EUROPEAN UNIVERSITY

Co-funded by the European Union

EUROPEAN UNIVERSITY FOR CUSTOMISED EDUCATION

STUDY GUIDE

FORENSICS AND COMPLIANCE AUDITING CYBERSECURITY 26-27 S2

Organised by

Polytechnic Institute of Viseu

Brandenburg University of Technology Cottbus - Senftenberg · Universidad de Cantabria · Università di Catania · Université Polytechnique Hauts-de-France · UMONS University of Mons · University of the Peloponnese · Vaasan yliopisto University of Vaasa · Politécnico de Viseu

1. IDENTIFYING DATA.	
· Course Name.	*Forensics and Compliance Auditing Cybersecurity 26-27 S2*
· Coordinating University.	*Polytechnic Institute of Viseu*
· Partner Universities Involved.	
· Course Field(s).	*Cybersecurity*
· Related Study Programme.	
· ISCED Code.	*0612*
· SDG.	*Goal 9: Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation*
· Study Level.	*M (Master)*
· EUNICE Key Competencies	• Green – strongly • Orange - moderately • Red – partially • Blank cell - not at all

Problem solving	
Teamworking	
Communication	
Self-management	
Cognitive flexibility	
Digital competence	
Technical competence	
Global intercultural competence	

· Number of ECTS credits allocated.	3
· Mode of Delivery.	Online self-study

· Language of Instruction.	*English*
· Course Dates.	*12/03/2027 – 30/06/2027*
· Precise Schedule of the Lectures.	*Duration: 75 hours total, comprising 15 hours of asynchronous lectures, 5 hours of synchronous lectures, and 55 hours of autonomous work.* *Asynchronous lectures can be reviewed at any time.*
· Key Words.	*Forensics, Compliance, Auditing, Cybersecurity*
· Catchy Phrase.	*The course provides the foundations on forensics and compliance auditing to identify and extract evidence and non-compliant events to be reported.*

· Prerequisites and co-requisites.	*B2 English level*
· Number of EUNICE students that can attend the Course.	20
Number of EUNICE students that can attend the course per institution	2
· Course inscription procedure(s).	*Eunice Application Portal*

2. CONTACT DETAILS.	
· Department.	*School of Technology and Management of Viseu, Department of Informatics*
· Name of Lecturer.	*João Pedro Menoita Henriques*
· E-mail.	joaohenriques@estgv.ipv.pt
· Other Lecturers.	*Filipe Manuel Simões Caldeira* *caldeira@estgv.ipv.pt*

3. COURSE CONTENT.

This course provides blended knowledge and hands-on learning to conduct effective forensic and compliance audits to improve the cybersecurity approach in organizations, including the ones managing critical infrastructures. This course also provides training and techniques to reduce risks and impact of threats by identifying, extracting, and analysing evidence and non-compliant events to report findings technically and scientifically.

4. LEARNING OUTCOMES.

This course provides forensics and compliance academic background and guidance with hands-on practical activities to develop skills to conduct forensic investigations and successful audits. The course covers the regulatory, standards, and policy practices to develop and implement effective auditing compliance programs while keeping confidentiality, reliability and integrity of the processed data. The experimental work offers the opportunity to develop the skills and apply in practice the acquired knowledge and skills and scientifically communicate the results. Students will understand forensics and compliance auditing frameworks for cybersecurity and acquire the knowledge and skills to scientifically communicate the results of experimental work.

5. OBJECTIVES.

- Understand the foundations of forensic and compliance auditing cybersecurity.
- Develop and conduct effective forensics and compliance auditing actions.
- Apply appropriate forensic techniques for gathering and analyzing evidence.
- Identify and detect non-compliant events with cybersecurity frameworks, standards, regulations, and internal policies.
- Report findings from forensics and compliance auditing actions in a technical and scientific manner

6. COURSE ORGANISATION.

UNITS

1.	**Name of the unit:** Introduction **Topics:** Security Information Security Computer Crime Computer Systems Cybersecurity Authentication and Identification Cryptography Vulnerabilities and Exploits MITRE ATT&CK® Forensics Compliance Auditing Main European Union and United States Directives Ethical Considerations Laws and Regulations Cybersecurity Frameworks Data Privacy Critical Infrastructures (CI) Industrial and Automation Control Systems

