ITU Cybersecurity BDT

Online Training Course on

Lifecycle, principles and good-practices on national cybersecurity strategy development and implementation

TRAINING COURSE OUTLINE (ONLINE)

COURSE DESCRIPTION

Title	Lifecycle, principles and good-practices on national cybersecurity strategy development and implementation
Objectives	The objective of the training is to prepare national leaders and policymakers in thinking strategically about cybersecurity at the national level. Through this training, users will achieve the following learning objectives: • Gain familiarity with the main concepts and definitions of cybersecurity and gain a solid foundation on how cybersecurity operates at the National level • Gain Familiarity with the Guide to Developing a National Cybersecurity Strategy • Learn the five phases of lifecycle of a National Cybersecurity Strategy (Initiation; Stocktaking and Analysis; Production; Implementation; Monitoring and Evaluation) • Learn the cross-cutting principles to be addressed during for developing forward-looking and holistic National Cybersecurity Strategy • Gain familiarity with relevant cybersecurity good practices and how they can be applied in the national context
Dates	26 July-22 December 2021
Duration	4h eLearning + 2h virtual class
Registration deadline	By Invitation only! Application and selection!
Training fees	Free
Course code	21OS26599MUL-E

DESCRIPTION OF THE TRAINING COURSE

Please not that this training is by invitation only.

Cybersecurity is a complex challenge that encompasses multiple different governance, policy, operational, technical and legal aspects. This training provides general knowledge to address, organise and prioritise many of these areas based on existing and well-recognised models, frameworks and other references.

The training focuses on elements for protecting civilian aspects of cyberspace and as such, it covers the overarching principles and good practice that need to be considered in the process of drafting, developing and managing a National Cybersecurity Strategy.

To this end, the training makes a clear distinction between the "process" that will be adopted by countries during the lifecycle of a National Cybersecurity Strategy (initiation, stocktaking and analysis, production, implementation, reviews) and the "content", the actual text that would appear in a National Cybersecurity Strategy document. This training does not cover aspects such as the development of defensive or offensive cyber-capabilities by a country's military, defence forces, or intelligence agencies.

The training also provides an overview of the core components of what it takes for a country to become cyber-prepared, highlighting the critical aspects that governments should consider when developing their national strategies and implementation plans.

Finally, this training provides to policymakers a holistic, high-level overview of existing approaches and applications, and a reference to additional and complementary resources that can inform specific national cybersecurity efforts.

LEARNING OUTCOMES

At the end of this training users will be able to:

- Understand the main concepts and definitions of cybersecurity and understand how cybersecurity operates at the National level
- Efficiently engage with the Guide to Developing a National Cybersecurity Strategy
- Understand the five phases of lifecycle of a National Cybersecurity Strategy (Initiation; Stocktaking and Analysis; Production; Implementation; Monitoring and Evaluation) and how they can be implemented in the national context
- Understand the cross-cutting principles to be addressed for developing a forward-looking and holistic National Cybersecurity Strategy
- Understand relevant cybersecurity good practices and how they can be applied in the national context

TARGET POPULATION

This NCS training is first and foremost targeted at policy-makers responsible for developing a National Cybersecurity Strategy. The secondary audience are all the other public and private stakeholders involved in the development and implementation of a Strategy, such as responsible government staff, regulatory authorities, law enforcement, ICT providers, critical infrastructure operators, civil society, academia and research institutions. The training could also prove useful to the different stakeholders in the international development community, who provide assistance in cybersecurity.

ENTRY REQUIREMENTS

Participants need to be invited to be enrolled in this course.

No specific qualifications or experience are needed to participate in this course. Users are invited to request this training through the ITU Academy platform. The ITU Cybersecurity Team will review the requests and confirm the participation. Policy-makers responsible for developing a National Cybersecurity Strategy are prioritized.

TUTORS/INSTRUCTORS

NAME OF TUTOR(S)/INSTRUCTOR(S)	CONTACT DETAILS
Orhan Osmani	Orhan.osmani@itu.int
Giacomo Assenza	Giacomo.assenza@itu.int

TRAINING COURSE CONTENTS

The training is organised in four eLearning modules and an online Table-top exercise, which are based on the Guide to Developing a National Cybersecurity Strategy. The content will cover the following topics:

- Module 0 Introduction: it introduces participants to the main concepts and definitions of cybersecurity, and provides a solid foundation on how cybersecurity operates at the national level
- Module 1: it provides an overview of the various phases in the development of a Strategy, which include:
    - Initiation
    - Stocktaking and analysis
    - NCS production
    - Implementation
    - Monitoring and evaluation
- Module 2: it presents cross-cutting principles, which help in the development of a forward-looking and holistic National Cybersecurity Strategy, namely :
    - Vision of an NCS
    - Comprehensive approach
    - Inclusiveness
    - Economic and social prosperity
    - Fundamental Human Rights
    - Risk Management and resilience
    - Policy instruments
    - Leadership, roles, and resource allocation
    - Trust environment

