European Security and Defence College

European Security and Defence College
Doc: ESDC/2025/037
Date: 20 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Cybersecurity Architect**	ECTS
Feb. 2027	***221***		**1**

Target audience	Aim
The participants should be cybersecurity military or civilian officials that wish to develop skills on cybersecurity architecture and cybersecurity controls from EU Institutions, Bodies and Agencies as well as EU Member States. Open to: • EU Member States / EU Institutions Bodies and Agencies	The aim of the course is to prepare the participants to design infrastructures, systems, assets, software, hardware and services based on security-by-design and privacy-by-design principles. Furthermore, this course will allow the cybersecurity officials to exchange their views and share best practices on how to improve architectural models and develop architectural documentation and specifications. By the end of this course, the participants will learn how to develop security-by-design IT solutions and cybersecurity controls.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber and the EU's Policy on Cyber Defence and Cyber Skills Academy	• *Specialised cyber course, at strategic level.* • *Linked with the strategic objectives of EU's Policy on Cyber Defence and Cyber Skills Academy* • *Supports the European Cybersecurity Skills Framework (ECSF) of ENISA Profile role 5. 'Cybersecurity Architect'*

Learning Outcomes	
Knowledge	LO1- Secure development lifecycle LO2- Security architecture reference models LO3- Cybersecurity controls and solutions LO4- Cybersecurity risk management
Skills	LO5- Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles LO6- Decompose and analyse systems to develop security and privacy requirements and identify effective solutions LO7- Conduct user and business security requirements analysis LO8- Propose cybersecurity architectures based on stakeholder's needs and budget LO9- Select appropriate specifications, procedures and controls

	LO10- Build resilience against points of failure across the architecture LO11- Coordinate the integration of security solutions
Responsibility and Autonomy	LO12- Design and propose a secure architecture to implement the organisation's strategy LO13- Develop organisation's cybersecurity architecture to address security and privacy requirements LO14- Adapt to the evolving cyber threat landscape LO15- Produce architectural documentation and specifications LO16- Analyse and evaluate the cybersecurity of the organisation's architecture LO17- Assess the implemented architecture to maintain an appropriate level of security

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 course is held over 5 days.

Main Topic	Suggested Residential Working Hours + (Hours required for individual learning E-Learning etc)	Suggested Contents
1. Introduction to cybersecurity architecture	5 + (2)	• What is ▪ Cyber Security Architecture ▪ ISO/IEC 27001 ▪ Zero Trust framework ▪ Secure Development Lifecycle ▪ Cybersecurity controls ▪ Risk management
2. The 3 Phases of Cybersecurity Architecture	20 + (6)	• Develop Policies, Standards, and Best Practices • Implementation ▪ Building Blocks of Security ▪ Policies ▪ Procedures • Monitoring ▪ Changes ▪ Updates ▪ Implementation
3. Vulnerability assessment	30 + (6)	• Penetration Testing • Vulnerability Scanning

		• Manual Analysis
		• Risk Management
		  ▪ Identify
		  ▪ Assess
		  ▪ Mitigate
		  ▪ Monitor

TOTAL	**55 + (14)**	

<u>Material</u>

Required:

- AKU 104: Module 3 – Experience a security incident
- AKU 104: Module 5 – Introductions to Risk Management
- AKU 104: Module 6 – Conduct Risk Management
- AKU 104: Module 7 – Risk Treatment
- AKU 104: Module 8 – Review Organisational Controls
- AKU 104: Module 9 – Review Technical Controls
- AKU 104: Module 10 – IT Security Risk Management Methodology

Recommended:

- AKU 1 – History and Context of the CSDP
- 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)

<u>Methodology</u>

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

<u>Additional information</u>

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".