Occupational standard project for the Project CB-36 ITSVET

Deliverable D.T.2.5.1. - Occupational standard project in Latvian

Prepared by: **Inta Klotiņa,**

Title: **RTK, Project manager**

Address: 16 Braslas Street, Riga, LV-1084, Latvia

Phone: +372 67081400

E-mail: inta.klotina@rtk.lv

Contributors: **Ainis Mūsiņš, Nadežda Semjonova, Māra Jākobsone, Andris Jaunkalns**

Last revised: 31.08.2016

PROFESIJAS STANDARTS

PROJEKTS (3. versija)

IKT drošības speciālists

Koledžas līmeņa izglītība

Eiropas kvalifikāciju sistēmas līmenis: 5

Valsts kvalifikācijas līmeņi:

Latvija: 5 (1. līmeņa profesionālā augstākā izglītība)

Igaunija: 5

Somija: 5

A daļa

AMATA APRAKSTS

A.1. Amata apraksts
IKT drošības speciālists īsteno organizācijas IKT drošības politiku. Piedāvā un ievieš nepieciešamās drošības kontroles. Konsultē, atbalsta un informē, lai garantētu drošu IKT darbību. Veic tiešas darbības, lai padarītu drošu visu vai daļu no tīkla vai IKT sistēmām. Kolēģu vidū tiek atzīts par IKT tehniskās drošības ekspertu. IKT drošības speciālista profesiju veido šādi uzdevumi: • Novērot ar IKT drošību saistītas tehnoloģiju attīstības tendences • Izveidot informācijas drošības zināšanu bāzi • Sniegt priekšlikumus jaunu tehnoloģiju integrēšanā • Veikt nepieciešamās drošības pārbaudes un atjaunināšanu • Izvēlēties un izmantot drošības līdzekļus • Kontrolēt un veikt IKT drošības novērtējumus, testus, apskates un auditus • Kontrolēt IKT resursu drošību un novērtēt IKT drošības riskus • Testēt IKT nepārtrauktības plānu • Rūpēties par organizācijas IKT drošības sistēmu atbilstību likumam, regulām, noteikumiem, procedūrām un dokumentācijai Kiberdrošības speciālists parasti strādā uzņēmumos, kur IKT sistēmas veido ievērojamu daļu no uzņēmuma aktīviem; biznesa procesi ir balstīti uz IKT sistēmām un rīkiem; komercinformācija tiek savākta un apstrādāta, izmantojot IKT sistēmas. 5. līmeņa kiberdrošības speciālists strādā ar dažādām IKT sistēmām un rīkiem. Viņš/viņa uzrauga

kolēģus un, ja nepieciešams, arī nelielu darba komandu.
A.2. Pozīcijas
5. līmeņa IKT drošības speciālista profesionālajā kvalifikācijā iekļautas 15 pozīcijas: 1. Lietotņu izstrāde (e-CF A6) 2. Tehnoloģiju attīstības tendenču pārraudzīšana (e-CF A7) 3. Komponentu integrācija (e-CF B2) 4. Testēšana (e-CF B3) 5. Risinājumu izvietošana (e-CF B4) 6. Dokumentācijas izstrāde (e-CF B5) 7. Lietotāju atbalsts (e-CF C1) 8. Atbalsts izmaiņu gadījumā (e-CF C2) 9. Pakalpojuma sniegšana (e-CF C3) 10. Problēmu pārvaldība (e-CF C4) 11. Informācijas drošības stratēģijas izstrāde (e-CF D1) 12. Personāla attīstība (e-CF D9) 13. Risku pārvaldība (e-CF E3) 14. Attiecību pārvaldība (e-CF E4) 15. Informācijas drošības pārvaldība (e-CF E8)
A.3. Darba vide un specifiski darba aspekti
5. līmeņa kiberdrošības speciālists darbojas vidē, kurā tehnoloģijas mainās ļoti strauji. Nepārtraukti tiek radīti jauni rīki un jauni draudi. Speciālistam jābūt gatavam visā profesionālās karjeras laikā attīstīt savas prasmes, kā arī apmācīt kolēģus, klientus, partnerus.
A.4. Instrumenti
Operētājsistēmas, drošības programmatūra, procesu apraksta un izstrādes rīki, programmatūru izstrādes rīki
A.5. Darbam nepieciešamās personiskās īpašības: spējas un raksturiezīmes
Kiberdrošības speciālista darbā nepieciešama loģiskā domāšana, spēja analizēt, koncentrēties, strādāt metodiski, jābūt rūpīgam, jāievēro un jāpārzina aktuālie standarti, paņēmieni, procedūras un metodes.
A.6. Profesionālā apmācība
Profesionālie kursi, konferences, pašmācība, e-mācības, sertifikācijas eksāmeni kvalifikācijas uzturēšanai.
A.7. Iespējamie amata nosaukumi
Kiberdrošības speciālists, IKT drošības speciālists, IKT drošības darbinieks, IKT drošības konsultants, kiberdrošības konsultants, incidentu pārvaldītājs, aizsardzības pārvaldītājs, testētājs.

