European Security and Defence College
Doc: ESDC/2022/071
Date: 1 April 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2024**	Activity number **259**	**Course for Cyber Awareness Trainers**	ECTS **1**

Target audience	Aim
The target audience of this specific training programme are civilian or military personnel within an organisation with the responsibility to develop, implement and evaluate cybersecurity awareness programmes in support of wider organisational security objectives.	The course aims to give participants a train-the-Training Manager/Trainer Pilot Course for standardised Cyber Awareness training in EU Member States and EU Institutions. During the course, the formation of networks among individuals will be encouraged. The final goal of the course is to support cybersecurity awareness programmes within EU Institutions and Member States.
Open to: ▪ EU Member States / EU Institutions Bodies and Agencies ▪ ESDC/2021/183: Switzerland, HybridCoE ▪ ESDC/2021/183: (On the basis of reciprocity for all EU MS) NATO CCD CoE	

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Specialised cyber course, at tactical/technical levels* • *Linked with the strategic objectives of Pillar 1 and Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning Outcomes	
Knowledge	LO1- List the main cyber vulnerabilities, including risks and threats for cyber security/defence/crime LO2- Explain cyber awareness, its role in cybersecurity and how to deliver cybersecurity awareness training LO3- Define the main goals of cyber awareness training LO4- Define main principles in cyber awareness training design and implementation LO5- Explain the role and significance of evaluation for cyber awareness training

Skills	LO6– Manage advantages and disadvantages of different cyber awareness approaches and delivery methods LO7- Manage barriers and enablers for cyber awareness training at an organisational level LO8- Manage different evaluative approaches and their relative strengths and weaknesses
Responsibility and Autonomy	LO9– Assess cyber awareness training requirements and design concept approach for developing and delivering courses LO10- Design conceptual evaluation approaches for cyber awareness training courses

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model: it makes use of *level 1 evaluation* (*based on participants' satisfaction with the course*) and *level 3 evaluation* (*assessment of participants' long-term change in behaviour after the end of the course*). *Evaluation feed-back* is given in the level 1 evaluation on the residential modules.

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential modules, including their syndicate sessions and practical activities as well as on their completion of the eLearning phases: course participants must finalise the autonomous knowledge units (AKUs) and pass the tests (*mandatory*), scoring at least 80% in the incorporated out-test/quiz. **However, no formal verification of the learning outcomes is foreseen; proposed ECTS is based on participants' workload only**.

The Executive Academic Board takes these factors into account when considering the award of *Certificates* to participants. Module leaders provide an evaluation report for each residential module. The Course Director is responsible for overall coordination, with the support of the ESDC Secretariat, and drafts the *final evaluation report* which is presented to the Executive Academic Board.

Course structure

The residential module is held over 3 days.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents
1. Cyber Fundamentals (Module 1)	4	1.1 Introducing fundamental concepts related to cyber and cybersecurity
2. Introduction to cyber awareness (Module 2)	4	2.1 Overview of the concept of cyber awareness 2.1.1 Define awareness 2.1.2 Awareness vs compliance 2.1.3 Why does awareness matter? 2.2 Cyber awareness in the European context 2.2.1 Roles and responsibilities/activities in cyber awareness in Europe
3. How to design and develop a cyber awareness programme (Module 3a)	4	3.1 Identifying the needs and requirements for awareness programmes 3.1.1 What organisational attributes matter when it comes to awareness? 3.1.2 Why do we need awareness? 3.1.3 When do we need awareness? 3.2 Identifying awareness objectives and linking to wider organisational goals and security culture 3.3 Enablers and barriers for awareness programmes
4. Ways and methods of delivering awareness (Module 3b)	4	4.1 Overview of different awareness delivery mechanisms 4.2 Strengths and weaknesses of methods

5. Evaluating and measuring performance (Module 3c)	4	4.1 Articulating the importance of evaluation 4.1.1 When to think about evaluation and when to evaluate? What to measure? 4.1.2 Evaluating a module vs evaluating a programme 4.1.3 Maturity as a concept to track progress 4.2 How to identify and develop performance indicators for awareness? 4.3 Different approaches to evaluation and measurement
5. Practical next steps, tools and resources (Module 4)	2	5.1 Summary of key points of course 5.2 Overview of "actionable" next steps 5.3 Inventory of resources developed by other organisations
TOTAL	**22**	

Materials	Methodology
Required: **Recommended:** • Materials will be made available online on the eLearning platform of the ESDC. • Cyber fundamentals • Course overview	The course is based on the following methodology: lectures, panels, workshops, exercises, labs Additional information Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used. All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular. The Chatham House Rule is applied during all residential phase of the course: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed".