INVITATION & AGENDA

DATE 25 – 28 OCTOBER, 2022
LOCATION UNIVERSITY OF PUBLIC SERVICE - BUDAPEST

INFORMATION ABOUT THE COURSE

Under the auspices of the European Security and Defence College (ESDC), the University of Public Service (UPS) and the European Union Agency for Cybersecurity (ENISA) has the honour of organising a course dedicated to Information Security Management and ICT security.

As part of ESDC's Cyber ETEE platform, this course is offered to public employees from EU Member States and EU institutions that need to cover roles in information security management and in risk management.

The course is structured in 2 parts:

1. An asynchronous eLearning part, which provides an introduction to Information Security and Risk Management. This part is mandatory and requires 8 hours of self-study.
2. A classroom course which will be held from 25th to 28th October 2022. It will focus on the implementation of the Information Security Management and on applying controls to minimize risks.

The overall objective of this course is to:

- Gain significant knowledge in implementing an Information Security Management System (ISMS);
- Reinforce technical knowledge in cybersecurity by identifying and implementing technical controls;
- Improve skills and abilities to manage a risk assessment program and identify necessary measures to protect information and ICT systems;
- Provide guidelines and follow best practises in managing information security policies, analysing critical assets, identifying threats and vulnerabilities.

At the end of the course, trainees will be able to participate in risk management tasks, to properly address security risks, and to develop and implement information security policies. They will also have the capability to establish action plans for securing information systems within an organization.

The course is offered free of charge. Applications are to be filled out by the national ENLIST nominators via the ESDC secure registration system (https://esdc.europa.eu/enlist/login) **no later than 27 September 2022** and the participants will receive a confirmation email with a unique link to join the course. A list of relevant ENLIST nominators can be retrieved from the ESDC website at https://esdc.europa.eu/nominators/.

For more information about the classroom course and its structure, please contact the Course director, Csaba Krasznay, Director, Institute of Cybersecurity, University of Public Service.

For more information about the elearning material, please contact Fabio Di Franco, Cybersecurity Officer, ENISA.
Fabio.DiFranco@enisa.europa.eu

ASYNCHRONOUS ELEARNING

The e-learning module consists of 10 sub-modules. These are organized as a story that follows an employee who assumes a new role in the Information Security Department of his organization. He is tasked with undertaking a risk analysis within the organization. The 9 sub-modules represent the steps that the employee has to take to accomplish his mission. A 10th sub-module is focused on a specific methodology that is adopted by the European Commission, namely the "IT Security Risk Management Methodology – ITSRM". These modules are presented in the Table below.

E-LEARNING SUB MODULES	TOPICS
1. Understand the Organization	Colleagues with key roles and responsibilities.
2. Learn about Information Security	Information Security Definitions and Terms Best Practices Legal and Regulatory requirements.
3. Experience a security incident	Follow the established incident handling procedure starting from reporting to incident analysis and communication.
4. Understand the Security Organization	Get to know the Organizational Structure, Roles and Responsibilities and the Organization's RASCI model.
5. Introduction to Risk Management	Learn about the Organization's Risk Management process (assets identification, threats and vulnerabilities assessment, risk treatment).
6. Conduct Risk Assessment	Interview key personnel to identify assets, existing security controls, threats, vulnerabilities and the associated risks.
7. Risk Treatment	Make a decision about risk treatment and establish an action plan for risk reduction.
8. Review Organizational Controls	Revise security policies and deploy a targeted awareness program.
9. Review Technical Controls	Audit technical controls and enhance protection with additional technical measures.
10. Understand the use of the ITSRM methodology	Conduct an IT security risk management using the method developed by EC.

At the end of the asynchronous eLearning, the trainee must go through a short assessment and complete it successfully in order to be admitted to the classroom course.

CLASSROOM COURSE

The classroom course will be held at the University of Public University -2 Ludovika tér, H-1083 Budapest - from the 25th to 28th October 2022. The course will follow a blending approach, mixing online lectures and exercise, and so facilitate achieving the learning objectives.
The scheduled activities and the related topics are indicated below.

UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

ETCE CYBER PLATFORM
ESDC ESD

enisa

DAY 1: TUESDAY, 25 OCTOBER 2022

8.30 – 9.30	Introduction to the course and Ice breaking session

9.30 - 16.30	Lectures and exercise on
	• Introduction to Information Security Management System (ISMS)
	• Information Security Roles & Responsibilities
	• Introduction to Risk Assessment
	  ○ Identification of Threats & Vulnerabilities
	  ○ Scope definition
	  ○ Assets Identification & Classification
	  ○ Risk Identification & Assessment)
	  ○ Risk Evaluation
	  ○ Risk Acceptance & Treatment
	  ○ Risk monitoring

DAY 2: WEDNESDAY, 26 OCTOBER 2022

8.30 – 16.30	Further explanation on Risk Assessment
	  ○ Identification of Threats & Vulnerabilities
	  ○ Scope definition
	  ○ Assets Identification & Classification
	  ○ Risk Identification & Assessment)
	  ○ Risk Evaluation
	  ○ Risk Acceptance & Treatment
	  ○ Risk monitoring

DAY 3: THURSDAY, 27 OCTOBER 2022

8.30 – 16.30	• Introduction to Technical Security controls
	  ○ Network Security Controls
	  ○ System Security Controls
	  ○ Data Security Controls
	  ○ User Access Controls
	  ○ Security Monitoring
	  ○ Technical Security Assessments
	• Information Security Policies & Procedures
	• Business Continuity Management System
	• Information Security Management System Implementation
	• Compliance and Security Audits

DAY 4: FRIDAY, 28 OCTOBER 2022

8.30 - 12.00	• Recap of the activities done in the previous days and conclusion remarks

During the first 3 days of the course, the following breaks are scheduled:

- 2 coffee breaks of 15 minutes (one in the morning and one in the afternoon)
- a lunch break of 1 hour

LEARNING OUTCOMES & TARGET AUDIENCE

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's 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 controls

This main target profile of this course according to European Cybersecurity Skills Framework (ESCF)[1] is the Risk Manager. Chief Information Security Officer, Cybersecurity Architect, Cybersecurity Auditor can also benefit from this course.

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework