Curriculum

To be reviewed by **Feb. 2024**	Activity number **204**	**Cybersecurity Organisational, Defensive Capabilities**	ECTS **1**

Target audience	Aim
Participants should be mid-ranking to senior officials dealing with technical and tactical aspects in the field of cyber security and cyber defence from EU MSs, relevant EU Institutions and Agencies. They should have a clear background related to the technical and tactical aspects of cyber security. Course participants must be available during the entire course and should be ready participate with their specific field of expertise and experience.. Open to: • EU Member States / EU Institutions Bodies and Agencies	This course will cover topics related to capabilities that need to be developed, implemented and provided by a Computer Security Incident Response Team. Furthermore, this course will allow cyber security experts to exchange their views and share best practices on cyber-related topics by improving their knowledge, skills and competencies. By the end of this course the participants will be able to assess the potential impacts and incidents on cyber policies and systems and determine cyber countermeasures on cyber policies and systems.

CORRELATION WITH CTG / MTG TRAs	EQUIVALENCES
CTG / MTG TRA on Cyber	• *Specialised cyber course, at technical and tactical levels* • *Linked with the strategic objectives of Pillar 1 and Pillar 2 of the EU's Cybersecurity Strategy for the Digital Decade [16.12.2020 JOIN (2020)]*

Learning Outcomes	
Knowledge	LO1— Identify the EU institutions and Agencies involved in cyber security, cyber defence and their respective roles LO2 - Identify the challenges of cyber security at a European level LO3 - Recognise the extensive nature of the information society we live in LO4 - Recognise the nature of the different cyber threats we are experiencing LO5 - Define the basic notions and concepts related to cyber security and cyber defence LO6 - Reflect on different trends among cyber threats LO7 - Identify concepts related to hybrid threats on cyber LO8 - Identify different trends of hybrid threats related to cyber security LO9 - Discern the challenges of industrial and public planning needed to face cyber threats LO10 - Identify the best practices and standards in information security management

Skills	LO11 – Analyse information related to Cyber Threat Intelligence and Information Gathering
	LO12- Analyse security incidents
	LO13- Classify the technical as well as organisational tools related to cyber security
	LO14- Classify the potential impacts of cyber threats in public policies
	LO15- Classify the potential impacts of cyber security on public policies
	LO16- Classify the critical risks for information security management
	LO17- Use of security detection and preventing techniques
	LO18- Apply concepts and techniques related to malware, forensic analysis and risk management
Responsibility and Autonomy	LO19 – Assess the potential impact of cyber threats on cyber policies and systems
	LO20 - Assess the potential impact of cyber incidents on cyber policies and systems
	LO21 - Determine cyber countermeasures on cyber policies and systems

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.

Main Topic	Suggested Working Hours (required for individual learning)	Suggested Contents

1. Risk Management	8(4)	1.1 Risk management process, Roles, responsibilities
		1.2 Risk identification, assessment, and response
		    1.2.1 Relevant definitions, Risk assessment process and steps
		    1.2.2 Risk register and assessment tables
		    1.2.3 Assessing risk, recording results in the risk register; different assessment approaches
		    1.2.4 Risk response strategies, developing risk response plans and actions
		    1.2.5 Examples of "actionable" risk responses
		1.3 Risk Monitoring
		    1.3.1 Tracking and reporting risks
		    1.3.2 Monitoring existing risks and execution of risk response plans and actions
		    1.3.3 Business impact analysis (BIA)

2. Cyber Threat Intelligence	8	2.1	Identification of cyber threat actors
		2.2	Analysis of the cyber threats
		2.3	Threat assessment and Hybrid threats
		2.4	Threat Intelligence Tools
		2.5	Incident handling and Threat Intelligence
3. Malware Analysis	5	3.1	Methodology on malware analysis, types, techniques and best practices
		3.2	Incident response on malware
4. Forensic Analysis	6	4.1	Methodology on forensic analysis, types, techniques and best practices
		4.2	Incident response on forensic analysis
TOTAL	**26(8)**		

Materials	Methodology
Required: AKU 2 on European Global Strategy, AKU106- Hybrid modules	The course is based on the following methodology: lectures, panels, workshops, exercises, labs
Recommended: • AKU104- 10 modules from ENISA • Council conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (November 2016) • European Parliament: Directive on security of network and information systems by the European Parliament (2016)	**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 supplemental (eLearning) study will reflect current developments in the field of cyber security/cyber defence in general and EU policies in particular. The Chatham House Rule is applied during all 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".