Co-funded by the
Erasmus+ Programme
of the European Union

EUROPEAN UNIVERSITY FOR CUSTOMISED EDUCATION

STUDY GUIDE

FORENSICS AND COMPLIANCE AUDITING CIBERSECURITY

Organised by

Polytechnic Institute of Viseu

1. IDENTIFYING DATA.	
· Course Name.	*Forensics and Compliance Auditing Cybersecurity*
· Coordinating University.	*Polytechnic Institute of Viseu*
· Partner Universities Involved.	
· Course Field(s).	*Cybersecurity*
· Related Study Programme.	*Master in Informatics Engineering - Information Systems*
· ISCED Code.	*0612*
· SDG.	*Goal 9: Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation*
· Study Level.	*M (Master)*

· Number of ECTS credits allocated.	*3*
· Mode of Delivery.	*Online live*
· Language of Instruction.	*English*
· Course Dates.	*Spring Semester*
· Schedule of the course.	*Duration: 78 work hours (10 hours for synchronous lectures + 10 hours for asynchronous lectures + 58 hours for autonomous work)* *Periodicity: Week, Friday 15:00 CET (2.5 hours/session) – Starts on March 7th and ends on May 9th*
· 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*
· 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 Oss
PLANNED LEARNING ACTIVITIES AND TEACHING METHODS.
Lectures, group work and tutorials

7. ASSESSMENT METHODS, CRITERIA AND PERIOD.

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.

S. Bosworth and M. E. Kabay, Computer security handbook. John Wiley & Sons, 2002.

H. Berghel, “The discipline of internet forensics,” Communications of the ACM, vol. 46, no. 8, pp. 15–20, 2003

M. M. Houck and J. A. Siegel, Fundamentals of forensic science. Academic Press, 2009.

Spreitzenbarth, M., & Uhrmann, J. (2015). Mastering python forensics. Packt Publishing Ltd.

Sammons, J. (2012). The basics of digital forensics: the primer for getting started in digital forensics. Elsevier.

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

Hosmer, C. (2014). Python forensics: a workbench for inventing and sharing digital forensic technology. Elsevier.

Nelson, B., Phillips, A., & Steuart, C. (2014). Guide to computer forensics and investigations. Cengage Learning.

Izedonmi, P. F. O. (2006). Introduction to Auditing.

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

Chisum, J. W. (1999). Crime reconstruction and evidence dynamics. Presented at the Academy of Behavioral Profiling Annual Meeting. Monterey, CA.

Henseler, J. (2000). Computer crime and computer forensics. In The encyclopedia of forensic science. London: Academic Press.

Cannon, D. L. (2011). CISA certified information systems auditor study guide. John Wiley & Sons.

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.

Jones, K. J., Bejtlich, R., & Rose, C. W. (2005). Real digital forensics: computer security and incident response. Addison-Wesley Professional.

Ahmed, S. Obermeier, S. Sudhakaran, and V. Roussev, "Programmable logic controller forensics," IEEE Security & Privacy, vol. 15, no. 6, pp. 18–24, 2017.

Johnson, T. A. (Ed.). (2015). Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare. CRC Press.

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

Steinberg, J. (2022). Cybersecurity for dummies. John Wiley & Sons.

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

A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," IEEE Access, 2022

T. W. HOUSE, "NATIONAL SECURITY PRESIDENTIAL DIRECTIVE INSPD-54," https://irp.fas.org/offdocs/nspd/nspd-54.pdf, 2008, visited on 2021-10-19.

C. of the European Union, "Council Directive 2008/114/EC," https://eur-lex.europa.eu/eli/dir/2008/114/oj, 2008, visited on 2023-05-09.

E. Casey, Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011.

H. Studiawan, F. Sohel, and C. Payne, "A survey on forensic investigation of operating system logs," Digital Investigation, vol. 29, pp. 1–20, 2019

S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, Tech. Rep., 2020

J. R. Vacca, Computer Forensics: Computer Crime Scene Investigation (Networking Series)(Networking Series). Charles River Media, Inc., 2005.