2.	**Name of the unit:** Research **Topics:** Terminology Paper Structure Research Activities Research Process Academic Writing Journals and Conferences Research Sources Research Tools
3.	**Name of the unit:** Threats detection **Topics:** Threats Malware Attacks TOR and the Deep Web Anomaly-based Detection Cybersecurity Kill Chain Critical Infrastructure NIST Framework for Improving Critical Infrastructure Cybersecurity Security Information Event Management (SIEM) Other Security Analytics Platform Endpoint Detection and Response (EDR)
4.	**Name of the unit:** Forensic Investigation **Topics:** Computer or Digital Forensics Digital Evidence Digital Forensics History Digital Forensics Specialization Digital Forensics Standards Post Mortem Digital Forensics Live Forensics Anti-forensics Case/Incident resolution process in Court Duty of Experts, Admissibility, Reliability of Digital Evidence, Levels of Certainty, Scientific Evidence, Direct vs Circumstantial Evidence, Digital Forensics Report, Expert Reports Forensic investigation process Digital and Network forensics Digital forensic readiness

	Forensic schemas Confidentiality, reliability, and integrity Chain of custody
5.	**Name of the unit:** Compliance Auditing **Topics:** Compliance Auditing Audit Stages Processes Audit Charter General Types of Audits Audit Approaches Auditor's Responsibility Audits vs Assessments Auditor vs Auditee Roles Internal controls Regulations Policies Laws and Legal Bodies Standards, guidelines, procedures Ethics Information security policies Audit Standards Audit Tasks vs Skills Matrix Communications Schedule

LEARNING RESOURCES AND TOOLS.
Slides, Papers, Books, Regulations, Standards, Security Frameworks, Python, LateX, Linux and Windows OS
PLANNED LEARNING ACTIVITIES AND TEACHING METHODS.
Lectures, practical work and tutorials

7. ASSESSMENT METHODS, CRITERIA AND PERIOD.
This course is graded. The evaluation will combine a written exam (50%) and practical work (50%). The practical work consists of carrying out research and hands on work on one of the topics of forensic auditing or compliance. The achieved results will be submitted with partial deliveries and reported as a scientific article.
OBSERVATIONS.

8. BIBLIOGRAPHY AND TEACHING MATERIALS.

Ahmed, S., Obermeier, S., Sudhakaran, S., & Roussev, V. (2017). Programmable logic controller forensics. IEEE Security & Privacy, 15(6), 18–24.

Amazon Editorial Staff. (2025). How to perform a GDPR compliance audit: Step-by-step guide. Independently published.

Anderson, R. (2020). Security engineering (3rd ed.). Wiley.

Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. Computers & Security, 105, 102237.

Asquith, A., & Horsman, G. (2019). Let the robots do it!–Taking a look at robotic process automation and its potential application in digital forensics. Forensic Science International: Reports, 1, 100007.

Benzaid, C., & Taleb, T. (2020). ZSM security: Threat surface and best practices. IEEE Network, 34(3), 124–133.

Death, D. (2017). Information security handbook: Develop a threat model and incident response strategy to build a strong information security framework. Packt Publishing Ltd.

Dotson, C. (2021). Practical cloud security: A guide for secure design and deployment. No Starch Press.

European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR). Official Journal of the European Union.

European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2 Directive). Official Journal of the European Union.

Gilman, E., & Barth, D. (2019). Zero trust networks: Building secure systems in untrusted networks. O'Reilly Media.

Hassan, N. A. (2019). Digital forensics basics: A practical guide using Windows OS. Apress.

Johansen, G. (2022). Digital forensics and incident response: Incident response tools and techniques for effective cyber threat response. Packt Publishing Ltd.

Martin, B. (2026). GDPR for startups and scaleups: A practical guide. DataReg Press.

Payment Card Industry Security Standards Council. (2022, March). Payment Card Industry Data Security Standard – Requirements and Testing Procedures, v4.0.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Santos, H. M. D. (2022). Cybersecurity: A practical engineering approach. CRC Press/Chapman & Hall.

Seitz, J., & Arnold, T. (2021). Black hat Python: Python programming for hackers and pentesters. No Starch Press.

Sulter, R., & Kramer, J. (2024). Digital Forensics and Investigations: People, process, and technologies to defend the enterprise. TechPress.

Tevault, D. A. (2018). Mastering Linux security and hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Packt Publishing Ltd.

Tzanou, M. (2026). Health data privacy under the GDPR: Big data challenges and regulatory responses. Compliance Press.

Stallings, W. (2022). Network security essentials: Applications and standards. Pearson.

Whitman, M. E., & Mattord, H. J. (2021). Principles of information security. Cengage Learning.