B daļa.

KOMPETENCES PRASĪBAS

B.1. Profesionālās kvalifikācijas struktūra
Piesakoties 5. līmeņa kiberdrošības speciālista profesijas kvalifikācijai, jāpiemēro šādas novērtējuma metodes:

Gala darba vai pēdējā eksāmena saturu un kārtošanas veidu apstiprina profesionālās kvalifikācijas piešķiršanas komisija.
Novērtēšanas metodes specifika:
Sākotnējā 5. līmeņa kiberdrošības speciālista profesijas kvalifikācija tiek iegūta, pabeidzot atbilstošus izglītības kursus, nokārtojot gala eksāmenu un/ vai aizstāvot noslēguma darbu.

B.2. kompetences

B.2.1. **IKT risinājumu izstrāde** (e-CF A6)

Analizē, nosaka, atjaunina un padara pieejamu IKT risinājumu ieviešanas modeli, kas ir saskaņā ar informācijas drošības politiku un atbilst lietotāja/klienta vajadzībām. Nodrošina, ka visos aspektos tiek ņemta vērā sadarbspēja, lietojamība un drošība.

Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Piedalās izstrādē un vispārēju funkcionālu specifikāciju un saskarņu veidošanā. Ir iepriekšējas zināšanas par drošas infrastruktūras metodoloģiju. Ir iepriekšējas IKT drošības standartu zināšanas .	a) prasību modelēšanas un vajadzību analīzes paņēmienus b) risinājumu izstrādes metodes un to pamatojumu (piemēram, prototipēšana, spējās metodes, reversā inženierija utt.) c) mobilās tehnoloģijas d) apdraudējumu modelēšanas paņēmienus e) drošu datu centru izstrādes pamatus f) drošu serveru izstrādes pamatus g) drošu krātuvju izstrādes pamatus h) drošu tīklu izstrādes pamatus	a) identificēt klientus, lietotājus un ieinteresētās puses b) savākt, noformēt un validēt funkcionālas un nefunkcionālas prasības c) novērtēt prototipu izmantošanu, lai veicinātu prasību validēšanu d) veidot sistemātisku un biežu komunikāciju ar klientiem, lietotājiem un ieinteresētajām pusēm e)

B.2.2. **Tehnoloģiju attīstības tendenču pārraudzīšana** (e-CF A7)

Pēta jaunākos IKT tehnoloģijas sasniegumus, lai veidotu izpratni par jaunām tehnoloģijām. Izstrādā novatoriskus risinājumus jaunu tehnoloģiju integrēšanai produktos, lietotnēs vai pakalpojumos vai veido jaunus risinājumus, ievērojot drošības pasākumus.

Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Izmanto zināšanas par jaunām un nākotnes tehnoloģijām un izpratni par biznesu, lai paredzētu un formulētu, kādus risinājumus izmantot nākotnē. Sniedz vadībai IKT drošības speciālista ieteikumus un padomus, lai nodrošinātu atbalstu stratēģisku lēmumu pieņemšanā.	a) nākotnes tehnoloģijas un tām atbilstošu izmantošanu tirgū b) atbilstošus informācijas avotus (piemēram, žurnāli, konferences un pasākumi, informatīvie biļeteni, vadošie speciālisti, tiešsaistes forumi utt.) c) diskusiju noteikumus	a) pārraudzīt informācijas avotus un nepārtraukti sekot daudzsološākajiem no tiem b) identificēt labākos risinājumu piegādātājus un pakalpojumu sniedzējus; novērtēt, pamatot un ieteikt piemērotāko

	tiešsaistes kopienās	
B.2.3. **Komponentu integrācija** (e-CF B2)		
Integrē aparatūru, programmatūru vai apakšsistēmu komponentus jau esošā vai jaunā sistēmā. Ievēro noteiktos procesus un procedūras, piemēram, konfigurācijas pārvaldību un programmatūras uzturēšanu. Ņem vērā esošo un jauno moduļu saderību, lai nodrošinātu sistēmas integritāti, sistēmas sadarbspēju un informācijas drošību. Verificē un pārbauda sistēmas noslodzi un veiktspēju; dokumentē veiksmīgu integrāciju.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Sistemātiski rīkojas, lai identificētu programmatūras un aparatūras specifikāciju saderību. Dokumentē visas instalēšanas laikā veiktās darbības un reģistrē novirzes un koriģējošās darbības. Ievēro atbilstošos drošības standartus un izmaiņu kontroles procedūras, lai saglabātu sistēmas funkcionalitātes un uzticamības integritāti.	a) novecojušas, esošas un jaunas aparatūras komponentus/ programmatūru/ moduļus b) sistēmas integrēšanas ietekmi uz esošo sistēmu/ organizāciju c) paņēmienus saskarnes veidošanai starp moduļiem, sistēmām un komponentiem d) integrēšanas pārbaudes paņēmienus e) izstrādes rīkus (piemēram, izstrādes vide, pārvalde, pirmkoda piekļuves/versiju kontroli	a) noteikt sistēmas veiktspēju pirms un pēc sistēmas integrēšanas un arī tās laikā b) dokumentēt un reģistrēt darbības, problēmas un ar tām saistītus labojumus c) atrast klientu vajadzībām atbilstošus produktus d) pārliecināties, ka integrētās sistēmas spējas un efektivitāte atbilst specifikācijai e) aizsargāt/ dublēt datus, lai sistēmas integrēšanas laikā nodrošinātu integritāti
B.2.4. **Testēšana** (e-CF B3)		
Izveido un izpilda sistemātiskas IKT sistēmas vai klientu lietojamības prasību testēšanas procedūras, lai tiktu ievērotas projekta specifikācijas. Nodrošina, ka jauni vai laboti komponenti vai sistēmas darbojas, kā paredzēts. Nodrošina, ka tiek ievēroti iekšējie, ārējie, valsts un starptautiskie standarti; tai skaitā veselības aizsardzības un drošības, lietojamības, veiktspējas, uzticamības un saderības standarti. Izstrādā dokumentus un ziņojumus, kas apliecina sertifikācijas prasību izpildi.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Veic vienkāršus testus, stingri ievērojot detalizētas instrukcijas. Organizē testēšanas programmas un veido skriptus, lai veiktu iespējamo vājo vietu spriedzes testus. Reģistrē iznākumus un ziņo par tiem, sniedzot rezultātu analīzi. Nodrošina, ka testi un rezultāti tiek dokumentēti, lai sniegtu ieskatu turpmākajiem procesa īpašniekiem, piemēram, projektētājiem, lietotājiem vai uzturētājiem. Ir atbildīgs par testēšanas procedūru, tai skaitā	a) paņēmienus, infrastruktūru un rīkus, kurus izmantot testēšanas procesā b) testēšanas procesa dzīves ciklu c) dažādu veidu testus (funkcionāli, integrācijas, veiktspējas, lietojamības, spriedzes utt.) d) valsts un starptautiskos standartus, kas nosaka testēšanas kvalitātes kritērijus e) tīmekļa, mākoņa un	a) izveidot un pārvaldīt testēšanas plānu b) pārvaldīt un novērtēt testēšanas procesu c) dokumentēt testus un rezultātus un ziņot par tiem d) pārbaudīt izmaiņas e) ieviest un pārbaudīt atsaukšanas procedūras

