**European Security and Defence College**
**Doc: ESDC/2022/ 062**
**Date: 23 March 2022**
**Origin:** ESDC Secretariat

# Curriculum

| To be reviewed by | Activity number | **Information Security Management and ICT security** | ECTS **2** |
|---|---|---|---|
| **Feb. 2024** | **205** | | EAB.CYBER **N/A** |

| Target audience | Aim |
|---|---|
| *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*<br><br>Open to:<br>▪ EU Member States / EU Institutions Bodies and Agencies | This course aims to:<br>• Reinforce technical knowledge in cybersecurity by identifying and implementing technical controls<br>• 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.<br>• 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. |

## Learning Outcomes

The course corresponds to the strategic objectives of The EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020) 18 final] and the objectives of the CTG / MTG TRA

| | |
|---|---|
| Knowledge | L01– Recognise the best practices and standards in information security management<br>L02- Identify the roles of key personnel for an efficient information security management system<br>L03- Recognize methodology and methods to conduct a risk analysis<br>L04- Define risk evaluation and treatment options<br>L05- Identify technical controls to reduce risk<br>L06- Identify business continuity and disaster recovery plans<br>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<br>L09- Analyse the organisation critical assets and identify threats and vulnerabilities<br>L10- Establish a risk management plan<br>L11- Design and document the processes for risk analysis and management<br>L12- Apply mitigation and contingency actions<br>L13- Select and implement ICT security tools<br>L14- Propose ICT security improvements |

| | |
|---|---|
| Responsibility and Autonomy | L15 – Implement information security policies.<br>L16- Ensure that security risks are analysed and managed with respect to organisation information and processes.<br>L17- 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. It is a specialised course, at technical and tactical levels, link with the Pillars 1 and 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN(2020).*
*Furthermore the course gives an overview of the CFSP/CSDP and the related EU policies and concepts and focuses on the foundations of the CFSP/CSDP [preparatory eLearning phase)*

| 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<br>1.2 Experience of a Modern Attack & Incident Handling Activities<br>1.3 Introduction to Information Security Management Systems<br>1.4 Information Security Roles & Responsibilities<br>1.5 Risk Assessment |
| 2. Implementation of the ISMS & Introduction to Controls | 16(6) | 2.1 Information Security Policies and Procedures<br>2.2 Business Continuity Management<br>2.3 Information Security Management System Implementation<br>2.4 Continuous Measurement & Improvement of the ISMS<br>2.5 Related directives, standards<br>2.6 Introduction to Technical Controls |
| 3. Selection & Implementation of ICT Security Controls | 10 | 3.1 Establishing a Cyber Security Architecture<br>3.2 Cyber Security Protection Controls covering some technical areas:<br>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.<br>3.4 Technical Security Assessments (Penetration Testing, Vulnerability Assessment) |
| **TOTAL** | **42** | |

| Materials | Methodology |
| --- | --- |
| **Required:**<br>Elearning on Risk Management and Implementation of an information security Management<br><br>**Recommended:**<br>Presentations<br>Case studies and exercises | The course is based on the following methodology: lectures, panels, workshops, exercises<br><br>Additional information<br><br>The Chatham House Rule is applied during all residential modules of the HLC: "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".<br><br>The mandatory EU security clearance to "Confidential" level should be valid for the entire duration of the HLC and participants must prove that they have an EU clearance certificate before the start of the first residential module (September). |