all project activities on time to allow the subsequent activity to continue. Failing which, the project will suffer in terms of delay in submission of its intended deliverables.

Listed below are items that are required to be made available on-site to the ITU/IMPACT experts to complete the onsite activities successfully. Should there be any issue in ensuring the availability of any of the items; the experts must be notified at least one week prior to the start of the onsite activities.

No	Items	Quantity
1	A secure work area	1
2	Laser printer	1
3	Photocopy machine/Scanner	1
4	LCD Projector	1
5	Broadband Internet connection	For 2 computers
6	Telephone (with IDD)	1
7	Training facility with Computer & Internet connection	To cater for all participants
8	Official Transportation	1

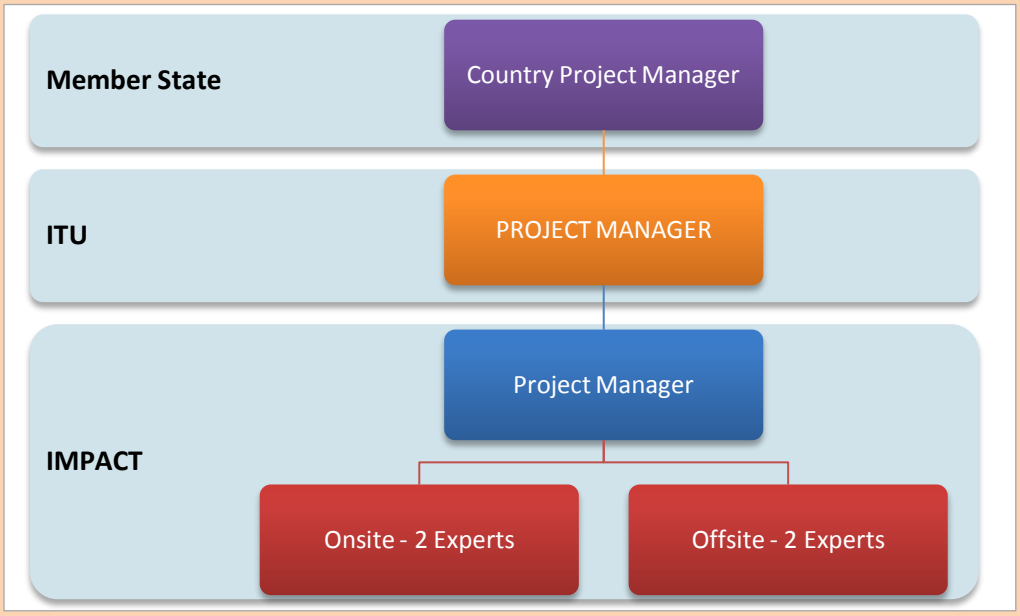
The project is also highly dependent on necessary documents and information that are promptly provided by the country. This is crucial for the successful implementation of the project as it is an assessment based project.

Project Organization

The Stakeholders for this project are as below;

- International Telecommunication Union (ITU) – Project Owner
- IMPACT – Project Implementer
- Government of member state – Partner Country

Figure 1: Organization Structure of the Project Implementation Team



Project Risk Management

1. **Initial Defined 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.
   - Travel Delays
   - Health-related conditions
   - Natural Disaster

2. **Project Assumption**
   - 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 "Project Assumption & Dependencies).

3. **Project Constraint**
   - Time to prepare.

4. **Project Interdependencies**
   - None.

5. **Issue & Change Request Management**
   - Will be administrated.

END OF DOCUMENT