dokumentētas revīzijas izsekojamības principa, ievērošanu.	mobilo tehnoloģiju un vides prasības f) nepieciešamību testēt izmaiņas, ziņot par izmaiņām un atsaukšanas plāniem	
B.2.5. **Risinājumu izvietošana** (e-CF B4)		
Sekojot iepriekš noteiktiem vispārējiem prakses standartiem, veic ieplānotas un nepieciešamas iejaukšanās darbības, lai ieviestu risinājumu, tai skaitā instalēšanu, atjaunināšanu vai ekspluatācijas pārtraukšanu. Konfigurē aparatūru, programmatūru vai tīklu, lai nodrošinātu sistēmas komponentu sadarbspēju un atkļūdo visus radušos defektus vai nesaderību. Ja nepieciešams, izmanto papildu speciālistu resursus, piemēram, trešās puses tīkla operatorus. Formāli nodod lietotājam pilnībā darboties spējīgu risinājumu un aizpilda dokumentāciju, reģistrējot visu atbilstošo informāciju, tai skaitā aprīkojuma adreses, konfigurācijas un veiktspējas datus.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Sistemātiski rīkojas, lai izstrādātu vai likvidētu sistēmas elementus. Identificē kļūdainus komponentus un nosaka kļūmju pamatcēloņus. Sniedz atbalstu mazāk pieredzējušiem kolēģiem.	a) veiktspējas analīzes paņēmieni b) ar problēmu pārvaldību saistītus paņēmienus (darbība, veiktspēja, saderība) c) programmatūras iepakošanas un izplatīšanas metodes un paņēmienus d) esošās arhitektūras ietekmi uz izvietošanu e) izvietošanas laikā izmantojamās tehnoloģijas un standartus f) tīmekļa, mākoņa un mobilo tehnoloģiju un vides prasības	a) organizēt un plānot beta testa darbības, testēšanas risinājumu gatavajā operatīvajā vidē b) konfigurēt komponentus jebkurā līmenī, lai garantētu pareizu sadarbspēju c) identificēt un veikt ekspertīzi, kas nepieciešama sadarbspējas problēmu risināšanai d) organizēt un kontrolēt sākotnējo atbalsta pakalpojumu nodrošināšanu, tai skaitā lietotāju apmācību sistēmas palaides laikā e) organizēt datubāžu aizpildīšanu un pārvaldīt datu migrāciju f) sadarboties, lai modificētu trešās puses kodu; atbalstīt un uzturēt modificēto programmatūru
B.2.6. **Dokumentācijas izstrāde** (e-CF B5)		
Izstrādā dokumentus, kuros aprakstīti produkti, pakalpojumi, komponenti vai lietotnes, tā, lai tiktu ievērotas atbilstošās dokumentācijas prasības. Izvēlas atbilstošo prezentācijas materiālu stilu un līdzekļus. Izstrādā dokumentu pārvaldības sistēmu veidnes. Nodrošina, ka funkcijas un līdzekļi tiek atbilstoši dokumentēti. Nodrošina, ka esošie dokumenti ir derīgi un atjaunināti.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Nosaka dokumentācijas prasības,	a) dažādus tehniskos	a) novērot un efektīvi