- Module 3 : it introduces a set of good-practice elements that can make the Strategy comprehensive and effective, while allowing for tailoring to the national context. These good-practice elements are grouped into the following focus areas:
    - Governance
    - Risk management in national cybersecurity
    - Preparedness and resilience
    - Critical Infrastructure services and essential services
    - Capability and capacity building, and awareness raising
    - Legislation and regulation
    - International cooperation
- Table-top exercise: Virtual TTXs are discussion-based sessions where users meet in a virtual classroom setting and have the opportunity to challenge the acquired knowledge through practical assignments and facilitated discussion. These TTXs will focus on the content of the training as well as on practical experience and best practice participants want to share

TRAINING COURSE SCHEDULE

Session	Topic	Exercises and interactions
Initial Quiz	Cybersecurity basics	Self-paced. If pass mark is achieved (24/30 correct answers) users are redirected to Module 1. If pass mark is not achieved users will have to complete Module 0 and pass the test
Module 0 + Quiz	Cybersecurity basics	Self-paced (1h). Attending the module and successfully completing the quiz is mandatory to move to the next activity. If quiz is failed, the user will have to repeat the module and the quiz
Module 1 + Quiz	NCS Lifecycle	Self-paced (1h). Attending the module and successfully completing the quiz is mandatory to move to the next activity. If quiz is failed, the user will have to repeat the module and the quiz
Module 2 + Quiz	NCS Principles	Self-paced (1h). Attending the module and successfully completing the quiz is mandatory to move to the next activity. If quiz is failed, the user will have to repeat the module and the quiz
Module 3 + Quiz	NCS Best practices	Self-paced (1h). Attending the module and successfully completing the quiz is mandatory to move to the next activity. If quiz is failed, the user will have to repeat the module and the quiz
Practical Assignment	NCS Lifecycle, principles and best practices	Self-paced (off-line). When registering to the Table-top exercise, users will receive a practical assignment. Users have to submit the completed assignment at least 5 days before the Table-top

		exercise. Timely submission is mandatory for participating the TTX
Virtual Table-top exercise (TTX)	NCS Lifecycle, principles and best practices	Virtual class (2h). After the completion of the eLearning modules, users have one year to register to a virtual TTX. ITU will organize regular TTX sessions and users can select the preferred date. Attending the TTX is mandatory for completing the training and receiving the certificate of completion

METHODOLOGY (Didactic approach)

The training will be delivered entirely online and will combine different didactic approaches:

- **4 self-paced eLearning modules**: Modules 0, 1, 2 and 3 are self-paced digital courses presented as slides with information and media (video, audio, and pictures). These modules contain gamification experience such as questionnaires, simulations, drag-and-drop elements etc. These modules are self-paced which leaves the possibility to users to autonomously organise their learning experience and completion of the modules.
- **4 digital quizzes**: each of the modules include a digital quiz of up to 30 questions to test the knowledge and learning progresses of users. Quizzes include different kind of questions (such as yes/no, multiple choices, branching, drag and drop etc.)
- **1 Practical assignment**: upon completion of the eLearning modules, participants will be provided with a practical assignment to be developed and completed autonomously and offline. The assignment consists in a set of theoretical and practical open questions covering the NCS lifecycle, principles, and focus areas. There are not right or wrong answers to these questions, but they are tailored to: a) Strengthen strategical planning; b) Stimulate Critical thinking; c) Raise awareness of the national cybersecurity context; d) Stimulate problem solving; e) Sharing lessons learned. Participants will have to return the completed assignments at least 5 days before the online discussion.
- **1 Table-top exercise**: Virtual TTXs are discussion-based sessions where users meet in a virtual classroom setting and have the opportunity to challenge the acquired knowledge through a facilitated discussion with the plenary group. In order to maximize the formative outputs, TTXs will be guided by ITU facilitators who will be on to control the pace and flow of the exercise. The facilitators will also stimulate the discussion and draw out relevant topics, challenges, lessons learned, solutions, and improvement areas from the debate. The online debate will include elements of interaction and gamification (polls, whiteboards, etc). The TTX will be conducted online through the zoom platform.

EVALUATION AND GRADING

To successfully conclude the training and receive the certificate of completion all participants will have to attend and pass the following elements:

- Initial quiz: the training will start with an initial quiz of up to 30 questions measuring the participant's knowledge and understanding of cybersecurity and national cybersecurity

strategy. If pass mark (80% correct) is achieved the participant will be redirected to Module 1. On the contrary, if the pass mark is not achieved, participants will have to attend Module 0 and successfully repeat the test to proceed.

- End-module quizzes: all modules will conclude with an assessment quiz of up to 30 questions measuring the learning progress of users. the successful completion of the quiz (at least 60% correct) is essential to proceed to the following Module. If the quiz is failed, users will have to repeat the module and re-take the test.

- Practical Assignment: Participants will have to return the completed assignments at least 5 days before the virtual table-top exercise. The assignment is not graded but its completion and timely submission is necessary to take part in the table-top exercise

- Virtual Table-top exercise: Attending the virtual table-top exercise in mandatory to conclude the training. Although there is not an assessment in this phase, participants are expected to actively engage in the conversation and activities conducted during the exercise (gamification, polls, whiteboards, etc)

TRAINING COURSE COORDINATION

Course coordinator:	**ITU coordinator:**
Name: na Email address: na	Name: Orhan Osmani Email address: orhan.osmani@itu.int

REGISTRATION

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

Training 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/lifecycle-principles-and-good-practices-national-cybersecurity-strategy-development-and

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