Y. Kwon, F. Wang, W. Wang, K. H. Lee, W.-C. Lee, S. Ma, X. Zhang, D. Xu, S. Jha, G. F. Ciocarlie et al., "Mci: Modeling-based causality inference in audit logging for attack investigation." in NDSS, vol. 2, 2018, p. 4.

I. Ahmed, S. Obermeier, M. Naedele, and G. G. Richard III, "SCADA Systems: Challenges for Forensic Investigators," Computer, vol. 45, no. 12, pp. 44–51,Dec. 2012

K. Sindhu and B. Meshram, "Digital Forensic Investigation Tools and Procedures," in International Journal of Computer Network and Information Security, ser. IJCNIS, April 2012

P. Sommer, "Digital evidence," Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers, The Information Assurance Advisory Council (IAAC),, 2012.

J. Williams, "Acpo good practice guide for digital evidence," https://npcc.police.uk, Metropolitan Police Service, Association of chief police officers, GB, Tech. Rep., 2012

E. Cornelius and M. Fabro, "Recommended practice: Creating cyber forensics plans for control systems," Idaho National Laboratory (INL), Tech. Rep., 2008

N. M. Karie and H. S. Venter, "Taxonomy of challenges for digital forensics," Journal of forensic sciences, vol. 60, no. 4, pp. 885–893, 2015

N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-design framework for cyberphysical cloud systems," IEEE Cloud Computing, vol. 3, no. 1, pp. 50–59, 2016.

A. Iqbal, M. Ekstedt, and H. Alobaidli, "Digital forensic readiness in critical infrastructures: A case of substation automation in the power sector," in International Conference on Digital Forensics and Cyber Crime. Springer, 2017, pp. 117–129.

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

M. Elyas, A. Ahmad, S. B. Maynard, and A. Lonie, “Digital forensic readiness: Expert perspectives on a theoretical framework,” Computers & Security, vol. 52, pp. 70–89, 2015

M. Elyas, S. B. Maynard, A. Ahmad, and A. Lonie, “Towards a systemic framework for digital forensic readiness,” Journal of Computer Information Systems, vol. 54, no. 3, pp. 97–105, 2014.

B. Endicott-Popovsky, D. A. Frincke, and C. A. Taylor, “A theoretical framework for organizational network forensic readiness.” J. Comput., vol. 2, no. 3, pp. 1– 11, 2007.

A. Aminnezhad, A. Dehghantanha, and M. T. Abdullah, “A survey on privacy issues in digital forensics,” International Journal of Cyber-Security and Digital Forensics, vol. 1, no. 4, pp. 311–324, 2012.

Jones, K. J., Bejtlich, R., & Rose, C. W. (2005). Real digital forensics: computer security and incident response. Addison-Wesley Professional.

B. Shebaro and J. R. Crandall, “Privacy-preserving network flow recording,” digital investigation, vol. 8, pp. S90–S100, 2011.

N. J. Croft and M. S. Olivier, “Sequenced release of privacy-accurate information in a forensic investigation,” Digital Investigation, vol. 7, no. 1-2, pp. 95–101, 2010.

S. Garfinkel, “Digital forensics xml and the dfxml toolset,” Digital Investigation, vol. 8, no. 3–4, pp. 161–174, 2012.

E. Casey, G. Back, and S. Barnum, “Leveraging cybox™ to standardize representation and exchange of digital forensic information,” Digital Investigation,vol. 12, pp. S102–S110, 2015.

W. B. Glisson, T. Storer, and J. Buchanan-Wollaston, “An empirical comparison of data recovered from mobile forensic toolkits,” Digital Investigation, vol. 10, no. 1, pp. 44–55, 2013

W. Alink, R. Bhoedjang, P. A. Boncz, and A. P. de Vries, “Xiraf–xml-based indexing and querying for digital forensics,” digital investigation, vol. 3, pp. 50–58, 2006.

R. A. Bhoedjang, A. R. van Ballegooij, H. M. van Beek, J. C. van Schie, F. W. Dillema, R. B. van Baar, F. A. Ouwendijk, and M. Streppel, “Engineering an online computer forensic service,” Digital Investigation, vol. 9, no. 2, pp. 96–108, 2012.

