SECŢIUNEA A

STANDARD OCUPAŢIONAL

1. Denumirea ocupaţiei şi codul COR

Manager securitatea informatiei
Cod COR 121118

2. Denumirea tradusă a ocupaţiei (En):

Chief Information Security Officer - CISO

3. Competenţe profesionale (capacitatea dovedită de a utiliza cunoştinţe, abilităţi şi capacităţi personale)

1. Stabilirea strategiei şi obiectivelor în domeniul securităţii informaţiei, armonizate cu strategia organizaţiei
2. Stabilirea cadrului de management al securităţii informaţiei
3. Stabilirea domeniului de securitate si managementul resurselor informationale
4. Planificarea sistemului de management al securităţii informaţiei pe baza riscurilor şi cerinţelor
5. Proiectarea măsurilor de securitate organizaţională şi procedurală necesare pentru tratarea riscurilor de securitate a informaţiei
6. Managementul accesului la resurse si informatii
7. Proiectarea măsurilor de securitate in procesele operationale
8. Proiectarea măsurilor de securitate IT&C
9. Proiectarea măsurilor de securitate ale organizaţiei în concordanţă cu analiza de risc la securitatea informaţiei
10. Integrarea cerinţelor de securitate a informaţiei stabilite la nivelul organizaţiei în contractele şi activităţile terţelor părţi
11. Implementarea şi urmărirea planului de acţiuni în domeniul securităţii informaţiilor
12. Consilierea conducerii organizaţiei cu privire la sistemul de management al securităţii informaţiilor
13. Gestionarea incidentelor de securitate a informatiei cu scopul minimizarii impactului acestora asupra afacerii.
14. Evaluarea sistemului de management al securităţii informaţiei
15. Aplicarea instrumentelor şi metodelor de îmbunătăţire a eficacităţii sistemului de management al securităţii informaţiei

4. Niveluri:

4.1. Nivelul de calificare conform Cadrului Naţional al Calificărilor (CNC)	6
4.2. Nivelul de referinţă conform Cadrului European al Calificărilor (EQF)	6
4.3. Nivelul educaţional corespondent, conform ISCED - 2011	6

5. Acces la altă ocupație/ ocupații cuprinse în nomenclatorul COR

5.1. Acces la ocupație/ ocupații de același nivel de calificare, conform CNC, pe bază de experiență/ recunoștere de competențe

Ocupația „Manager securitatea informației" (cod COR 121118), reprezintă o specializare a personalului care activează în domeniul IT (tehnologia informației), dedicată persoanelor care gestionează, realizează designul, supraveghează și evaluează securitatea informațională a unei organizații, pentru practicarea acesteia fiind necesare studii superioare tehnice. Prin prisma competențelor formate în sistemul formării inițiale în domeniul tehnic și ca urmare a similitudinii cu alte ocupații din aceeași grupă de bază, ocupațiile accesibile acestor specialiști sunt:

Ocupația	**COD COR**
Director departament securitate	134920
Manager securitate	121306

5.2. Acces la ocupație/ ocupații de nivel de calificare imediat superior, conform CNC, pe bază de programe de formare profesională și experiență

Nu este cazul.

6. Informații suplimentare

Ocupația „Manager securitatea informației" (cod COR 121118) se adresează persoanelor (fizice) care proiectează, dezvoltă și gestionează securitatea informațiilor organizaționale și care au experiență în următoarele domenii:

- Guvernanța securității informaționale;
- Managementul riscului informațiilor;
- Dezvoltare programului de securitate a informațiilor;
- Managementul programului de securitate a informațiilor;
- Managementul incidentelor.

SECŢIUNEA B

STANDARD PENTRU ASIGURAREA CALITĂŢII ÎN EDUCAŢIE ŞI FORMARE PROFESIONALĂ, ASOCIAT OCUPAŢIEI

1.1. Cerinţe specifice de acces la program

1.1.1. Competenţe şi deprinderi necesare accesului la program:

Competenţe şi deprinderi necesare accesului la program:

Competenţe:

- gestionarea de activităţii sau proiecte tehnice ori profesionale complexe şi imprevizibile
- gestionarea dezvoltării profesionale a indivizilor şi grupurilor

Deprinderi:

-abilităţi avansate de planificare, managementul riscurilor, coordonare echipe, abilităţi decizionale, management al conflictelor, evaluare şi revizuire, raportare, furnizare şi obţinere de feedback, autoevaluare.

