SYLLABUS

1. Data about the program of study

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

2. Data about the subject

2.1 Subject name	***Information System Audit and Risk Management***			Subject code	**7**
2.2 Course responsible / lecturer	Dr. eng. Lutas Dan - dan.lutas@cs.utcluj.ro				
2.3 Teachers in charge of seminars / Laboratory / project	Dr. eng. Lutas Dan - dan.lutas@cs.utcluj.ro				
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: DF – fundamental, DS – speciality, DC – complementary				DS
	Optionality: DOB – mandatory, DOP – optional (alternative), DFA – optional (free choice)				DOB

3. Estimated total time

3.1 Number of hours per week	3	of which	3.2 Course	2	3.3 Seminar	1	3.3 Laboratory	-	3.3 Project	-
3.4 Total hours in the curriculum	42	of which	3.5 Course	28	3.6 Seminar	14	3.6 Laboratory	-	3.6 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										-
(e) Exams and tests										2
(f) Other activities										-

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 competence

6.1 Professional competences	• execute ICT audits • develop contingency plans for emergencies • manage system security • identify ICT security risks • perform risk analysis • educate on data confidentiality • establish an ICT security prevention plan • ensure compliance with legal requirements • monitor developments in field of expertise • keep up with the latest information systems solutions
6.2 Cross competences	• develop an analytical approach • taking a proactive approach • developing strategies to solve problems • being open minded

7. Expected Learning Outcomes

Knowledge	• assessment of risks and threats • ICT network security risks • ICT encryption • attack vectors • quality assurance methodologies • information security strategy • internal risk management policy • risk management • audit techniques • levels of software testing • system backup best practices • systems development life cycle
Skills	• advise on security risk management • communicate with stakeholders • ensure adherence to organisational ICT standards • execute ICT audits • identify ICT security risks • manage disaster recovery plans
Responsibilities and autonomy	The student has the ability to work independently in order to: • develop an analytical approach • take a proactive approach • develop strategies to solve problems • be open-minded

8. Discipline objective (as results from the *key competences gained*)

8.1 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)
8.2 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

9. Contents

9.1 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

9.2 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	1		

regarding advanced attacks			

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

10. 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

11. 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.	**Summative evaluation** consisting in a 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	**Summative evaluation** consisting in delivering 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) 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: 29.04.2026	Responsible	Title First name Last name	Signature
	Course	Dr. eng. Dan-Horea LUTAS	
	Applications	Dr. eng. Dan-Horea LUTAS	

Date of approval in the department	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council	Dean, Prof.dr.eng. Vlad Mureșan