



## Training Course Outline

ITU and National Computer Board / Computer Emergency Response Team of Mauritius

Title	Cyber disaster response: development of simulation exercises
Modality	Online instructor-led
Level	Intermediate
Dates	14 – 16 June 2023
Duration	3 days (9 hours, Zoom sessions, Exercises)
Language	English
Region	World or Multi-Regional
Registration type	Application and selection
Registration deadline	2 <sup>nd</sup> June 2023
Training fees	Free

Description	<p>Cyber security exercises are a very effective way of learning the practical aspects of information security. But designing such exercises is not an easy task. This course provides a number of steps and guidelines that should be followed when designing a cyber exercise. The steps include defining the objectives, choosing an approach, designing network topology, creating a scenario, establishing a set of rules, choosing appropriate metrics and learning lessons.</p> <p>These 3 days training course examines the key elements required to develop Cyber Disaster Response Simulation exercises. It will enable participants to increase collaboration, through greater understanding and familiarity of interaction between private and public sector and a better understanding of cyber-attacks as well as the protection and defense of critical information infrastructures so that knowledge and skills for planning, implementing, and following up on cyber disasters can be improved.</p>
Training topics	<i>Cybersecurity</i>
Certification	<i>Certificate</i>
Code	<i>23OI100191MUL-E</i>

## 1. TARGET POPULATION

- Chief Information Officers
- Chief Technical Officers
- Chief Information Security Officers
- Information Security Officers
- Security Directors
- Security Managers
- Network Engineers
- Systems Administrators

## 2. ENTRY REQUIREMENTS

Experience in Incident response, Network Security, Information System Security and System administration.

## 3. TRAINING OBJECTIVES

The main objective of the course is to enable participants to develop simulation exercises that will help them build their capabilities and train them in handling cyber incidents. Other objectives include:

- Develop crisis management capabilities and leadership with responsible actors;
- Improve the ability to interact with other actors in the crisis management system;
- Increase the ability to make quick decisions and communicate situation information;
- Develop the participants' knowledge and skills in incident response;
- Maintain awareness of the complexity that is characteristic of crisis situations;
- Examine and develop contingency plans that mirror reality;
- Highlight weaknesses and strengths in resources and technology.

Upon completion of this course, participants will be able to::

- Develop incident response and crisis management plans;
- Develop and design a cyber security simulation exercise;
- Learn how to execute the simulation exercises such as TTX and technical simulations.

## 3. METHODOLOGY

The training will be carried out online through the ITU Academy Platform. It will include presentations by instructors and explanation on the group work exercises.

## 4.ASSESSMENT AND GRADING

An exam consisting of 25 – 30 multiple choice questions will be carried out at the end of the last day.

Participants who will achieve a total score higher than 70% will obtain the ITU certificate.



## 5. TRAINING DETAILS & INSTRUCTIONAL APPROACH

Day	Sessions/Topics covered	Key learning points (detail learning outcomes)	Training activities details
<b>Day 1</b> <b>14 June 2023</b> <b>11am – 1pm</b> <b>(CEST)</b>	<b>Exercise Preparation &amp; Planning</b> <ul style="list-style-type: none"> <li>• Cybersecurity preparedness</li> <li>• Cyber incident response plan</li> <li>• What is a simulation exercise?</li> <li>• Benefits of simulation exercises</li> <li>• Types of exercises</li> <li>• Exercise planning</li> </ul>	<ul style="list-style-type: none"> <li>• Understanding of the development of a cyber incident response plan</li> </ul>	<ul style="list-style-type: none"> <li>• Interaction with participants</li> <li>• Discussion on the topics</li> <li>• Discussion on case-studies and practical scenarios</li> </ul>
<b>Day 2</b> <b>15 June 2023</b> <b>11am – 1pm</b> <b>(CEST)</b>	<b>Exercise Preparation &amp; Planning (contd.)</b> <ul style="list-style-type: none"> <li>• Actors and roles in exercise organisation</li> <li>• Design components and development of scenarios</li> <li>• Scenario example walkthrough</li> <li>• Establishment of communication channels, planning of logistics, support materials and pre-exercise training</li> <li>• Best practices</li> </ul>	<ul style="list-style-type: none"> <li>• Formulation of the requirements for developing cyber exercises scenarios.</li> </ul>	<ul style="list-style-type: none"> <li>• Interaction with participants</li> <li>• Discussion on the topics</li> <li>• Discussion on case-studies and practical scenarios</li> </ul>

<p><b>Day 3</b> <b>16 June 2023</b> <b>11am – 1pm (CEST)</b></p>	<p><b>Implementation &amp; Evaluation</b></p> <ul style="list-style-type: none"> <li>• Information Gathering</li> <li>• Exercise Elaborated</li> <li>• Implementation of a TTX Scenario</li> <li>• Infrastructure Requirements</li> <li>• Simulation Environment</li> <li>• Example of the Implementation of a Simulation Exercise</li> </ul>	<ul style="list-style-type: none"> <li>• Environment setup and the implementation of cyber exercises</li> </ul>	<ul style="list-style-type: none"> <li>• Interaction with participants</li> <li>• Discussion on the topics</li> <li>• Conducting the Exam</li> </ul>
--	---	---	--

## 6. TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Title	Contact details
Dr. Kaleem Ahmed Usmani	Officer-in-Charge, CERT-MU	kusmani@cert.govmu.org
Mr. Sachindra Reechaye	Information Security Specialist	sreechaye@cert.govmu.org
Mrs. Selvana Naiken Gopalla	Information Security Specialist	sgopalla@cert.govmu.org

## 7. TRAINING COURSE COORDINATION

Course coordinator	ITU coordinator
Name: Manish Lobin Title: Mr Email address: mlobin@cert.govmu.org	Name: Emmanuel Niyikora Title: Mr Email address: <a href="mailto:emmanuel.niyikora@itu.int">emmanuel.niyikora@itu.int</a>