Competenţele şi deprinderile menţionate vor fi demonstrate la înscriere, astfel:

- printr-un program de formare sau o certificare de competenţe cu recunoaştere naţională (copie de pe diplomă/certificat plus suplimentul descriptiv din care să reiasă competenţele/deprinderile necesare);
- recomandare de la ultimul loc de muncă, în care să fie evidenţiată asumarea responsabilităţii pentru competenţele şi deprinderile menţionate;

Pentru competenţele şi deprinderile care nu pot fi dovedite conform procedurii menţionate mai sus, se va susţine, la începutul cursului, un test de evaluare, aplicat de furnizor, prealabil începerii cursului. Testul va fi structurat distinct, pe fiecare domeniu menţionat, iar în situaţia deţinerii unora dintre competenţe evaluarea se va realiza doar pentru celelalte domenii.

1.1.2. Condiţii minime de acces la program, raportate la nivelul de studii:

Nivelurile de studii:

- învăţământ general obligatoriu ☐
- învăţământ profesional prin şcoli profesionale ☐
- învăţământ liceal, fără diplomă de bacalaureat ☐
- învăţământ liceal, cu diplomă de bacalaureat ☐
- învăţământ postliceal ☐
- învăţământ superior cu diplomă de licenţă ☒
- învăţământ superior cu diplomă de master ☐

1.1.3. Alte studii necesare:

Studii superioare tehnice

1.1.4. Cerinţe speciale:

-să fie apt medical
-să aibă experienţă practică de minim 2 ani.
Dovada experienţei se face cu adeverinţe în original eliberate de angajator sau ITM, care atestă perioadele de activitate şi funcţia deţinută în cadrul societăţii.

2. Descrierea programului de educaţie şi formare profesională

6.1. Durata totală, nr. ore 180 **din care :**

- 60 **teorie;**
- 120 **practică.**

2.2. Planul de pregătire (anexa B1)

2.3. Programa de pregătire teoretică şi practică (anexa B2)

2.4. Echipamente/utilaje/programe software necesare pregătirii practice

Pregătirea practică se va desfăşura sub coordonarea unui formator, va consta în aplicarea cunoştinţelor asimilate pentru dezvoltarea, implementarea şi îmbunătăţirea procesului de mentenanţă al unei organizaţii.
Echipamente necesare:

- Computer / Laptop;
- Echipamente de proiecţie;
- Sistem de operare, programe software şi aplicaţii aferente.

Alte materiale: Manuale/suporturi de curs, standarde specifice.

2.5. Cerinţe privind nivelul minim de calificare şi experienţa profesională pentru: formatori, instructori/preparatori formare şi evaluatori.

Selecţia formatorilor cooptaţi în programul de formare profesională pentru ocupaţia de "Manager securitatea informaţiei" se realizează din rândul specialiştilor care îndeplinesc cumulativ următoarele condiţii:

- Pentru pregătirea teoretică – pregătire psiho-pedagogică de specialitate şi experienţă în domeniu de cel puţin 2 ani
- Pentru pregătirea practică - pregătire psiho-pedagogică de specialitate şi experienţă practică de cel puţin 3 ani în domeniu;
- Pentru evaluarea competenţelor – pregătire psiho-pedagogică de specialitate şi experienţă recentă de muncă în domeniu, de cel puţin 5 ani.

3. Informaţii referitoare la procesul de elaborare, verificare, validare, avizare şi aprobare a standardului ocupaţional pentru educaţie şi formare profesională:

3.1. Realizare:
Iniţiator/Autori:
Luminiţa Tatomir, Specialist elaborare standarde ocupaţionale, S.C. FiaTest S.R.L.
Camelia Ducaru, Specialist elaborare standarde ocupaţionale, S.C. FiaTest S.R.L.
Andrei Hohan, Consultant securitatea informatiei, S.C. FiaTest S.R.L.

