INVITATION

DATE   12 – 13 SEPTEMBER, 2019
LOCATION ENISA HERAKLION OFFICE, NIKOLAOU PLASTIRA 95- VASSILIKA VOUTON, 700 13 HERAKLION, GREECE

Under the auspices of the European Security and Defence College (ESDC), ENISA has the great honour of organising a blended course dedicated to Information Security and Risk Management.

As part of ESDC's Cyber ETEE platform, this course offers a training to public employees from EU Member States and EU institutions 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.

The course will be held in English and can accommodate 30 participants.

The course is scheduled **in 2 parts**:

- An asynchronous eLearning part which provides an introduction to Information Security and Risk Management. This part is mandatory and requires self-study for 6-8 hours.
- A two-day residential course which will be held in ENISA Heraklion office on the 12th and 13th September 2019 and 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

- Reinforce knowledge in cybersecurity
- 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 IT 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.

At the end of the course, trainees will be able to develop and implement information security policies, to ensure that security risks are properly analysed and have the capability to establish action plans for securing information systems within an organization.

For more information about the the content of the course, please contact Dr. Fabio Di Franco - Fabio.difranco@enisa.europa.eu

PILOT ACTIVITY UNDER THE CYBER ETEE PLATFORM

TRAINING IN INFORMATION SECURITY MANAGEMENT

The **nomination of the suitable candidates for attending the course** should be done via the ENLIST registration system of the ESDC by the designated EU ENLIST Nominators. A list with relevant ENLIST nominators can be retrieved from the ESDC website at https://esdc.europa.eu/nominators/.

Deadline for registration is **22 Aug 2019** and will not be final until confirmed by the ESDC Secretariat.

The course is offered for free but the expense of the mission must be covered by the participants.

AGENDA OF THE RESIDENTIAL COURSE

DAY 1: 12TH SEPTEMBER 2019	
8.30	Meeting at Eleftherias square (in front if El. Venizelos statue) - Heraklion
8.40	Bus leaves from Eleftherias square
9.00	Registration
9.20 -18.00	Implementation of the **Information Security Management System** will be analysed through: • Information Security Strategy Objectives and Roadmap • Risk Management • Roles and Responsibilities • ISMS Documentation Requirements • Information Security Policies and Procedures • Continuous Measurement & Improvement of the ISMS
18.15	Bus leave for the restaurant (or on request to Eleftherias square –Heraklion)
19.30	Networking Dinner in Heraklion city centre

DAY 2: 13TH SEPTEMBER 2019	
8.30	Meeting at Eleftherias square (in front if El. Venizelos statue) - Heraklion
8.40	Bus leaves from Eleftherias square
9.15 -17.45	**Selection & Implementation of Technical Security Controls** Establishing a Cyber Security Architecture • Cyber Security Protection Controls covering the following 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 • Technical Security Assessments (Penetration Testing, Vulnerability Assessment) • Continuous Measurement & Improvement of the ISMS
18.00	Bus to Eleftherias square –Heraklion (or on request to Heraklion airport)

Lunches and coffees will be provided during the 2 days.

Shuttle bus will be provided both days from Eleftherias square. **Meeting both days at 8.30am in front if El. Venizelos statue.**

TOPICS COVERED IN THE MANDATORY ASYNCHRONOUS E-LEARNING

TRAINING IN INFORMATION SECURITY MANAGEMENT

Introduction to ISMS & Risk Management (6-8 hours)

- Introduction to Information Security
- Experience of a Modern Attack & Incident Handling Activities
- Introduction to Information Security Management Systems
- Risk Management
- Organizational Controls
- Technical Controls

Access to the elearning will be given immediately after the confirmation by the ESDC Secretariat.

MEET THE TEAM

Lectures, Tabletop Exercises and Case Studies – combined approach to facilitate the understanding and the practising of the above topics- will be taught and moderated by:

- Dr. Fabio Di Franco – ENISA
- Mr. Kostas Papadatos -Cybernoesis
- Prof. Kostantinos Rantos – International Hellenic University
- Mr. Evangelos Rekleitis – ENISA.

PILOT ACTIVITY UNDER THE CYBER ETEE PLATFORM

TRAINING IN INFORMATION SECURITY MANAGEMENT

enisa

LEARNING OUTCOMES & PREREQUISITE

Knowledge	K1 the best practices and standards in information security management K2 the roles of key personnel for an efficient information security management system K3 security management policy and its implications for engagement with customers, suppliers and subcontractors K4 the methodology to conduct a risk analysis considering organization values and interests K5 risk evaluation and treatment options K6 technical controls to reduce risk K7 business continuity and disaster recovery plans K8 cyber-attack techniques and counter measures for avoidance
Skills	S1 document the information security management policy, linking it to business strategy S2 analyse the organization critical assets and identify threats and vulnerabilities S3 establish a risk management plan to identify required preventative actions S4 communicate and promote the risk analysis outcomes and risk management processes S5 design and document the processes for risk analysis and management S6 apply mitigation and contingency actions S7 establish a business continuity plan

Prerequisite	English: Common European Framework of Reference for Languages (CEFR) Level B2 Intermediate knowledge and experience in IT or networking.

EUROPEAN UNION AGENCY FOR CYBERSECURITY