



**ITU Centre of Excellence Network for Africa
National Computer Board / Computer Emergency Response Team of Mauritius**

**Online Training Course on
Building an effective Cyber Incident Response Team
17 – 19 November 2021**

COURSE OUTLINE

COURSE DESCRIPTION

Title	Building an effective Cyber Incident Response Team
Objectives	<p>The main objective of this training course is to allow participants to acquire sufficient knowledge on how to empower an incident response team for effective incident resolution and mitigate the impact of security threats within their organizations. Other objectives include:</p> <ul style="list-style-type: none">• Learning the fundamentals of incident response, different incident response approaches from established international frameworks, the need for setting up a dedicated team and types of incident response teams• Learning the basic requirements of an incident response team and assessing the team's effectiveness• Learning about different strategies that can be employed to enhance an existing incident response team's functions
Dates	17 – 19 November 2021
Duration	3 days
Registration start date	28 September 2021
Registration deadline	12 November 2021
Training fees	No charge
Course code	21OI26527AFR-E

DESCRIPTION

The frequency and complexity of today's cyber attacks makes incident response a critical function for organizations. The management of an incident response team is a very often-neglected topic. Incident response is the last line of defense against cyber attacks for many organisations or even countries.

Detecting and efficiently responding to incidents requires strong management processes and driving an incident response team requires special skills and knowledge. A background in information security management or security engineering is not sufficient for managing incidents. On the other hand, incident responders with strong technical skills do not necessarily become effective incident response managers.

LEARNING OUTCOMES

This 3-day training course examines the key elements required to develop and improve the effectiveness of an incident response team. By the end of the course, participants will be able to understand the functions of an incident response team, how to assess their maturity and how to improve on existing capabilities.

TARGET POPULATION

- Current and future CSIRT/CIRT/CERT managers and team members
- C-level managers such as CIOs, CSOs, CROs, CISOs
- Project leaders interested in establishing or starting a CSIRT/CIRT/CERT
- Cybersecurity professionals such as information security analysts, security engineers, incident handlers, network security administrators, malware analysts, IT professionals from ISPs, RENs, IXPs, SOCs, NOCs, TLDs, amongst others
- Other staff who work closely with CSIRTs/CIRTs/CERTs and would like to gain a deeper understanding of how these teams operate, e.g. CSIRT/CIRT/CERT constituents, higher-level management, media relations, human resources, audit or risk management professionals.

ENTRY REQUIREMENTS

Knowledge in cybersecurity and incident response

TUTORS/INSTRUCTORS

NAME OF TUTOR(S)/INSTRUCTOR(S)	CONTACT DETAILS
Kaleem Usmani	kusmani@cert.ncb.mu
Sachindra Reechaye	sreechaye@cert.ncb.mu
Selvana Naiken Gopalla	sgopalla@cert.ncb.mu

EVALUATION

Evaluation of participants at this course will be based on the following:

Evaluation Type	Percentage Score%
Class Attendance	N/A
Assignments	N/A
Quiz	100%
Forum Participation	N/A
TOTAL	100%

Only participants who have successfully completed all assessments with a pass mark of 60% shall be awarded the ITU Certificate

TRAINING SCHEDULE AND CONTENTS

Session	Topic
Day 1 17 Nov 2021 11am – 2pm (Geneva Time)	Introduction to incident response and management <ul style="list-style-type: none">• What is incident response?• Types of incidents• Existing incident response frameworks• Incident response from a CERT's perspective• The rationale behind setting up an incident response team• Types of incident response teams
Day 2 18 Nov 2021 11am – 2pm (Geneva Time)	Design, establishment and assessment of incident response teams <ul style="list-style-type: none">• Requirements for the setup of an incident response team• Operationalisation of the team• Assessment of the team
Day 3 19 Nov 2021 11am – 2pm (Geneva Time)	Incident response teams improvement strategies <ul style="list-style-type: none">• Enhancement strategies• Exam

METHODOLOGY

The training will be carried out online through the ITU Academy Platform. It will include presentations, discussion, group work, case studies and an exam.

COURSE COORDINATION

[Details of the course coordinators and their contact details]

Course coordinator: Name: Mr. Manish Lobin Email address: mlobin@cert.ncb.mu	ITU coordinator: Name: Emmanuel Niyikora Email address: emmanuel.niyikora@itu.int
---	---

REGISTRATION AND PAYMENT

ITU Academy portal account

Registration should be made online at the ITU Academy portal.

To be able to register for the course you **MUST** first create an account in the ITU Academy portal at the following address: <https://academy.itu.int/user/register>

Course registration

When you have an existing account or created a new account, you can register for the course online at the following link:

<https://academy.itu.int/training-courses/full-catalogue/building-effective-cyber-incident-response-team>

You can also register by finding your desired course in our training catalogue <https://academy.itu.int/training-courses/full-catalogue>

Payment

The training course is free of charge.