Instituţia/instituţiile/persoane interesate: S.C. FiaTest S.R.L.
Data elaborării: 30.07.2015

3.2. Verificare profesională:
Specialist/Instituţia de profil:
Matache Bogdan Valentin - Consultant securitatea informatiei
Data verificării: 26.08.2015

3.3. Avizare:
Instituţie de profil: UPC România

3.4. Validare documentaţie:
Comitet sectorial/semnatari: Chifu Gabriel- preşedinte, Căpraru Valentina- expert verificare metodologica, Voievozeanu Ion-expert sectorial domeniu
Data validării: 02.10.2015

3.5. Aprobare:
Autoritatea Naţională pentru Calificări conform deciziei nr.415 din data...03.11.2015.....

ANEXA B1

PLAN DE PREGĂTIRE

Nr. crt.	Competenţa dobândită	Modul	Nr. ore teorie	Nr. ore practică
1.	Stabilirea strategiei şi obiectivelor în domeniul securităţii informaţiei, armonizate cu strategia organizaţiei	1. Securitatea informaţiei	8	18
2.	Stabilirea cadrului de management al securităţii informaţiei	2. Sistemul de management al securităţii informaţiei	10	22
3.	Stabilirea domeniului de securitate si managementul resurselor informaţionale			
4.	Planificarea sistemului de management al securităţii informaţiei pe baza riscurilor şi cerinţelor	3. Managementul riscurilor	10	16
5.	Proiectarea măsurilor de securitate organizaţională şi de resurse umane necesare pentru tratarea riscurilor de securitate a informaţiei	4. Proiectarea măsurilor de securitate	9	18
6.	Managementul accesului la resurse si informaţii			
7.	Proiectarea măsurilor de securitate în procesele operaţionale			
8.	Proiectarea măsurilor de securitate IT&C			
9.	Proiectarea măsurilor de securitate ale organizaţiei în concordanţă cu analiza de risc la securitatea informaţiei			
10.	Integrarea cerinţelor de securitate a informaţiei stabilite la nivelul organizaţiei în contractele şi activităţile terţelor părţi.			
11.	Implementarea şi urmărirea planului de acţiuni în domeniul securităţii informaţiilor	5. Implementarea sistemului de management al securităţii informaţiilor	8	16
12.	Consilierea conducerii organizaţiei cu privire la sistemul de management al securităţii informaţiilor			
13.	Gestionarea incidentelor de securitate a informatiei cu scopul minimizării impactului acestora asupra afacerii.			
14.	Evaluarea sistemului de management al securităţii informaţiei	6. Monitorizare, evaluare, îmbunătăţire	15	30
15.	Aplicarea instrumentelor şi metodelor de îmbunătăţire a eficacităţii sistemului de management al securităţii informaţiei			
	TOTAL ORE		60	120
	TOTAL GENERAL		**180**	

ANEXA B2

PROGRAMA DE PREGĂTIRE TEORETICĂ ŞI PRACTICĂ

Nr. crt.	MODUL	DISCIPLINĂ	CONŢINUT TEMATIC	METODE / FORME DE DESFĂŞURARE	MIJLOACE DE INSTRUIRE, MATERIALE DE ÎNVĂŢARE	CRITERII DE EVALUARE	NR.ORE	
							Teorie	Practică
1.	**Securitatea informaţiei**	Securitatea informaţiei	- Definiţii în managementul securităţii informaţiei - Tendinţe în securitatea informaţiei - Elemente generale de arhitecturi informatice - Notiuni despre securitatea cibernetica - Legislaţia în domeniul Informaţiilor clasificate	Prezentare, dezbatere,	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme	- Utilizează corect conceptele de bază ale securităţii informaţiei: confidenţialitate, integritate , disponibilitate, autenticitate, non-repudiere şi ale analizei de risc: ameninţare, vulnerabilitate, mijloace şi metode de control - Poziţionează măsurile de securitate în relaţie cu contextul actual de ameninţări şi atacuri la adresa informaţiei	2	6
		Elemente de management strategic	- Componentele strategiei - Modele şi metode de management strategic - Înţelegerea organizaţiei şi a contextului organizaţiei - Înţelegerea nevoilor şi aşteptărilor părţilor interesate - Definirea obiectivelor strategice	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte, descrie şi utilizează elementele componente ale strategiei; - Relaţionează misiunea, viziunea şi principiile conducătoare cu planul strategic. - Identifică şi clasifică necesităţile factorilor interesaţi pentru a asigura alinierea acestora cu obiectivele strategice ale organizaţiei - Analizează punctele tari, punctele slabe, oportunităţile şi	3	6

