European Security and Defence College
Doc: ESDC/2024/044
Date: 21 February 2024
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number		ECTS
Feb. 2026	**205**	**Cybersecurity Risk Management**	**2**

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Support ECSF Role 10. Cybersecurity Risk Manager* • *Specialised cyber course, at technical and tactical 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	Aim
Participants should be technical experts (civilians or military personnel) who have to take roles in information security management, in particular those with technical responsibilities in IT and networking who need or plan to take information security management roles and responsibilities Open to: ▪ EU Member States / EU institutions, bodies and agencies ▪ Candidate countries	The overall aim of the Risk Management course is to • Build skills and abilities for the identification, analyses, assessment, estimation, mitigation of the cybersecurity-related risks of ICT infrastructures, systems and services by planning, applying, reporting and communicating risk analysis, assessment and treatment.

Learning Outcomes	
Knowledge	LO1– Recognise best practices and standards in information security management LO2- Identify the roles of key personnel for an efficient information security management system LO3- Recognise methodology and methods to conduct a risk analysis LO4- Define risk evaluation and treatment options LO5- Identify technical controls to reduce risk
Skills	LO6– Document information security management policy, linking it to organisation strategy LO7- Analyse organisation critical assets and identify threats and vulnerabilities LO8- Establish a risk management plan LO9- Design and document processes for risk analysis and management LO10- Apply mitigation and contingency actions

Responsibility and Autonomy	LO11 – Implement information security policies. LO12- Ensure that security risks are analysed and managed with respect to organisation information and processes.

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 4 days.

Main topic	Suggested working hours (required for individual learning)	Suggested content
1. Introduction to ISMS & Information Security Policies	8(4)	1.1 Introduction to Information Security 1.2 Experience of a Modern Attack & Incident Handling Activities 1.3 Introduction to Information Security Management Systems 1.4 Information Security Policies and Procedures 1.5 Information Security Roles & Responsibilities
2. Risk assessment and implementation	8(4)	2.1. Identification, analyses, assessment, estimation of risks 2.2. Risk management in practise 2.3. Continuous Measurement & Improvement of the ISMS
3. Risk Mitigation	8(4)	3.1 Risk Mitigations 3.2. Organisational, Physical and Technical Controls which support the prevention, detection or correction of risks
TOTAL	**24(12)**	

Materials

Required:
- AKU104: Risk Management and Implementation of an information security Management and ITSRM
- AKU 55 - Strategic Compass

Recommended:
- Council Conclusion on EU Policy on Cyber Defence (22.05.2023)
- EU Policy on Cyber Defence, JOIN(22) 49 final (10.11.2022)

Methodology

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

• 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)	mandatory. The materials proposed for supplementary (eLearning) study will reflect current developments in the field of cybersecurity 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".