ņemot vērā tās pielietojuma mērķi un vidi. Piemēro detalizācijas pakāpi saskaņā ar dokumentācijas mērķi un mērķauditoriju.	dokumentus, kas nepieciešami produktu, lietotņu un pakalpojumu izstrādei, pilnveidošanai un izvietošanai b) produktu versiju kontroles dokumentāciju c) organizācijas drošības dokumentāciju	izmantot uzņēmuma publikāciju standartus b) uz visu dzīves ciklu saglabāt risinājumam pielīdzinātas publikācijas c) uzturēt atjauninātu organizācijas drošības dokumentāciju

B.2.7. **Lietotāju atbalsts** (e-CF C1)

Atbild uz lietotāju prasībām un problēmām, reģistrējot atbilstošo informāciju. Nodrošina atrisinājumu vai eskalē incidentus un optimizē sistēmas veiktspēju saskaņā ar iepriekš noteiktiem pakalpojuma līmeņa līgumiem (PLL). Izprot, kā kontrolēt risinājuma iznākumu un no tā izrietošo klienta apmierinātību.

Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Sistemātiski interpretē lietotāju problēmas un identificē risinājumus un iespējamās blakusparādības. Izmanto pieredzi, lai risinātu lietotāja problēmas, un pārlūko datubāzi, meklējot iespējamos risinājumus. Eskalē sarežģītus vai neatrisinātus incidentus. Reģistrē problēmu un izseko tai no rašanās brīža līdz atrisināšanai.	a) atbilstošas IKT lietotāja lietotnes b) datubāžu struktūras un satura organizāciju c) uzņēmuma eskalēšanas procedūras d) programmatūras izplatīšanas metodes un procedūras labojumu pielietojuma un datņu pārraides metodoloģijai, kas attiecas uz programmatūras labojumiem e) iespējamo risinājumu informācijas avotus	a) efektīvi uzdot jautājumus lietotājiem, lai noskaidrotu simptomus b) analizēt simptomus, lai identificētu lietotāja kļūdas vai tehniskas kļūmes aptuveno veidu c) izmantot atbalsta rīkus, lai sistemātiski izsekotu kļūdas vai tehniskas kļūmes avotu d) skaidri komunicēt ar gala lietotājiem, lai sniegtu instrukcijas par to, kā rīkoties problēmu gadījumā e) reģistrēt un kodēt problēmas, lai veicinātu tiešsaistes atbalsta rīku attīstību un integritāti

B.2.8. **Atbalsts izmaiņu gadījumā** (e-CF C2)

Ievieš un vada IKT risinājuma attīstību. Nodrošina efektīvu kontroli un programmatūras vai aparatūras izmaiņu plānošanu, lai novērstu vairāku atjauninājumu neparedzētu iznākumu. Minimizē izmaiņu rezultātā radušos pārtraukumu pakalpojumu sniegšanā un ir saskaņā ar pakalpojuma līmeņa līgumu (PLL). Nodrošina to, ka informācijas drošības procedūras tiek ņemtas vērā un ievērotas.

Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Izmaiņu laikā sistemātiski rīkojas, lai atbildētu uz ikdienas operatīvajām vajadzībām un reaģētu uz tām, izvairoties no pārtraukuma pakalpojuma sniegšanā un ievērojot PLL un informācijas drošības prasības.	a) informācijas sistēmas funkcionālo specifikāciju b) esošās IKT lietotnes tehnisko struktūru c) kā tiek integrēti biznesa procesi un to atkarību no IKT lietotnēm d) izmaiņu pārvaldības	a) dalīties funkcionālā un tehniskā specifikācijā ar IKT komandām, kas atbild par IKT risinājumu uzturēšanu un attīstību b) pārvaldīt komunikāciju ar IKT komandām, kas atbild par informācijas sistēmu risinājumu uzturēšanu un attīstību