						ameninţările pentru organizaţie, dezvoltă acţiuni necesare şi stabileşte priorităţi privind implementarea acţiunilor; - Defineşte caracteristicile obiectivelor strategice şi operaţionale (SMART, relaţionate cu strategia, etc.). - Defineşte şi utilizează indicatori de performanţă pentru monitorizarea performanţelor organizaţiei şi evaluează rezultatele obţinute în relaţie cu rezultatele planificate.		
		Strategia în domeniul securităţii informaţii	- Contextul strategic al securităţii informaţiei - Cadrul de guvernanţă al securităţii informaţiei - Definirea şi asigurarea resurselor pentru sistemul de management al securităţii informaţiei - Leadership şi angajamentul conducerii	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte şi menţine o Strategie de Securitate a informaţiei aliniată cu obiectivele organizaţiei, în scopul orientării sistemului de management al securităţii informaţiei - Integrează guvernanţa securităţii informaţiei cu cadrul organizaţional de guvernanţă pentru a asigura că sistemul de management al securităţii informaţiei sprijină îndeplinirea obiectivelor organizaţionale - Identifică influenţele interne şi externe asupra organizaţiei (de exemplu tehnologii, mediul de afaceri, toleranţa la risc, locaţia geografică, cerinţe legale şi de reglementare)	3	6

						pentru a asigura că strategia de securitate a informaţiei adresează aceşti factori - Pregăteşte analize de oportunitate pentru justificarea investiţiilor în securitatea informaţiei - Obţine angajament din partea conducerii de vârf şi suportul părţilor interesate pentru a maximiza şansele de success ale implementării SMSI		
2.	**Sistemul de management al securităţii informaţiei**	Sisteme de management	- Evoluţia conceptului de sisteme de management. Sisteme de management al calităţii. - Relaţia dintre diferite Sisteme de management - Standarde ISO în domeniul sistemelor de management al securităţii informaţiei. Prezentare, evolutie. Relaţia între standarde - Criteriile Modelului de Excelenţă al EFQM	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte şi descrie modul în care pot fi folosite standardele ISO pentru a susţine sistemul de management al organizaţiei. - Descrie şi face diferenţa între diferitele tipuri de sisteme de management standardizate: calitate, mediu, securitate şi sănătate în muncă, servicii, securitatea informaţiei. - Descrie şi face diferenţa între standardele şi normele de securitate a informaţiei - Defineşte şi descrie modul în care sunt folosite criteriile Modelului de Excelenţă al EFQM ca suport în obţinerea unui nivel de excelenţă a performanţelor organizaţiei.	2	4

		Managementul proceselor	- Abordarea procesuală şi abordarea sistemică a managementului - Descrierea interconectării proceselor - Obiective şi indicatori de performanţă ai proceselor - Analiza proceselor - Analiza tendinţelor şi tiparelor	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Identifică procesele ce urmează a fi incluse în sistemul de management. - Descrie modul în care sunt stabilite, măsurate şi monitorizate obiectivele proceselor şi care este impactul pe care îl au acestea asupra calităţii produsului sau serviciului. - Foloseşte harta procesului, diagrama flux şi alte instrumente vizuale pentru a analiza un proces şi a-l compara cu procedurile scrise, instrucţiunile de lucru şi alte documente. - Identifică fluxurile de informaţii şi resursele informaţionale necesare pentru desfăşurarea proceselor şi cerinţele de confidenţialitate, integritate, disponibilitate privind acestea.	2	4
		Definirea domeniului de aplicare al SMSI	- Domeniul şi limitele SMSI - Managementul activelor informaţionale - Clasificarea informaţiilor	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte domeniul de aplicare al SMSI, în conformitate cu cerinţele ISO/CEI 27001:2013 - Identifică resursele informaţionale din cadrul SMSI şi defineşte o schemă de evaluare şi clasificare din punct de vedere al confidenţialităţii, integrităţii, disponibilităţii. - Întocmeşte inventare de resurse informaţionale, aliniate cu alte inventare relevante în organizaţie	2	6

