European Security and Defence College
Doc: ESDC/2022/297
Date: 18 November 2022
Origin: ESDC Secretariat

Curriculum

To be reviewed by **Feb. 2025**	Activity number **214**	**Course on Data Governance**	ECTS **1**

Target audience	Aim
Participants should be mid-ranking to senior officials employed in the field of cybersecurity from MS or EU institutions, bodies and agencies. *Course participants must be available for the duration of the course. Participants are expected, based on their experience and expertise, to actively engage and participate during the course.*	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 mid-ranking to senior officials to exchange their views and share best practices on data governance in connection with cyber-related topics, thus improving their knowledge, skills and competencies. By the end of this course, participants will be able to create and implement a data governance strategy, drawing on their enhanced knowledge and understanding of the relevant principles.
Open to: ▪ EU Member States and EU institutions	

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Non-specialised cyber course, at awareness level* • *Linked with the strategic objectives of Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning outcomes

Knowledge	LO01 - Define the basic principles of data governance. LO02 - List the seven critical factors for effective strategy execution on data: strategy, shared values, structure, systems, style, staff and skills. LO03 - Identify the roles of an organisation involved in the planning, development, implementation, monitoring and evaluation of data governance related to cybersecurity under international law. LO04 - Identify the nature of the various cyber threats affecting data governance.
Skills	LO05 - Classify cyber incidents affecting data governance. LO06 - Classify the impact of the cyber threats in data governance. LO07 - Categorise the impact of cyber incidents affecting an organisation's data governance.
Responsibility and Autonomy	LO08 - Evaluate the potential impacts of cyber threats on an organisation's data governance. LO09 - Select the appropriate mitigation measures to protect data governance within an organisation.

Evaluation and verification of learning outcomes

The course is evaluated in accordance with the Kirkpatrick model, with level 1 evaluation (based on participants' satisfaction with the course).

In order to complete the course, participants have to accomplish all learning objectives, which are evaluated based on their active contribution to the residential module, including syndicate sessions and practical activities, as well as on the 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. There is active observation by the course director/lead instructor and a feedback questionnaire is filled in by participants at the end of the course.

However, no formal verification of learning outcomes is planned; the proposed ECTS is based on participants' workload only.

Course structure

The residential module is held over three days.

Main topic	Suggested working hours (required for individual learning)	Suggested content
1. Applicable policies, standards and 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 Defence 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 to 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 of data governance to protect the assets of an organisation 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

Pre-course questionnaire on learning expectations and possible briefing topic from the specific area of expertise may be used.

All course participants have to prepare for the residential module by going through the relevant eLearning preparatory phase, which is mandatory. The materials proposed for supplementary (eLearning) study will reflect current developments in the field of cybersecurity/cyber-defence in general and EU policies in particular.

The Chatham House rule is applied during the residential phase of the course: "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".