European Security and Defence College
Doc: ESDC/2020/033
Date: 14 February 2020
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Course (*and module*)	ECTS
February 2022	*205*	**Information Security Management and ICT security**	**2**

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	This course aims to: • 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.

Learning outcomes***		
	Knowledge	Recognise the best practices and standards in information security management Identify the roles of key personnel for an efficient information security management system Recognize methodology and methods to conduct a risk analysis Define risk evaluation and treatment options Identify technical controls to reduce risk Identify business continuity and disaster recovery plans Identify cyber-attack techniques and ICT security controls for prevention, detection and correction.
	Skills	Document the information security management policy, linking it to the organization strategy Analyse the organisation critical assets and identify threats and vulnerabilities Establish a risk management plan Design and document the processes for risk analysis and management Apply mitigation and contingency actions Select and implement ICT security tools Propose ICT security improvements
	Competences	Implement information security policies. Ensure that security risks are analysed and managed with respect to organisation information and processes. Make recommendations for the design, implementation and evaluation of technical control

Prerequisite	English: Common European Framework of Reference for Languages (CEFR) Level B2 Intermediate knowledge and experience in IT or networking. Intermediate knowledge in some of these topics: Basic Information Security Controls, Cryptography concepts, Secure communications.

Evaluation and verification of learning outcomes****

- **Level 1 Observation and satisfaction**:
  Active observation by the course director and lead instructor, and feedback questionnaire filled by course participants at the end of each residential day.

However, no formal verification of learning outcomes is foreseen. The proposed ECTS is based on participants' workload only.

Course structure		
Main Topic	**Recommended Working Hours (of that eLearning)**	**Contents**
Introduction to ISMS & Risk Management	16(6)	- Introduction to Information Security - Experience of a Modern Attack & Incident Handling Activities - Introduction to Information Security Management Systems - Information Security Roles & Responsibilities - Risk Assessment
Implementation of the ISMS & Introduction to Controls	16(6)	- Information Security Policies and Procedures - Business Continuity Management - Information Security Management System Implementation - Continuous Measurement & Improvement of the ISMS - Related directives, standards - Introduction to Technical Controls
Selection & Implementation of ICT Security Controls	10	- Establishing a Cyber Security Architecture - Cyber Security Protection Controls covering some technical areas: - 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.

		- Technical Security Assessments (Penetration Testing, Vulnerability Assessment)
TOTAL	**42**	

Materials Elearning on Risk Management and Implementation of an information security Management Presentations Case studies and exercises	Additional information Elearning material which covers the knowledge mandatory Passing the elearning final test is mandatory to access the residential course. This course is organised in cooperation with ENISA

* Description of the number, level and background of the participants. Selection criteria are also described in case there is need to limit the participation. This is copied to the invitation to advice the nominators.

** The aim describes the reason why this training is organised.

*** Learning outcomes should contain action verbs and be performance-based, describing what the participant will be able to do at the end of the course. When writing learning objectives, it is better to avoid vague and generic words such as "know, understand, internalize and appreciate".

**** Learning outcomes are closely linked to learning evaluation questions before, during and after the course. Evaluation criteria can be developed by making use of speed, accuracy and quality. Sometimes the parameters or conditions might need to be detailed.