AUDITUL SECURITĂȚII INFORMAȚIONALE

I. PRELIMINARII

Disciplina *Auditul securității informaționale (ASI)* se referă la teoria și practica auditului securității informaționale pentru diferite *entități (întreprinderi și organizații private, de stat, publice).*

Scop. Cursul este destinat pentru studenții de la masterat, specialitatea/ traseul *„Securitatea informațională”* ultimul an de studii și are ca scop formarea unui complex de cunoștințe, abilități și competențe pentru efectuarea auditului securității informaționale.

Precondiții. Însușirea disciplinei este condiționată de sistematizarea cunoștințelor anterior obținute în cursul de *Gestionarea securității informației, Auditul sistemelor de management.*

Competențe profesionale și finalități de studiu. Însușirea cu succes a cursului va permite studenților:

- Să achiziționeze un set de cunoștințe teoretice și abilități practice necesare în desfășurarea activității auditor intern al securității informaționale.
- Să organizeze, planifice, și să monitorizeze auditul securității informaționale a unei entități;
- Să elaboreze *Raportul de audit* intern și *Recomandări de îmbunătățire* a securității informației a unei entități.

Cadrul normativ și de reglementare: Familia de standarde ISO/IEC 27k, CoBIT, ITIL, cerințele ISACA, standardul ISO 19011, legislația națională, reglementări ramurale și interne .

Administrarea disciplinei. 30 ore de curs și 30 ore de laborator/lucrări practice, în total 60 ore de contact direct 90 ore lucru individual, 5 credite academice.

II. TEMATICA ȘI REPARTIZAREA ORIENTATIVĂ A ORELOR

Nr. d/o	Unități de conținut	Ore		
		Curs	Labo-rator	Lucrul individual
1.	Auditul SMSI	6	6	18
2.	Cadrul procedural de evaluare a securității informației	6	6	18
3.	Auditul securității infrastructurii tehnico-tehnologice	6	6	20
4.	Auditul/evaluarea conformității standardelor și certificarea	6	6	22
5.	Auditul activ și instrumente informatice de audit (CAATs)	6	6	12
Total		**30**	**30**	**90**

III. UNITĂȚI DE ÎNVĂȚARE

Tema 1. Cadrul conceptual de audit	
Obiectivele de referință	**Conținuturi**
- *Să cunoască recomandările cadrului normativ de referință privind auditul SMSI, IT, IS, tipurile de audit, etapele auditului, modurilor de documentare* - *Să politicile de securitate a informației* - *Să elaboreze politici și proceduri de securitate a informației potrivite necesităților unei USE*	• Cadrul normativ de referință • ISO 27k. COBIT. ITIL. ISACA • Legislația Republicii Moldova în domeniul auditului • Regulamente și instrucțiuni interne de audit • Cerințe profesionale pentru auditor ISO 19011 și ISO 27006-27008 • Codul de etică al auditorului (ISACA) *Lab 1. Elaborarea programului de audit, definirea frontierelor în cadrul cărora se va desfășura auditul*
Tema 2. Cadrul procedural de evaluare a securității informației	
Obiectivele de referință	**Conținuturi**
- *Să cunoască procedurile de audit intern, modurile de colectare a probelor de audit, de evaluare și documentare a auditului* - *Să aplice instrumentele potrivite în efectuarea auditurilor interne pentru diferite active* - *Să documenteze procesul de audit*	• Liste de verificare, machete, chestionare • Proceduri de evaluare a securității informaționale • Proceduri de audit a securității pentru diferite active: echipamente, date, suporturi de date, aplicații informatice, web aplicații, rețele, Internet • Documentarea procesului de audit *Lab 2. Colectarea informațiilor, metode de colectare, instrumente speciale utilizate în procesul de audit*
Tema 3. Auditul securității infrastructurii tehnico-tehnologice	
Obiectivele de referință	**Conținuturi**
- *Să cunoască principiile de audit IT/IS conform CobiT, ITIL, ITSM, ISO 27007/08* - *Să stabilească factorii de succes, indicatorii-cheie a scopurilor și a rezultatelor* - *Să identifice cadrul potrivit de audit al unei USE* - *Să evalueze nivelul de maturitate al unei USE conform modelului Nolan*	• Utilizarea CobiT pentru managementul și auditul IT • Esența CobiT: divizarea în management și audit • CobiT: principii de management și principii de audit • Factori de succes • Indicatori - cheie a scopurilor • Indicatori - cheie a rezultatelor • Interacțiunea CobiT cu alte standarde, e.g. ITIL, ISO 27k • Modelul de maturitate Nolan *Lab3: Studii de caz privind Auditul IT/IS.*

Tema 4. Auditul/evaluarea conformității standardelor/certificarea	
Obiectivele de referință	**Conținuturi**
- *Să cunoască avantajele auditului de conformitate, etapele, procedurile, fluxul activităților și documentația de certificare a SMSI* - *Să planifice și să gestioneze un program de audit de conformitate* - *Să evalueze controalele de securitate SMSI* - *Să elaboreze un raport de audit* - *Să elaboreze propuneri de valorificare a constatărilor de audit*	• Pregătirea către auditul de conformitate a SMSI • Efectuarea auditului • Încheierea auditului • Fluxul activităților de evaluare a conformității • Evaluarea controalelor de securitate SMSI • Structura raportului de audit • Elaborarea raportului de audit • Elaborarea propunerilor de valorificare a constatărilor consemnate • Revizuirea auditului SMSI *Lab 4. Planificarea – desfășurarea – gestionarea programului de audit al conformității ISO 27001:2018*
Tema 5. Auditul activ și instrumente informatice de audit (CAATs)	
• *Să explice esența și avantajele tehnicilor de audit asistate de calculator* - *Să justifice alegerea tehnicilor de audit potrivite cazului* - *Să opereze cu instrumente CAATs.*	• Tehnici de audit asistate de calculator • Utilizarea CAATs pentru munca de investigație • Integrarea CAATs cu instrumentele oferite de SO și platforme open source de genul Open XDAS, Free BSD, MAC OS *Lab.5. Explorarea unor proceduri automatizate de audit, instrumente de colectare a informațiilor privind vulnerabilitățile depistate, teste de penetrare, scanare a rețelei etc.*

VII. BIBILIOGRAFIE RECOMANDATĂ și *principalele standarde de sprijin*

1. Certified Information Systems Security Proffesional (CISSP), Ghid oficial de studii, ed.VII, 2015
2. ISACA Cybersecurity Fundamentals Glossary, 2016. https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf/
3. ISO/IEC 19011:2018. Ghid pentru auditarea sistemelor de management
4. ISO/IEC 27000:2019. Information security management systems. Overview and vocabulary
5. ISO/IEC 27001:2017. Information security management systems. Requirements
6. ISO/IEC 27002:2017 Code of practice for information security controls
7. ISO/IEC 27006:2019. Requirements for bodies providing audit and certification of information security management systems
8. ISO/IEC 27007:2019. Guidelines for information security management systems auditing
9. ISO/IEC TR 27008:2019. Guidelines for auditors on information security controls