	rīkus un paņēmienus e) labāko informācijas drošības pārvaldes praksi un standartus	c) analizēt funkcionālo/tehnisko izmaiņu ietekmi uz lietotājiem d) paredzēt visas darbības, kas nepieciešamas, lai mazinātu izmaiņu ietekmi (apmācības, dokumentācija, jauni procesi...) e) novērtēt ar izmaiņām saistītos iespējamos riskus
B.2.9. **Pakalpojuma sniegšana** (e-CF C3)		
Nodrošina pakalpojuma sniegšanu saskaņā ar noteiktiem pakalpojuma līmeņa līgumiem (PLL). Veic proaktīvas darbības, lai nodrošinātu stabilas un drošas lietotnes un IKT infrastruktūru, lai izvairītos no iespējamiem pārtraukumiem pakalpojuma sniegšanā, rūpējoties par noslodzes plānošanu un informācijas drošību. Atjaunina operatīvo dokumentu bibliotēku un reģistrē visus pakalpojuma sniegšanas incidentus. Uztur pārraudzības un pārvaldes rīkus (t.i. skriptus, procedūras). Uztur informācijas drošības pakalpojumus. Veic proaktīvus pasākumus.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Rīkojas saskaņā ar norādījumiem, lai reģistrētu un izsekotu uzticamības datus. Sistemātiski analizē veiktspējas datus un ziņo vecākajiem ekspertiem par atklājumiem. Eskalē iespējamās servisa līmeņa kļūmes un drošības riskus, iesaka darbības, lai uzlabotu pakalpojuma uzticamību. Izseko uzticamības datus un salīdzina tos ar PLL.	a) kā interpretēt IKT pakalpojuma sniegšanas prasības b) labāko IKT pakalpojumu sniegšanas praksi un standartus c) kā pārraudzīt pakalpojuma sniegšanu d) kā reģistrēt pakalpojuma sniegšanas darbības un spēt identificēt kļūmes e) labāko informācijas drošības pārvaldes praksi un standartus f) tīmekļa, mākoņa un mobilās tehnoloģijas	a) lietot procesus, kas veido organizācijas IKT pakalpojuma sniegšanas stratēģiju b) aizpildīt un nodrošināt dokumentāciju, kas izmantota IKT pakalpojuma sniegšanā c) analizēt pakalpojuma sniegšanas nodrošināšanu un ziņot vecākajiem kolēģiem par iznākumu d) plānot un lietot darbaspēka darba slodzi/prasības efektīvai un izdevīgai pakalpojuma sniegšanai e) ieviest dažādus drošības pasākumus f) novērtēt dažādu drošības pasākumu ieviešanu g) novērtēt tīkla darbības h) konfigurēt telesakaru ierīces i) analizēt tīkla darbības j) identificēt šifrēšanas nepieciešamību k) pierādīt šifrēšanas ieviešanas nepieciešamību l) novērtēt izmantoto šifrēšanu
B.2.10. **Problēmu pārvaldība** (e-CF C4)		
Identificē un novērš incidentu pamatcēloni. Veic proaktīvas darbības, lai novērstu vai identificētu IKT		