R. van Baar, H. van Beek, and E. van Eijk, “Digital forensics as a service: A game changer,” Digital Investigation, vol. 11, pp. S54–S62, 2014.

M. Cohen, S. Garfinkel, and B. Schatz, “Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary in formation and forensic workflow,” digital investigation, vol. 6, pp. S57–S68, 2009.

A. Moser and M. I. Cohen, “Hunting in the enterprise: Forensic triage and incident response,” Digital Investigation, vol. 10, no. 2, pp. 89 – 98, 2013, triage in Digital Forensics. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1742287613000285

S. Almulla, Y. Iraqi, and A. Jones, “Feasibility of Digital Forensic Examination and Analysis of a Cloud Based Storage Snapshot,” Journal of Digital Information Management, vol. 15, no. 1, 2017

A. Razaque, M. B. H. Frej, B. Alotaibi, and M. Alotaibi, “Privacy preservation models for third-party auditor over cloud computing: A survey,” Electronics, vol. 10, no. 21, p. 2721, 2021

S. Zawoad, A. K. Dutta, and R. Hasan, “SecLaaS: Secure Logging-as-a-Service for Cloud Forensics,” CoRR, vol. abs/1302.6267, 2013. [Online]. Available: http://arxiv.org/abs/1302.6267

A. Patrascu and V.-V. Patriciu, “Logging system for cloud computing forensic environments,” Journal of Control Engineering and Applied Informatics, vol. 16, no. 1, pp. 80–88, 2014

K. Ruan and J. Carthy, “Cloud computing reference architecture and its forensic implications: A preliminary analysis,” in Digital Forensics and Cyber Crime. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 1–21

C. F. Tassone, B. Martini, and K.-K. R. Choo, “Visualizing digital forensic datasets: A proof of concept,” Journal of forensic sciences, 2017.

O. Setayeshfar, C. Adkins, M. Jones, K. H. Lee, and P. Doshi, “Graalf: Supporting graphical analysis of audit logs for forensics,” Software Impacts, vol. 8, p. 100068, 2021.

A. Asquith and G. Horsman, “Let the robots do it!–taking a look at robotic process automation and its potential application in digital forensics,” Forensic Science International: Reports, vol. 1, p. 100007, 2019.

R. Verma, J. Govindaraj Dr, S. Chhabra, and G. Gupta, “Df 2.0: An automated, privacy preserving, and efficient digital forensic framework that leverages machine learning for evidence prediction and privacy evaluation,” Journal of Digital Forensics, Security and Law, vol. 14, no. 2, p. 3, 2019.

C. Benzaid and T. Taleb, “Zsm security: Threat surface and best practices,” IEEE Network, vol. 34, no. 3, pp. 124–133, 2020.

J. Gallego-Madrid, R. Sanchez-Iborra, P. M. Ruiz, and A. F. Skarmeta, “Machine learning-based zero-touch network and service management: A survey,” Digital Communications and Networks, 2021

C. Curt and J.-M. Tacnet, “Resilience of critical infrastructures: Review and analysis of current approaches,” Risk analysis, vol. 38, no. 11, pp. 2441–2458, 2018

K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to integrating forensic techniques into incident response,”NIST Special Publication, vol. 10, pp. 800–86, 2006

R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Role-based access control models,” Computer, vol. 29, no. 2, pp. 38–47, 1996

S. Slapnicar, T. Vuko, M. Cular, and M. Drascek, “Effectiveness of cybersecurity audit,” International Journal of Accounting Information Systems, vol. 44, p. 100548, 2022

M. Lee, B. Hatfax, and J. Wingad, “Critical function monitoring and compliance auditing system,” https://www.google.com/patents/US20070136814, Jun. 14 2007, uS Patent App. 11/299,049.

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

C. I. Cybersecurity, “Framework for improving critical infrastructure cybersecurity,” Framework, vol. 1, no. 11,2014.

G. Disterer, “Iso/iec 27000, 27001 and 27002 for information security management,” Journal of Information Security, vol. 4, no. 2, 2013.

R. C. Nickerson, U. Varshney, and J. Muntermann, “A method for taxonomy development and its application in information systems,” European Journal of Information Systems, vol. 22, no. 3, pp. 336–359, 2013.