European Security and Defence College Doc: ESDC/2022/ 068
Date: 23 March 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2024**	Activity number **214**	**Course on Data Governance**	ECTS **1**
			EAB.CYBER **N/A**

Target audience

Participants should be mid-ranking to senior officials employed in the field of cyber security from MS, EU Institutions Bodies and Agencies.

Course participants must be available for the duration of the course. Participants are expected, through their experience and expertise, to actively engage and participate during the course.

Open to:

- EU Member States / EU Institutions Bodies and Agencies

Aim

This course presents the mechanism for effective Data Governance and outlines the seven critical factors for effective Strategy Execution: strategy, shared values, structure, systems, style, staff and skills.

Furthermore, this course will allow the mid-ranking to senior officials to exchange their views and share best practices on data governance linked with cyber-related topics, hence improving their knowledge, skills and competencies.

By the end of this course, the participants will be able to create and implement a Data Governance Strategy drawing on their enhanced knowledge and understanding of the relevant principles.

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 - Define the basic principles of data governance. L02 - List the seven critical factors for an effective Strategy Execution on data: strategy, shared values, structure, systems, style, staff and skills. L03 - Identify the roles of an organization involved in the planning, development, implementation, monitor and evaluation of the data governance related to cyber security within International Law. L04 - Identify the nature of the different cyber threats affecting data governance.
Skills	L05 - Classify the cyber incidents affecting data governance. L06 - Classify the impact of the cyber threats in data governance. L07 - Categorize the impact of cyber incidents affecting an organization’s data governance.
Responsibility and Autonomy	L08 - Evaluate the potential impacts of cyber threats to an organization’s data governance. L09 - Select the appropriate mitigation measures to protect data governance within an organization.

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 non-specialised course, at awareness level, link with the Pillar 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. Applicable policies, standards, guidelines in data governance	4(2)	1.1 Presentation and analysis of the applicable EU policies in data governance and cyber 1.2 Presentation and analysis of the applicable standards and guidelines in data governance and cyber
2. The seven critical factors for effective Strategy Execution	9 (4)	2.1 Strategy 2.1.1 Development of Strategy 2.1.2 Key Fundamentals of Strategy 2.2 Systems 2.2.1 Defense Planning 2.2.2 Security Contingency Planning 2.2.3 Education and Awareness 2.2.4 Blended Learning 2.3 Structure 2.3.1 Internal environment 2.3.2 External environment 2.4 Skills 2.5 Style 2.6 Staff description 2.7 Shared values
3. The hybrid threats on data governance	5(2)	3.1 The conceptual framework on hybrid threats and the interaction with data governance
4. Best Practices of data governance in the cyber space	11	4.1 Effective controls on data governance 4.2 Application and practice on data governance to protect the assets of an organization from cyber threats 4.3 Related case studies on data governance and cyber
TOTAL	**29(8)**	

Materials Required:

- AKU1- History and Context of ESDP/CSDP development, AKU2- The European Global Strategy (EGS), AKU3- Role of EU institutions in the field of CFSP/CSDP, AKU4- CSDP crisis management structures and the Chain of Command, AKU5- Civilian and military capability development, AKU6- CSDP Decision Shaping/Making, AKU107- Awareness course on Cyber Diplomacy

Recommended:

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016)
- The EU Cybersecurity Act (June 2019)
- The EU's Cybersecurity Strategy for the Digital Decade (December 2020)

Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises

Additional information

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".

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).