						- Defineşte criterii de responsabilitate şi norme de utilizare acceptabilă a resurselor. - Defineşte ghiduri de clasificare, marcare şi manipulare a informaţiilor care asigură că informaţiile primesc o protecţie adecvată în conformitate cu importanţa lor pentru organizaţie.		
		Sistemul de management al securităţii informaţiei	- Cerinţele ISO 27001 - Roluri, responsabilităţi şi autorităţi - Organizarea securităţii informaţiei	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte şi comunică rolurile şi responsabilităţile de securitate a informaţiei în cadrul organizaţiei pentru a stabili responsabilităţi clare şi linia de autoritate - Defineşte şi menţine politici de securitate a informaţiei pentru a comunica directivele conducerii şi a furniza îndrumare pentru dezvoltarea de reguli, proceduri şi ghiduri. - Defineşte reguli şi mecanisme pentru stabilirea, implementarea, menţinerea şi îmbunătăţirea continuă a sistemului de management al securităţii informaţiei, conforme cu cerinţele standardelor internaţionale aplicabile. - Defineşte reguli de segregare a responsabilităţilor pentru	4	8

						prevenirea oportunităţilor de fraudă şi eroare. - Defineşte mecanisme de contact cu autorităţile şi grupurile profesionale relevante pentru securitatea informaţiei.		
3.	**Managementul riscurilor**	Introducere în managementul riscurilor	- Rolul managementul riscului - Contextul managementului riscului - Procesul de management al riscului	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Utilizează corect conceptele de management al riscului , aşa cu sunt definite de standardul internaţional în domeniu, ISO 31000:2009 - Identifică şi descrie contextul extern şi intern al organizaţiei pentru managementul riscului, conform îndrumărilor ISO 3100:2009 - Identifică toate activităţile şi responsabilităţile componente ale procesului de management al riscurilor relevante.	2	4
		Cerinţe legale şi contractuale de securitate a informaţiilor	- Cerinţe comerciale - Cerinţe legale privind securitatea informaţiei - Cerinţe de reglementare sectoriale	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Identifică cerinţele legale, de reglementare, organizaţionale şi contractuale cu privire la securitatea informaţiei relevante pentru organizaţie. - Identifică măsurile de securitate necesare pentru conformarea cu cerinţele identificate.	2	4
		Analiza şi evaluarea riscurilor de securitate a informaţiilor	- Criterii de evaluare a riscului - Ameninţare, vulnerabilitate, risc - Metodologii de analiză	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector	- Defineşte criterii pentru evaluarea riscurilor. - Defineşte criterii de risc de securitate a informaţiilor, care includ	4	4

			şi evaluare a riscurilor de securitate a informaţiilor		• reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	criterii de acceptanţă a riscurilor şi criterii de efectuare a analizelor de risc. - Utilizează metodologiile descrise de standardele internaţionale pentru a defini o metodologie de management al riscurilor de securitate a informaţiilor. - Identifică, analizează şi evaluează riscurile în conformitate cu metodologia definită cu rezultate coerente şi repetabile.		
		Tratarea riscurilor	- Selectarea opţiunilor de tratare a riscurilor - Identificarea măsurilor de securitate pentru tratarea riscurilor - Declaraţia de aplicabilitate - Planul de tratare a riscurilor / conformare	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Determină opţiunile de tratare a riscurilor în funcţie de rezultatele analizei şi evaluării riscurilor. - Selectează măsurile de securitate a informaţiilor adecvate pentru reducerea riscurilor la un nivel acceptabil. - Redactează o declaraţie de aplicabilitate, în conformitate cu cerinţele ISO/IEC 27001:2013, care documentează cerinţele de securitate aplicabile în domeniul de aplicare al SMSI, pe baza analizei riscurilor şi cerinţelor. - Redactează un plan de tratare a riscurilor conţinând acţiunile şi măsurile necesare pentru reducerea riscurilor până	2	4

