European Security and Defence College
Doc: ESDC/2024/63
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Cybersecurity Auditor**	ECTS
Feb. 2025	**222**		**1**

Target audience	Aim
The participants should be cybersecurity military or civilian officials that wish to develop skills on cybersecurity audit plan and audit report from EU Institutions, Bodies and Agencies as well as EU Member States. Agencies as well as EU Member States. • EU Member States / EU Institutions Bodies and Agencies • Candidate Countries	The aim of the course is to prepare the participants to cybersecurity audits on the organisation's ecosystem, to ensure compliance with statutory, regulatory, policy information, security requirements, industry standards and best practices. Furthermore, this course will allow the cybersecurity officials to exchange their views and share best practices on how to conduct independent reviews to assess the effectiveness of processes and the security controls in place. By the end of this course, the participants will learn how to develop a cybersecurity audit plan and audit report

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber and the EU's Policy on Cyber Defence and Cyber Skills Academy	• *Aligned with ECSF Role 6. Cybersecurity Auditor* • *Specialised cyber course, at strategic level.* • *Linked with the strategic objectives of EU's Policy on Cyber Defence and Cyber Skills Academy*

Learning Outcomes	
Knowledge	LO1- Define cybersecurity auditing procedures LO2- Define the legal, regulatory and legislative compliance requirements LO3- Recognise cybersecurity controls LO4- Describe conformity assessment standards and methodologies

Skills	LO5- Practice auditing frameworks, standards and methodologies LO6- Apply auditing tools and techniques LO7- Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls LO8- Decompose and analyse systems to identify weaknesses and ineffective controls LO9- Collect and evaluate auditing information
Responsibility and Autonomy	LO10- Define audit scope, objectives and criteria to audit again LO11- Develop auditing policy, procedures, standards and guidelines LO12- Develop an audit plan describing the frameworks, standards, methodology, procedures and auditing test LO13- Execute the audit plan and collect evidence and measurements

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 behavior 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, the 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. Introduction to cybersecurity auditing	5(3)	• Cybersecurity auditing procedures • Conformity assessment standards and methodologies • Legal, regulatory and legislative compliance requirements • Cybersecurity technical controls
2. Audit	12(3)	• Auditing tools and techniques • Audit scope, objectives and criteria • Collect and evaluate auditing information • The role of AI in system auditing
3. Reporting	12(3)	• Produce a cybersecurity audit report
TOTAL	29(9)	

Material	Methodology
Required: • **AKU 104: Module 3 – Experience a security incident** • **AKU 104: Module 8 – Review Organisational Controls** • **AKU 104: Module 9 – Review Technical Controls** **Recommended:** *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**)* • *EU Policy on Cyber Defence, JOIN(22) 49 final, 10.11.2022* • *The EU's Cybersecurity Strategy for the Digital Decade (December 2020)* • *The EU Cybersecurity Act (June 2019)* • *The EU Cyber Diplomacy Toolbox (June 2017)* • *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* • *Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)*	The course is based on the following methodology: lectures, panels, workshops, exercises and/or case studies **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".

Developed by: ESDC Secretariat