SYLLABUS

1. Data about the program of study

1.1 Institution	Technical University of Cluj-Napoca
1.2 Faculty	Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Master of Science
1.6 Program of study / Qualification	Cybersecurity Engineering / Master
1.7 Form of education	Full time
1.8 Subject code	7.00

2. Data about the subject

2.1 Subject name				***Information System Audit and Risk Management***	
2.2 Course responsible / lecturer				Dr. eng. Luțaș Dan - dlutas@bitdefender.com	
2.3 Teachers in charge of seminars				Dr. eng. Luțaș Dan - dlutas@bitdefender.com	
2.4 Year of study	I	2.5 Semester	2	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary				DS
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)				DI

3. Estimated total time

3.1 Number of hours per week	3	of which:	Course	2	Seminar	1	Laboratory	-	Project	-
3.4 Total hours in the curriculum	42	of which:	Course	28	Seminar	14	Laboratory	-	Project	-
3.7 Individual study:										
(a) Manual, lecture material and notes, bibliography										48
(b) Supplementary study in the library, online and in the field										18
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										15
(d) Tutoring										0
(e) Exams and tests										2
(f) Other activities										0

3.8 Total hours of individual study (sum (3.7(a)...3.7(f)))	83
3.9 Total hours per semester (3.4+3.8)	125
3.10 Number of credit points	5

4. Pre-requisites (where appropriate)

4.1 Curriculum	Information Security
4.2 Competence	Computer Architecture; Operating Systems

5. Requirements (where appropriate)

5.1 For the course	blackboard, beamer, computers
5.2 For the applications	blackboard, beamer, computers

6. Specific competences

6.1 Professional competences	**C1.** Identify and understand the security issues specific to the different contexts of computing system usage. Appropriately apply the basic elements of security management and methods of evaluation and management of information security risks. • **C1.1.** Knowledge of advanced theoretical and practical terminology, concepts, and principles specific to cybersecurity field. Knowledge of concepts about cybersecurity risk evaluation, and management. • **C1.2.** Understanding cybersecurity risks specific to new situations and their relationship with previously experienced situations and risks. Be able to predict possible threat scenarios when using cybersecurity solutions in new fields or situations. • **C1.3.** Capability to identify and model new types of cybersecurity risks affecting end users, computing systems, and software applications, and identify and evaluate possible solutions against such risks. • **C1.4.** Capability to identify and assess the limitations of existing cybersecurity solutions and their security risks, relative to well-known classifications. • **C1.5.** Capability to develop new theoretical models and methods to analyze and assess the cybersecurity properties and effectiveness of existing solutions. **C3.** Analyze and evaluate the security characteristics of computing system. Identify the misconfigurations and software vulnerabilities. • **C3.1.** Theoretical and practical knowledge of different cases of computing system misconfiguration and misusage that expose them to cybersecurity attacks, and of different types of software vulnerabilities and possible cybersecurity attacks. • **C3.2.** Be able to analyze and understand new kinds of software and communication protocols, in order to identify new possible cybersecurity threats, vulnerabilities, and risks. Be able to use commonly used databases of reported vulnerabilities and attacks in the process of assessing the cybersecurity of a new computing system. • **C3.3.** Capability to make cybersecurity assessments and identify possible attack surface of unknown computing systems, networks, or software applications. • **C3.4.** Capability to identify and assess theoretical and practical limitations of existing automatic vulnerability detection tools and propose possible combinations of such tools for improved results, where and if possible.
6.2 Cross competences	N/A

7. Discipline objectives (as results from the *key competences gained*)

7.1 General objective	Studying and developing a knowledge base about of information systems audit and risk management; understanding the process of auditing information systems according to international standards (such as ISACA)
7.2 Specific objectives	1. Understanding the process of auditing information systems, considering international standards (ISACA) and best practices. 2. Understanding the processes of IT Governance and IT Management and the activity of auditing the IT Governance and Management 3. Understanding the processes of acquiring, developing and implementing information systems and the activity of auditing these processes. 4. Understanding the processes information systems operations and maintanance, developing business continuity and disaster recorvery plans, and the activity of auditing these processes and plans. 5. Understanding the process of protecting information systems (information systems security, access control, securing the network infrastructure and physical security) and the activity of auding this process.