						la un nivel acceptabil. - Monitorizează riscurile pentru a identifica şi gestiona modificările relevante pentru managementul riscurilor.		
4.	**Proiectarea măsurilor de securitate**	Securitate organizaţională şi resurse umane	- Organizarea securităţii - Securitatea resurselor umane	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Identifică cerinţele familiei de standarde ISO 27000 cu privire la securitatea organizaţională şi de resurse umane. - Defineşte politici, obiective, procese şi proceduri pentru gestionarea cerinţelor de organizare şi de resurse umane pentru securitatea informaţiei.	1	2
		Managementul accesului la resurse şi informaţii	- Controlul accesului	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte şi documentează o politică de control al accesului pe baza cerinţelor de business şi securitatea informaţiei. - Defineşte măsuri procedurale şi tehnice pentru a asigura accesul utilizatorilor autorizaţi şi a preveni accesul utilizatorilor neautorizaţi la informaţii, sisteme şi servicii - Defineşte reguli privind responsabilizarea utilizatorilor pentru protejarea informaţiilor de autentificare. - Defineşte cerinţe privind măsurile tehnice de control al accesului la sisteme şi aplicaţii.	2	4

		Măsuri de securitate în procesele operaţionale	- Integrarea cerinţelor de securitate în procese operaţionale: - Managementul schimbării - Managementul proiectelor - Achiziţii - Continuitatea activităţii - Procese specifice	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Verifică identificarea şi documentarea cerinţelor de securitate a informaţiei în procesele operaţionale: managementul schimbării, dezvoltare, continuitatea activităţii, achiziţii, etc.	1	2
		Măsuri de securitate IT&C	- Protecţia sistemelor IT&C - Recomandările ISO 27002 - ISO/IEC 27032 — Ghid pentru securitate cibernetică - ISO/IEC 27033 Securitatea reţelei	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte proceduri şi responsabilităţi operaţionale pentru operarea corectă şi sigură a sistemelor IT&C. - Defineşte cerinţe tehnice şi organizatorice pentru protecţia împotriva software-ului maliţios. - Defineşte cerinţe pentru efectuarea copiilor de siguranţă care să asigure protecţia împotriva pierderii datelor - Defineşte cerinţe privind jurnalizare şi monitorizarea, care să asigure înregistrarea evenimentelor relevante şi generarea de dovezi. - Defineşte cerinţe privind controlul software-ului operaţional, care să asigure integritatea sistemelor operaţionale. - Defineşte cerinţe privind managementul vulnerabilităţilor tehnice, care să prevină	3	4

						exploatarea acestora. - Defineşte cerinţe privind auditul sistemelor informatice, care să minimizeze impactul auditurilor asupra sistemelor operaţionale. - Defineşte cerinţe privind managementul securităţii reţelelor, care să asigure protecţia informaţiilor din reţele, pe baza bunelor practici definite în standardele internaţionale ISO/IEC 27002 şi ISO/IEC 27035. - Defineşte cerinţe privind securitatea informaţiilor transferate între organizaţie şi entităţi externe. - Defineşte cerinţe pentru managementul mijloacelor criptografice, care să asigure utilizarea eficace a acestora pentru protejarea confidenţialităţii, autenticităţii şi/sau integrităţii informaţiei.		
		Securitate fizică	Zone sigure Securitatea echipamentelor	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte cerinţe privind securizarea locaţiilor relevante pentru securitate informaţiilor, care să prevină accesul neautorizat, deteriorarea sau interferenţa cu informaţia sau facilităţile de procesare ale informaţiei. - Defineşte cerinţe pentru prevenirea deteriorării,	1	2

