Invitation to the

CYBERSECURITY RISK MANAGEMENT

(ESDC Activity Number 24-25/205/1)

Budapest, Hungary, 14–17 October 2024

Annex A

Course administrative instructions

- **Target audience:** As part of ESDC's Cyber ETEE platform, this course is offered to public employees from EU Member States and EU institutions and also from the Candidate Countries who need to cover roles in information security management and in risk management.
- **Seats and nominations:** A maximum of 28 participants.
- **Application and deadline**: **The course is offered free of charge**. Applications should be submitted by designated nominators using the ESDC ENLIST Platform https://esdc.europa.eu/enlist/login, no later than 16 September 2024. A list with the relevant ENLIST nominators can be retrieved from the ESDC website at https://esdc.europa.eu/nominators/. **Late registration:** Subject to availability of seats, the course is open for late registration. Please contact the course administration: Ms Anna MALEC (ESDC Training Manager, Anna.MALEC@eeas.europa.eu) or the Course Directors, Ms Dora MOLNAR (Molnar.Dora@uni-nke.hu) or Goce STEVANOSKI (goce.stevanoski@ugd.edu.mk).
- **Registration will not be final until confirmed by the ESDC Secretariat**. Please do not book flights and accommodation before receiving confirmation.
- **Selection of participants** will be based on applicant backgrounds, experience, suitability, gender balance and country of origin. The decision on which applications are accepted remains solely with the Training Institutions and the ESDC Secretariat. When the participant list is finalised, the course administration will contact the selected participants and provide more detailed information about the course and logistics.
- **Mandatory e-learning and attendance**: The course consists of an e-learning preparatory phase, (online) to be completed using the ESDC e-Learning platform ILIAS, and a residential activity in Budapest (Hungary); both parts are compulsory. For the first part (i.e. the online modules), the ESDC will provide the relevant links to the selected participants. Participants must complete these online e-learning modules before the start of the residential part. The participants' attendance during the residential course in Budapest is mandatory on all days. A certificate will be awarded, on the last day, to those course participants who have completed both the e-learning phase and the residential course.
- **Course venue (location)**: The course will be held mainly in the premises of the Hungarian Ludovika University of Public Service (2 Ludovika tér, H-1083 Budapest).
- **Language**: The working language is English, without translation.

- **Course (tuition) fees**: The course has no registration or tuition fees.
- **Travel expenses, transfers, accommodation, meals and catering:** Participants should arrange their own travel and accommodation. All costs for travelling to/from Hungary, accommodation, catering and meals (including breakfast), daily allowances, transfers and local transport must be covered by the participants or by their sending authorities.

  Hotel reservations: There are numerous hotels in the Budapest area, and participants are responsible for their own arrangements.

  Participants should not make booking arrangements before receiving the confirmatory message on their complete course registration.
- **Liabilities, medical and life insurance**: In the event of medical emergencies or accidents, the costs will be covered directly by the health, life and accident insurance provided by the participants' sending countries, national authorities or organisations. The organiser does not provide health, life or accident insurance for participants at the event or during their stay in Hungary.
- **Dress code:** As far as the dress code is concerned, we recommend that participants wear business attire (or a dress) for the opening event and closing ceremony. Members of the armed forces, gendarmerie and police are not required to wear their uniforms. During the course, a networking social dinner will be offered to all course participants, experts and trainers. For this specific event, as well as course classes and field visits, comfortable business/smart casual attire will be appropriate.
- **Arrival/Departure**: Participants are invited to arrive in Budapest on Sunday 13 October 2024 or Monday early morning. The course will start around 12:30 on Monday 10 October 2024 and will finish around 13:00 on Thursday 17 October 2024.
- **Diversity and inclusion:** The ESDC is committed to an inclusive, gender-sensitive and discrimination-free environment. We do not and will not discriminate on the basis of race, colour, religion, gender, gender expression, age, national origin, disability, marital status, or sexual orientation in any of our activities or operations. Only in an inclusive environment can all people, and therefore the ESDC and its partners, realise their true potential. We therefore particularly encourage applicants from groups likely to be underrepresented to apply. The ESDC and the Training Institutions will not tolerate any conduct that violates these values.
- The final course agenda will be distributed to all selected participants. Nevertheless, for matters regarding the course programme and planned activities, please do not hesitate to contact the Course Director, Dóra MOLNÁR.
- **Additional information**: *Cybersecurity Risk Management (14-17 October)* Versus *Cyber Threat Management (7-10 October).* Both training activities are organised by LUPS under the auspices of the ESDC. These are two different training offers.

For more information about the classroom course and its structure, please contact the course directors, Dóra Molnár (Vice-Director, Institute of Cybersecurity, Ludovika University of Public Service, molnar.dora@uni-nke.hu) and Anna Molnár (Head of International Security Policy Department, molnar.anna@uni-nke.hu).

