European Security and Defence College

European Security and Defence College
Doc: ESDC/2025/030
Date: 20 February 2025
Origin: ESDC Secretariat

Curriculum

To be reviewed by	Activity number	Data Governance	ECTS
February 2027	**214**		**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.* Open to: ▪ EU Member States and EU institutions	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.

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, both internal and external affecting data governance. LO05 – Identify Technical, organisational and operational controls to mitigate risks
Skills	LO06 - Classify cyber incidents affecting data governance. LO07 - Classify the impact of the cyber threats in data governance. LO08 - Categorise the impact of cyber incidents affecting an organisation's data governance.
Responsibility and Autonomy	LO09 - Evaluate the potential impacts of cyber threats on an organisation's data governance. LO10 - Select the appropriate mitigation measures to protect data governance within an organisation.

Evaluation and verification of learning outcomes

The course is evaluated according to the Kirkpatrick model, particularly 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 feedback is given in the level 1 evaluation of the residential modules.

In order to complete the course, participants have to fulfil all the learning objectives, and are evaluated on the basis of their active contribution to the residential modules, including their teamwork sessions and practical activities, and on their completion of the eLearning phases. Course participants must complete the autonomous knowledge units (AKUs) and pass the tests (mandatory), scoring at least 80% in the incorporated test/quiz. However, no formal verification of the learning outcomes is provided for; the proposed ECTS is based solely on participants' coursework.

The Executive Academic Board takes these factors into account when considering whether to award 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 course is held over 3 days.

Main topic	Suggested Residential Working Hours + (Hours required for individual learning E-Learning etc)	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, cyber, and AI 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 framework and controls on data governance and AI, including GDPR, NIS2 and ISO27001 4.2 Application and practice of data governance to protect the assets of an organisation from cyber threats (data loss/leakage prevention measures and controls; data security / data retention / data recovery - controls and measures standards (EU policies, ISO/IEC 38500, COBIT) 4.3 Related case studies on data governance, cyber and AI
TOTAL	**29 + (8)**	

Materials required:

- AKU 1 - History and context of the CSDP
- AKU 104B Information Security Management and ICT Security
- AKU 2 - The European Global Strategy (EUGS)
- AKU4- CSDP crisis management structures and the chain of command
- AKU6- CSDP decision shaping/making
- AKU107- Awareness course on cyber diplomacy
- AKU 108 The Cyber Defence Policy Framework (CDPF)

Recommended:

- AKU3- Role of EU institutions in the field of CFSP/CSDP
- AKU5- Civilian and military capability development
- 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 (NIS Directive)
- 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)
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union (NIS 2)
- Council Conclusion on EU Policy on Cyber Defence (22.05.2023)
- 024/1689 REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act

Methodology

The course is based on the following methodology: lectures, panels, workshops, exercises and/or case studies

Additional information

Pre-course questionnaire on learning expectations and possible briefing topic form 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. Course participants must be willing to contribute with their specific expertise and experience throughout the course.

The Chatham House Rule is applied during all residential modules 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".

The Chatham House Rule is applied during all residential modules 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".