						furtului sau compromiterii resurselor informaţionale şi întreruperea proceselor operaţionale.		
		Integrarea cerinţelor de securitate în contractele şi activităţile terţilor	Cerinţe de securitate în contractele cu terţi Managementul serviciilor externalizate	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Identifică şi integrează cerinţele de securitate în contractele şi activităţile efectuare de terţi (parteneri, furnizori, clienţi) pentru menţinerea obiectivelor de securitate. - Defineşte reguli privind managementul serviciilor externalizate pentru asigura păstrarea nivelurilor agreate de prestare a serviciilor şi de securitate.	1	4
5.	**Implementarea sistemului de management al securităţii informaţiilor**	Definirea şi urmărirea planului de acţiuni în domeniul securităţii informaţiei.	Definirea planului de acţiuni în domeniul securităţii. Planificarea şi controlul operaţional. Documentaţia Sistemului de Management al Securităţii Informaţiei.	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte şi menţine planul de acţiuni în domeniul securităţii informaţiilor. - Coordonează şi monitorizează participarea proceselor de business (resurse umane, IT, achiziţii, etc.) la realizarea planului de acţiuni. - Identifică, defineşte cerinţe, achiziţionează şi gestionează resursele interne şi externe necesare pentru implementarea planului de acţiuni. - Gestionează executarea activităţilor de securitate planificate. - Defineşte, comunică şi menţine reguli, proceduri, ghiduri şi alte documente	2	4

						necesare pentru asigurarea conformităţii cu politicile de securitate a informaţiei aprobate.		
		Managementul incidentelor	Managementul incidentelor de securitate a informaţiilor. ISO/IEC 27035 Identificarea, colectarea şi păstrarea dovezilor digitale; standardul ISO/IEC 27037	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte responsabilităţi şi proceduri, în conformitate cu bunele practici descrise în standardele internaţionale ISO/IEC 27002 şi ISO/IEC 27035, care asigură un răspuns rapid, ordonat şi eficace la evenimentele de securitate a informaţiei. - Defineşte criterii pentru evaluarea evenimentelor şi identificarea incidentelor de securitate. - Defineşte mecanisme pentru învăţarea din incidente - Defineşte mecanisme pentru identificarea, colectarea, achiziţia şi păstrarea informaţiilor ce pot fi folosite ca dovezi, în conformitate cu bunele practici definite în standardele internaţionale.	4	4
		Aspecte de managemental continuităţii in cadrul SMSI	-	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Determină cerinţele pentru securitatea informaţiei derivate din cerinţele pentru continuitatea activităţii organizaţiei. - Defineşte şi documentează procese, proceduri şi măsuri pentru a asigura menţinerea nivelului de continuitate pentru securitatea informaţiei	2	8

						cerut în situaţii adverse. - Defineşte procese de evaluare, testare şi revizuire a planurilor de continuitate.		
6.	**Monitorizare, evaluare, îmbunătăţire**	Evaluarea securităţii informaţiilor	Monitorizare, măsurare, analiză şi evaluare – cerinţele ISO/IEC 27001:2013 ISO/IEC 27004 – Măsurare Analiza efectuată de management	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Defineşte, monitorizează şi raportează indicatori de performanţă de management şi operaţionali pentru evaluarea eficacităţii şi eficienţei sistemului de management - Redactează agenda analizei efectuate de management cu includerea tuturor elementelor relevante.	4	8
		Auditul intern	Cerinţe privind auditul sisstemului de management al informaţiei: - ISO/IEC 27007 - ISO/IEC 27008	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop • videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	- Planifică activităţile de audit, în conformitate cu cerinţele ISO/IEC 27001:2013 şi îndrumările ISO/IEC 27008 - Identifică riscurile şi neconformităţile cu cerinţele aplicabile, utilizând metodele descrise de standardele ISO/IEC 27007 şi ISO/IEC 27008. - Identifică acţiuni corective şi preventive - Urmăreşte eficacitatea acţiunilor corective - Determină eficacitatea procesului de audit	8	16
		Managementul acţiunilor de îmbunătăţire	Îmbunătăţirea continuă a SMSI	Prezentare, dezbatere, exerciţii, studii de caz	• suport de curs • prezentare • resurse web • laptop	- Defineşte planul de acţiuni corective, pe baza rezultatelor activităţilor de management al riscului,	3	6

					• videoproiector • reprezentări grafice, scheme • organizaţie exemplu • standarde şi normative.	monitorizare şi evaluare, audit, management al incidentelor de securitate, managementul schimbărilor, şi al oricăror activităţi care pot duce la oportunităţi de îmbunătăţire a adecvării şi eficacităţii sistemului de management. - Urmăreşte implementarea şi eficacitatea acţiunilor corective/ preventive.		