European Security and Defence College
Doc: ESDC/2024/050
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Course for Cyber Awareness Trainers	ECTS
Feb. 2026	**259**		**1**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Support ECSF Role 7 Cyber Educator* • *Specialised cyber course, at tactical/technical/ strategic 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)]*

Target audience

The target audience for this training programme is civilian or military personnel within an organisation with responsibility for developing, implementing and evaluating cybersecurity awareness programmes in support of wider organisational security objectives.

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

Aim

The course aims to give participants a training for Training Manager/ Trainer which helps to standardise 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.

Learning Outcomes

Knowledge	L01- List the main cyber vulnerabilities, including risks and threats for cyber security/defence/crime L02- Explain cyber awareness, its role in cybersecurity and how to deliver cybersecurity awareness training L03- Define the main goals of cyber awareness training L04- Define main principles in cyber awareness training design and implementation L05- Explain the role and significance of evaluation for cyber awareness training
Skills	L06– Manage advantages and disadvantages of different cyber awareness approaches and delivery methods L07- Manage barriers and enablers for cyber awareness training at organisational level L08- Manage different evaluative approaches and their strengths and weaknesses

Responsibility and Autonomy	L09– Assess cyber awareness training requirements and design concept approach for developing and delivering courses L10- Design conceptual evaluation approaches for cyber awareness training courses

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model, particularly 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 feedback is given in the level 1 evaluation of the residential modules.

In order to complete the course, participants have to fulfil all the learning objectives, and are evaluated on the basis of their active contribution to the residential modules, including their teamwork sessions and practical activities, and on their completion of the eLearning phases. Course participants must complete the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated test/quiz. However, no formal verification of the learning outcomes is provided for; the proposed ECTS is based solely on participants' coursework.

The Executive Academic Board takes these factors into account when considering whether to award 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 content
Cyber fundamentals (Module 1)	3	Introducing fundamental concepts related to cyber and cybersecurity
Introduction to cyber awareness (Module 2)	4	Overview of the concept of cyber awareness - Define awareness - Awareness vs compliance - Why does awareness matter? Cyber awareness in the European context - Roles and responsibilities/activities in cyber awareness in Europe
How to design and develop a cyber awareness programme (Module 3a)	4	Identifying needs and requirements for awareness programmes - What organisational attributes matter when it comes to awareness? - Why do we need awareness? - When do we need awareness? - The importance on shaping awareness over real cases shared e.g. by SOC, CERTs or built over MITRE ATT&CK. Identifying awareness objectives and linking to wider organisational goals and security culture Enablers and barriers for awareness programmes
Ways and methods of delivering awareness (Module 3b)	9	Overview of different awareness delivery mechanisms Strengths and weaknesses of methods Example of a cyber security campaign (e.g. simple fact-based, short series of message about an event that affects the cyber domain) and cyber awareness campaign (e.g. tailored and developed explanation of who such events affect, the human dimension and how users should respond) Use of technical tools and software for developing e.g. social engineering paradigm, phishing campaigns and cyber awareness videos, among other things (e.g. use of AI tools for a cyber awareness campaign). Voluntary presentations about Cyber Awareness programmes/ campaigns from the participants

Evaluating and measuring performance (Module 3c)	2	Articulating the importance of evaluation - When to think about evaluation and when to evaluate? What to measure? - Impact vs compliance – how and when to use such data - Evaluating a module vs evaluating a programme How to identify and develop performance indicators for awareness? (e.g. during a TTX which gathers successful und least successful cyber awareness campaigns and to evaluate this material incl. solution-oriented discussion). - Evaluating a module vs evaluating a programme How to identify and develop performance indicators for awareness? Different approaches to evaluation and measurement
5. Practical next steps, tools and resources (Module 4)	2	Summary of key points of course Overview of 'actionable' next steps Inventory of resources developed by other organisations
TOTAL	**24**	

Materials

Required:
- AKU 55 - Strategic Compass

Recommended:
- AKU 2 on European Global Strategy
- Council Conclusion on EU Policy on Cyber Defence (22.05.2023)
- EU Policy on Cyber Defence, JOIN(22) 49 final (10.11.2022)
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (NIS 2)
- COUNCIL DECISION (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States
- EU's Cybersecurity Strategy for the Digital Decade (December 2020)
- The EU Cybersecurity Act (June 2019)
- The EU Cyber Diplomacy Toolbox (June 2017)

Additional comments
Bring your own device

Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises and/or labs

Additional information

Pre-course questionnaire on learning expectations and possible briefing topic form 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 supplementary (eLearning) study will reflect current developments in the field of cybersecurity/cyber-defence in general and EU policies in particular. Course participants must be willing to contribute with their specific expertise and experience throughout the course.

The Chatham House Rule is applied during all residential modules 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".