European Security and Defence College

European Security and Defence College
Doc: ESDC/2025/036
Date: 20 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	**Chief Information Security Officer (CISO)**	ECTS
Feb. 2027	***220***		**1**

Target audience	Aim
The participants should be mid-ranking to senior military or civilian officials dealing with cybersecurity management tasks 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, apply and manage the implementation of cybersecurity policies across the organisation. Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on the implementation of cybersecurity strategies in organisations by improving their knowledge, skills and competencies. By the end of this course, the participants will learn how to manage the implementation of cybersecurity policies across an organisation.

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 'Chief Information Security Officer' profile*

Learning Outcomes	
Knowledge	LO1- Describe cybersecurity policies LO2- Describe cybersecurity procedures LO3- Describe resource management LO4- Describe Risk management standards, methodologies and frameworks LO5- Describe a cyber-attack prevention plan
Skills	LO6- Implement cybersecurity policies, certifications, standards, methodologies and frameworks LO7- Review and enhance security documents, reports, SLAs and ensure the security objectives LO8- Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing

Responsibility and Autonomy	LO9- Establish a cybersecurity plan LO10- Supervise the application and improvement of the Information Security Management System (ISMS) LO11- Prepare and present cybersecurity vision, strategies and policies LO12- Communicate, coordinate and cooperate with internal and external stakeholder LO13- Manage continuous capacity building within the organisation

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 3 days.

Main Topic	Suggested Residential Working Hours + (Hours required for individual learning E-Learning etc)	Suggested Contents
1. Introduction to cybersecurity planning	4 + (1)	• Cybersecurity strategies, policies and procedures • Cybersecurity prevention plan • Business continuity
2. Risk management	7 + (4)	• Identify • Assess • Mitigate • Monitor
3. Implementation	8 + (4)	• Building Blocks of Security • Policies • Procedures
4. Recovery	7 + (3)	• Design a recovery plan • Apply recovery procedures • Organise recovery exercises
5. Business model	7 + (3)	• Business discussion on the evolving digital landscape • Implement and scale emerging technologies • Resource management • Tactical activities delegation
TOTAL	**33 + (15)**	

Material	Methodology
Required: • Seven Strategies for CISOs • Ten Tenets of CISO Success • CISO Success Strategies • Communicating to and Influencing • Cybersecurity Frameworks for CISOs • CEOs and Boards of Directors: What Works and What to Avoid **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)	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".