

# AFRICA

## **ITU-IMPACT CIRT Assessment at Kampala, Uganda, April 2010**

ITU-IMPACT Alliance conducted a CIRT readiness assessment and capacity building program for the team at Kampala, Uganda, in April 2010. The mission was aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country. CIRT assessments were conducted for Uganda, Tanzania, Kenya and Zambia.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is imminent that the governments of identified countries should focus on setting up a National CIRT, which must be appropriately position within the government's institutional and organizational structure, as soon as possible.

## **ITU-IMPACT CIRT Assessment at Ouagadougou, Burkina Faso, May 2010**

Sivanathan Subramaniam, Manager of Global Response Centre (GRC) and Kayltana Sabin, GRC Analyst, conducted a CIRT readiness assessment and capacity building program for the team at Ouagadougou, Burkina Faso, in May 2010. CIRT assessments were conducted for Burkina Faso, Nigeria, and Côte d'Ivoire.

The mission was aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- h) Study and analyze the countries' current Cybersecurity status and needs.
- i) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- j) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- k) Capacity building program for the CIRTs.
- l) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- m) Design specifications for hardware and software for the CIRTs.
- n) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is imminent that the governments of identified countries should focus on setting up a National CIRT, which must be appropriately position within the government's institutional and organizational structure, as soon as possible.

## **ITU-IMPACT CIRT Assessment in Cote d'Ivoire, May 2010**

The International Telecommunication Union (ITU) and the International Multilateral Partnership Against Cyber Threats (IMPACT), had successfully conducted a Computer Incident Response Team (CIRT) assessment for Cote d'Ivoire at Yamoussoukro, in May 2010.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current cybersecurity status and needs.
- b) Provide high-level recommendations to improve the cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

The assessment focused on recommendations to improve the existing CIRT. The stakeholders should focus on positioning the CIRT in a strategic manner in order to address the cybersecurity needs of the country. Based on the assessment carried out, it is imminent that the government of Cote d'Ivoire should focus on setting up a National CIRT which must be appropriately positioned within the government's institutional and organizational structure as soon as possible.

## **ITU-IMPACT CIRT Assessment at Yaoundé, Cameroon, December 2010**

The International Telecommunication Union (ITU) and the International Multilateral Partnership Against Cyber Threats (IMPACT), had successfully conducted a Computer Incident Response Team (CIRT) assessment at Yaoundé, Cameroon in December 2010. CIRT assessments were conducted for Cameroon, Chad, Democratic Republic of Congo and Gabon.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is recommended that the government of identified countries should focus on setting up national CIRT, which must be appropriately positioned within the government institutional and organisational structure, as soon as possible

## **ITU-IMPACT CIRT Assessment at Senegal, November 2011**

ITU-IMPACT Alliance conducted a CIRT readiness assessment and capacity building program for Senegal, Niger, Togo and Gambia at Dakar, Senegal in November 2011. The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is imminent that the governments of identified countries should focus on setting up a National CIRT, which must be appropriately position within the government's institutional and organizational structure, as soon as possible

## **ITU-IMPACT CIRT Assessment in Benin, April 2012**

ITU-IMPACT Alliance conducted a CIRT readiness assessment and capacity building program for Benin at Proto-Novu, in April 2012. The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist Benin in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is recommended that the government of Benin should focus on setting up national CIRT, which must be appropriately positioned within the government institutional and organisational structure, as soon as possible.

## **ITU-IMPACT CIRT Assessment for Botswana, October 2012**

ITU-IMPACT Alliance conducted a CIRT readiness assessment and capacity building program for Botswana at Gaborone, in October 2012. The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist Botswana in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- i. Study and analyze the countries' current Cybersecurity status and needs.
- ii. Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- iii. Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- iv. Capacity building program for the CIRTs.
- v. Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- vi. Design specifications for hardware and software for the CIRTs.
- vii. Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is recommended that the government of Botswana should focus on setting up a national CIRT, which must be appropriately positioned within the government institutional and organizational structure, as soon as possible.

## **ITU-IMPACT CIRT Assessment in Lesotho, November 2012**

ITU-IMPACT Alliance conducted a CIRT readiness assessment and capacity building program for Lesotho at Maseru in November 2012. The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist Benin in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is imminent that the government of Lesotho should focus on setting up a national CIRT, which must be appropriately positioned within the government's institutional and organizational structure, as soon as possible.



## **ITU-IMPACT CIRT Assessment in Burundi, November 2012**

ITU-IMPACT Alliance conducted a CIRT readiness assessment and capacity building program for Burundi at Bujumbura in November 2012. The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist the Burundi in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is recommended that the government of Burundi should focus on setting up a national CIRT, which must be appropriately positioned within the government institutional and organizational structure, as soon as possible.

## **ITU-IMPACT CIRT Assessment in Mauritania, December 2012**

ITU-IMPACT Alliance conducted a CIRT readiness assessment and capacity building program for Mauritania in December 2012. The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

The assessment results show that in order to establish a National Cybersecurity Agency (NCA) the government must take into consideration all needs and responsibilities from the national Cybersecurity stakeholders. The success of the NCA depends on the coordinated effort of all stakeholders and their constituencies.

## **ITU-IMPACT CIRT Assessment at Accra, Ghana, November 2011**

Jairam Ramesh, Manager of Security Assurance and Nadher Al-Safwani, Manager of Security Assurance conducted a CIRT readiness assessment and capacity building programme for Ghana at Accra, in November 2011. The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the cybersecurity posture of the country.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current cybersecurity status and needs.
- b) Provide high-level recommendations to improve the cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is recommended that the government of Ghana should focus on setting up national CIRT, which must be appropriately positioned within the government institutional and organizational structure, as soon as possible.

## **ITU-IMPACT CIRT Assessment in Djibouti, December 2012**

Jairam Ramesh, Manager of Security Assurance and Nadher Al-Safwani, Manager of Security Assurance conducted a CIRT readiness assessment and capacity building program for Djibouti in December 2012. The missions were aimed at assisting the country in assessing its readiness to implement a national CIRT – a national CIRT will provide the capability to identify, respond and manage cyber threats as well as to enhance the Cybersecurity posture of the country.

The primary objectives of this project are to assist the identified countries in the assessment of its readiness to implement a National CIRT (Computer Incident Response Team) and fulfil all the descriptions of duties as stipulated in the Project Scope below.

The scope of the assessment consists of:

- a) Study and analyze the countries' current Cybersecurity status and needs.
- b) Provide high-level recommendations to improve the Cybersecurity posture of the countries.
- c) Study and suggest institutional and organizational requirements, and arrangements for setting-up National CIRTs.
- d) Capacity building program for the CIRTs.
- e) Conduct trainings for human capacity building to impart knowledge and skills for operation, maintenance and coordination of CIRTs with relevant agencies, both local and international.
- f) Design specifications for hardware and software for the CIRTs.
- g) Include all the above mentioned details with a Mission Report and any other information deemed necessary in a report to be submitted in electronic copy to ITU.

Based on the assessment carried out, it is recommended that the government of the Djibouti should focus on setting up a national CIRT, which must be appropriately positioned within the government institutional and organisational structure, as soon as possible.