8. Contents

8.1 Lectures	Hours	Teaching methods	Notes
Introducere to Information Systems Auditing and Risk Management	2	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges.	
IT Governance (roles and responsabilities, security strategies, policies, standards and procedures, governance KPIs and meterics)	2		
Auditing of IT Governance	2		
Information Systems Risk Management (risk evaluation – vulnerabilities, threats, analysis and monitoring) and auditing a risk management program.	2		
BCP (Business Continuity Planning) and Disaster Recovery (management, administration and auditing - Impact Analysis, RPO/RTO, backups)	2		
Incident handling (procedures for incident response, preparing and developing an incident response plan, testing the incident response/BCP/DR plans)	2		
Software Project Management: Development Life Cycle (DLC), certification and accreditation, business software (e-commerce, electronic data exchange, banking applications, electronic fund transfer)	2		
Auditing the Software Project Management program	2		
Systems security operations (patch management, change management) and maintanance, auditing (operating systems, networking infrastructure)	2		
Administration of Information Systems (frameworks, auditing), logical access controls (identification/authorization), physical access and auditing the management of information security program	2		
Network infrastructure security (LAN, WAN, Wireless, Firewall, IDS, IPS, VoIP, PBX, testing for network vulnerabilities)	2		
Auditing the network infrastructure	2		
Information Security Management (governance, risk management, developing and maintaining an information security program)	2		
Synthetic overview of entire course, highlight of important conclusions, discuss subjects chosen by students	2		

Bibliography:

1. CISA Certified Information Systems Auditor Study Guide (Cannon, David – 2011 – Sybex) (3rd ed)
2. IT Auditing Using Controls to Protect Information Assets (Davis, Chris – 2011 – McGraw-Hill) (2nd ed)
3. CISM Review Manual 2013 (ISACA – 2012 – ISACA) (11th edition)
4. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (Landoll, Douglas – 2011 – CRC Press) (2nd ed)
5. Various white-papers or scientific papers on the subject of auditing informations systems security

8.2 Applications - Seminars / Laboratory / Project	Hours	Teaching methods	Notes
Importance of securing and auditing information systems	1	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges	
Risk Management. Disaster recovery : principles and techniques	1		
Importance of security patch management. Network security.	1		
Analysis of recent technical reports, white-papers, scientific papers regarding vulnerabilities in operating systems.	1		
Analysis of recent technical reports, white-papers, scientific papers regarding vulnerabilities in network infrastructure.	1		

Analysis of recent technical reports, white-papers, scientific papers regarding application specific vulnerabilities.	1		
Analysis of recent technical reports, white-papers, scientific papers regarding advanced attacks	1		

Bibliography:

1. CISA Certified Information Systems Auditor Study Guide (Cannon, David – 2011 – Sybex) (3rd ed)
2. IT Auditing Using Controls to Protect Information Assets (Davis, Chris – 2011 – McGraw-Hill) (2nd ed)
3. CISM Review Manual 2013 (ISACA – 2012 – ISACA) (11th edition)
4. The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (Landoll, Douglas – 2011 – CRC Press) (2nd ed)
5. Various white-papers or scientific papers on the subject of auditing informations systems security

9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

Achieved through periodic discussions with the representatives of significant employers, mainly companies that have projects in information security.

Information systems audit and security risk management disciplines are present in many similar master programs in computers and information security, like :

- IT&C Audit – IT&C Security Master Program - THE BUCHAREST ACADEMY OF ECONOMIC STUDIES, http://ism.ase.ro/files/Curriculum/Y2012-2014/analyticalprograms/en/S4/ISM_PA_EN_024.pdf
- Information Technology Auditing - Master of Science in Information Systems Audit and Control – Georgia State University, http://cis.robinson.gsu.edu/academic-programs/ms-is-audit/curriculum/
- Audit & Security - Information Security and Audit, MSc – University of Greenwich http://www2.gre.ac.uk/study/courses/pg/inftec/isa/cms-courses?banner=COMP1431&cyear=1415

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Ability to solve problems specific to the Information Systems Audit and Risk Management domain, attendance, active participation to the activities during lectures.	Written exam and/or multiple-choice questions on Moodle and/or giving a presentation about a topic studied during the lectures.	60%
Seminar	Ability to solve problems specific to the Information Systems Audit and Risk Management domain, attendance, active participation to the activities during lectures.	Giving a presentation (PowerPoint) about a research topic regarding Information Systems Audit and Risk Management and / or solving and presenting a solution to similar problems discussed during the lecture hours.	40%

Minimum standard of performance:

Lecture. Attending minimum 50% of lecture classes, to be allowed to take the final examination. Minimum final grade must be 5 for the exam to be considered passed.

Seminar. Attendance to 100% of classes (1 class can be recovered during the semester and a second one during the re-examination interval) in order to be admitted to the final exam. Minimum seminar grade must be 5 for being allowed at final exam.

Being able to define and explain in a specific context the base notions regarding auditing information systems and risk management, such as: the audit process, the IT governance and management process, acquiring, developing, implementing, maintaining and protecting information systems, together with audit methods and procedures specific to each process.

Date of filling in: 26.02.2025	**Responsible**	**Title First name Last name**	**Signature**
	Course	Dr. eng. Dan-Horea LUȚAȘ	
	Applications	Dr. eng. Dan-Horea LUȚAȘ	

Date of approval in the department
17.09.2025

Head of department,
Prof.dr.eng. Rodica Potolea

Dean,
Prof.dr.eng. Vlad Mureșan

Date of approval in the faculty
19.09.2025