Training Course Outline

ITU and NRD Cyber Security

Title	National Cyber Crisis Management
Modality	Online instructor-led
Level	Introductory
Dates	14/11/2023 – 15/11/2023
Duration	10 h
Language	English
Region	World or Multi-Regional
Registration type	Direct registration
Registration deadline	31/10/2023
Training fees	400 USD
Description	National cyber crisis management course is the introductory two-day, scenario-based, purpose-built training designed to take students to the intermediate level. The course will include both theoretical and practical components that cover a wide range of topics related to national cyber crisis management. Students will explore the main concepts of cyber crisis management, understand the key roles and responsibilities of key stakeholders involved in national cybersecurity crisis management, including the role CERTs. In addition, the importance of effective crisis communication will be explained during the course. Lastly, the course will include a scenario-based discussion where participants will be able to test the knowledge acquired during the training course.

Training topics	*Cybersecurity*
Certification	*Certificate*
Code	*To be filled by ITU*

1. TARGET POPULATION

This training course is intended for national and sectorial CSIRTs, relevant national cyber crisis management authorities.

2. ENTRY REQUIREMENTS

No prerequisites required.

3. TRAINING OBJECTIVES

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

- Demystify the key concepts and definitions related to cyber crisis and its management;
- Apply the structure and general content of national cyber crisis management plan;
- Define the key roles and responsibilities of cyber crisis management at the strategic and operational level;
- Comprehend the importance of effective cyber crisis communication;
- Utilise the acquired knowledge during scenario-based discussion.

3. METHODOLOGY

This training course is designed to provide practical, real-world insights into cybersecurity crisis management. Participants will have the opportunity to learn from illustrative case studies and analysis, delivered through a range of teaching methods, including lectures, roundtable discussions, case studies, and group play activities.

All necessary course materials, including handouts (where applicable), slide sets, and additional resources, will be provided through the ITU Academy platform.

To ensure maximum engagement and retention, the 4MAT teaching methodology will be utilized in all sessions. This involves interactive discussions on a topic, practical exercises, discussions to identify learning points, and individual note-taking to reflect on relevant habits that can be changed moving forward. At the end of each day, individual notes will be reviewed to reinforce the key takeaways.

4.ASSESSMENT AND GRADING

Besides the final exam (or test) score (80% of total), participants will be evaluated according to their presence, active participation in roundtables, exercises sessions and other course activities (20% of total).

A total score higher than 70% is required to obtain the ITU certificate.

5. TRAINING DETAILS & INSTRUCTIONAL APPROACH

Module	Sessions/Topics covered	Key learning points (detail learning outcomes)	Training activities details
Module 1	Introduction to Cyber Crisis Management. This section covers the fundamentals of cyber crisis management, including defining a cyber crisis and the key principles of crisis management.	Identification of crisis and its types	Lecturing, group discussions
Module 2	Cybersecurity Threats and Vulnerabilities. This section focuses on the various types of cybersecurity threats and vulnerabilities against CIIs that can lead to a cyber crisis.	ENISA Cyber Threat Landscape, MITRE ATT&CK framework	Lecturing, group discussions
Module 3	Crisis Communication. This section focuses on the importance of effective communication during a cyber crisis, including developing communication plans, templates, communicating with stakeholders and the public, and managing the media.	Elaboration of the communication tactics facing the crisis	Lecturing, group discussions, group work on the development of cyber crisis communication plan
Module 4	National cyber crisis management framework. This section focuses on the overall structure and general content for the preparation of the national cyber crisis management plan. It includes defining the purpose and key elements of the plan, including key roles and responsibilities such as national CSIRT and other relevant authorities, developing procedures for detecting and responding to incidents and crises, and conducting drills and exercises for the preparation of cyber crisis management.	Elaboration on a crisis management plan	Lecturing Scenario-based exercise: *a simulation exercise that allows participants to apply the knowledge and skills learned during the course to a realistic cyber crisis scenario.* Final assessment

6. TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Title	Contact details
Dr. Tadas Jakštas	Cyber Security Capacity Building Expert	taj@nrdcs.lt
Živilė Nečejauskaitė	Director of marketing and communication	zn@nrdcs.lt

7.TRAINING COURSE COORDINATION

Course coordinator	ITU coordinator
Title: Training Coordinator Name: Rūta Jašinskienė Email address: rj@nrdcs.lt	Title: Associate Capacity Development Officer Name: Célia Pellet Email address: hcbmail@itu.int