For more information about the e-learning material, please contact Fabio Di Franco, Cybersecurity Officer, ENISA (Fabio.DiFranco@enisa.europa.eu)

.

Invitation to the

CYBERSECURITY RISK MANAGEMENT

(ESDC Activity Number 24-25/205/1)

Budapest, Hungary, 14–17 October 2024

Annex B

Tentative course agenda

The course is structured in two parts:

PART I: AN ASYNCHRONOUS SELF- LEARNING PART, which introduces information security and risk management. This part is mandatory and requires 8 hours of self-study.

The e-learning module consists of 10 sub-modules. These are organised as a story that follows an employee who takes on a new role in the Information Security Department of his organisation. He is tasked with undertaking a risk analysis within the organisation. The 9 sub-modules represent the steps that the employee has to take to accomplish his mission. A 10th sub-module focuses 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 Organisation	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, from reporting to incident analysis and communication.
4. Understand the Security Organisation	Get to know the organisational structure, roles and responsibilities and the organisation's RASCI model.
5. Introduction to Risk Management	Learn about the organisation'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 associated risks.
7. Risk Treatment	Make a decision about risk treatment and establish an action plan for risk reduction.
8. Review Organisational controls	Revise security policies and deploy a targeted awareness programme.
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.

PART II: A CLASSROOM COURSE, which will be held at the Ludovika University of Public Service (2 Ludovika Tér, H-1083 Budapest) from 10 to 17 October 2024. The course will take a blending approach, mixing online lectures and exercises, and so facilitate achieving the Learning Objectives. The scheduled activities and related topics are indicated below in the table:

Time	**Day 1 (14 October 2024)** Location: John Lukacs hall (Side Building)
13:00 - 13:30	**Opening ceremony** Dr. László Kovács, Vice-Rector for Academic Affairs (LUPS) Andreja Mihailovic (University of Montenegro) Goce Stevanoski (Military Academy 'General Mihailo Apostolski')
13:30 – 15.00	**Introduction to information security and ISMSs** Lecturer: Dimitar Bogatinov (Military Academy 'General Mihailo Apostolski')
15:00 – 15:15	**Coffee break**
15:15 – 16.45	**Information security roles and responsibilities** Lecturer: Goce Stevanoski (Military Academy 'General Mihailo Apostolski')

Time	**Day 2 (15 October 2024)** Location: Room A-B (College Building)
08:30 – 10:00	**Information security policies and procedures** Lecturer: Dr Péter Kohári (Hungarian Development Bank)
10:00 – 10:15	**Coffee break**
10:15 – 11:45	**Organisational, Physical and Technical Controls supporting the PreDeCo of risks** Lecturer: Csaba Krasznay (LUPS)
12:00 – 13:00	**Lunch**
13:00 – 14:30	**Supply chain attacks and security measures** Lecturer: Fabio Di Franco (ENISA) and Arne Roar Nygård (Elvia, Norway)
14:30 – 14:45	**Coffee break**
14:45 – 16:15	**NIS 2 scope and NIS 2 measures** Lecturer: Arne Roar Nygård (Elvia, Norway)
17.00 – 19.00	**Guided tour of Castle of Buda** Ibolya Horváthné Szalóczy

Time	**Day 3 (16 October 2024)** Location: Computer lab (Education Building)
08:30 – 10:00	**Identification, analyses, assessment and estimation of risks I** Lecturer: Sándor Magyar (LUPS)
10:00 – 10:15	**Coffee break**
10:15 – 11:45	**Identification, analyses, assessment and estimation of risks II** Lecturer: Sándor Magyar (LUPS)
12:00 – 13:00	**Lunch**
13:00 – 13:30	**Visit of the Ludovika Museum**
13:30 – 15:00	**Risk management is practice** Lecturer: András Szabó (LUPS)
15:15 – 15:30	**Coffee break**
15:30 – 17:00	**Continuous measurement and improvement of ISMSs** Lecturer: András Szabó (LUPS)

Time	**Day 4 (17 October 2024)** Location: John Lukacs hall (Side Building)
08:30 – 10:00	**Cybersecurity ecosystem in the Western Balkans** Lecturer: Andreja Mihailovic (University of Montenegro)
10:00 – 10:15	**Coffee break**
10:15 – 11:45	**Case studies in the Western Balkans** Lecturer: Andreja Mihailovic (University of Montenegro)
12:00 – 12:30	**Certificate ceremony - closing remarks**
12:30 – 13:30	**Lunch**

LEARNING OUTCOMES:	
Knowledge	Recognise best practices and standards in information security management.
	Identify the roles of key personnel for an efficient information security management system.
	Recognise methodology and methods for conducting 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 organisation 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 design and implementation.

The main target profile for this course according to European Cybersecurity Skills Framework (ESCF) is the Risk Manager.

Chief Information Security Officer, Cybersecurity Architect, Cybersecurity Auditor can also benefit from this course.