

Curriculum

To be reviewed by Feb. 2024	Activity number 205	Information Security Management and ICT security	ECTS 2
---------------------------------------	-------------------------------	---	-----------------------------

<p style="text-align: center;"><u>Target audience</u></p> <p><i>Participants (30) should be technical experts (civilians or military personnel) that need to cover roles in information security management, in particular those who have technical responsibilities in IT and networking and need or plan to assume information security management roles and responsibilities</i></p> <p><u>Open to:</u></p> <ul style="list-style-type: none"> ▪ EU Member States / EU Institutions Bodies and Agencies 	<p style="text-align: center;"><u>Aim</u></p> <p style="text-align: center;">This course aims to:</p> <ul style="list-style-type: none"> • Reinforce technical knowledge in cybersecurity by identifying and implementing technical controls • Improve skills and abilities to implement and run an information security management system (ISMS), and manage a risk assessment program to identify necessary measures to protect information and ICT systems. • Provide guidelines and follow best practises in managing information security policies, analyse the critical assets and identify threats and vulnerabilities and help to develop business continuity plan.
---	--

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	<ul style="list-style-type: none"> • <i>Specialised cyber course, at technical and tactical levels</i> • <i>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)]</i>

Learning Outcomes	
Knowledge	L01- Recognise the best practices and standards in information security management L02- Identify the roles of key personnel for an efficient information security management system L03- Recognize methodology and methods to conduct a risk analysis L04- Define risk evaluation and treatment options L05- Identify technical controls to reduce risk L06- Identify business continuity and disaster recovery plans L07- Identify cyber-attack techniques and ICT security controls for prevention, detection and correction.
Skills	L08- Document the information security management policy, linking it to the organization strategy L09- Analyse the organisation critical assets and identify threats and vulnerabilities L010- Establish a risk management plan L011- Design and document the processes for risk analysis and management L012- Apply mitigation and contingency actions L013- Select and implement ICT security tools

	LO14- Propose ICT security improvements
Responsibility and Autonomy	LO15 – Implement information security policies. LO16- Ensure that security risks are analysed and managed with respect to organisation information and processes. LO17- Make recommendations for the design, implementation and evaluation of technical control

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 behaviour 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, 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 ISMS & Risk Management	16(6)	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 Roles & Responsibilities 1.5 Risk Assessment
2. Implementation of the ISMS & Introduction to Controls	16(6)	2.1 Information Security Policies and Procedures 2.2 Business Continuity Management 2.3 Information Security Management System Implementation 2.4 Continuous Measurement & Improvement of the ISMS 2.5 Related directives, standards 2.6 Introduction to Technical Controls
3. Selection & Implementation of ICT Security Controls	10	3.1 Establishing a Cyber Security Architecture 3.2 Cyber Security Protection Controls covering some technical areas: 3.3 Network Firewalls & Perimeter Security, Network Segmentation, Network Access Control (NAC), Intrusion Detection / Prevention Mechanisms, Web & Email Security Gateways, Secure Remote Access, Applied Cryptographic Controls, Application Whitelisting, Mobile Device Security, Cloud Security. 3.4 Technical Security Assessments (Penetration Testing, Vulnerability Assessment)

TOTAL	42	
--------------	-----------	--

<p style="text-align: center;"><u>Materials</u></p> <p>Required: ELearning on Risk Management and Implementation of an information security Management</p> <p>Recommended: Presentations Case studies and exercises</p>	<p style="text-align: center;"><u>Methodology</u></p> <p>The course is based on the following methodology: lectures, panels, workshops, exercises</p> <p style="text-align: center;"><u>Additional information</u></p> <p>Pre-course questionnaire on learning expectations and possible briefing topic form specific area of expertise may be used.</p> <p>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.</p> <p>The Chatham House Rule is applied during all residential phase 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".</p>
---	--