problēmu pamatcēloni. Izmanto zināšanu sistēmu, kas balstīta uz plaši izplatītu kļūdu atkārtošanos. Atrisina vai eskalē incidentus. Optimizē sistēmas vai komponenta veiktspēju.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Identificē un klasificē incidentu veidus un traucējumus pakalpojuma sniegšanā. Reģistrē incidentus, ievietojot tos katalogā pēc simptoma un risinājuma.	a) organizācijas kopējo IKT infrastruktūru un galvenos komponentus b) organizācijas ziņošanas procedūras c) organizācijas kritisku situāciju eskalēšanas procedūras d) diagnostikas rīku lietojumu un pieejamību e) saikni starp sistēmas infrastruktūras elementiem un kļūmes ietekmi uz biznesa procesiem, kas ir saistīti ar tiem f) organizācijas informāciju, kas var būt drošības incidentu mērķis	a) pārraudzīt problēmu progresu visā dzīves ciklā un efektīvi komunicēt b) identificēt iespējamas kritiskas komponentu kļūmes un veikt darbības, lai mazinātu kļūmes efektus c) veikt riska pārvaldības revīzijas un rīkoties, lai minimizētu risku d) novērtēt iespējamos problēmas radītos bojājumus e) noteikt prioritātes gadījumā, ja vienlaicīgi ir vairāk nekā viens incidents
B.2.11. **Informācijas drošības stratēģijas izstrāde** (e-CF D1)		
Definē un padara piemērojamu formālu organizatorisko stratēģiju, darbības lauku un kultūru, lai aizsargātu informāciju no ārējiem un iekšējiem draudiem, t.i., digitālā ekspertīze uzņēmuma iekšējā izmeklēšanā vai ielaušanās izmeklēšana. Nodrošina informācijas drošības pārvaldības pamatu, tai skaitā lomu identifikāciju un atbildību. Izmanto noteiktus standartus, lai veidotu informācijas integritātes, pieejamības un datu konfidencialitātes mērķus.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Izmanto padziļinātu ekspertīzi un gūst labumu no ārējiem standartiem un labākajām praksēm. Vada drošības vadlīniju izstrādi/piedalās drošības vadlīniju izstrādē. Vada drošības instrukciju izstrādi/piedalās drošības instrukciju izstrādē.	a) atbilstošo standartu un labāko prakšu potenciālu un iespējas b) tiesisko prasību ietekmi uz informācijas drošību c) organizācijas informācijas stratēģiju d) iespējamos drošības draudus e) mobilitātes stratēģiju f) dažādus pakalpojuma modeļus (SaaS, PaaS, IaaS) un darbības formas (t.i. mākoņdatošana)	a) attīstīt un kritiski analizēt uzņēmuma informācijas drošības stratēģiju b) definēt, iesniegt un veicināt informācijas drošības politikas apstiprināšanu no organizācijas augstākās vadības puses
B.2.12. **Personāla attīstība** (e-CF D9)		
Diagnosticē individuālo un grupu kompetenci, identificējot nepieciešamās un trūkstošās prasmes. Apskata apmācības un attīstības iespējas un izvēlas piemērotu metodoloģiju, ņemot vērā		

individuālās, projekta un biznesa prasības. Trenē un/ vai sniedz padomus personām vai komandām apmācību nolūkā.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Informē/apmāca personas un grupas, vada apmācību kursus. Pārrauga personu un komandu attīstības vajadzības un rīkojas saskaņā ar tām.	a) mācīšanās un attīstības atbalsta metodes (piemēram, trenēšana, mācīšana)	a) identificēt kompetenču un prasmju trūkumu b) identificēt un ieteikt uz darbu balstītas attīstības iespējas c) rutīnas darba procesos iekļaut prasmju attīstības iespējas
B.2.13. **Riska pārvaldība** (e-CF E3)		
Ievieš riska pārvaldību visās informācijas sistēmās, izmantojot uzņēmuma definēto riska pārvaldības politiku un procedūru. Novērtē organizācijas biznesa risku, tai skaitā tīmekļa, mākoņa un mobilo resursu risku. Dokumentē iespējamo risku un tā ierobežošanas plānus. Izprot un piemēro riska pārvaldības principus un izpēta IKT risinājumus, lai mazinātu identificētos riskus		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Izprot un piemēro riska pārvaldības principus un izpēta IKT risinājumus, lai mazinātu identificētos riskus. Nosaka atbilstošas darbības, kas nepieciešamas, lai pielāgotu drošību un mazinātu riskantumu. Novērtē, uztur un nodrošina izņēmumu validēšanu; veic IKT procesu un vides revīziju.	a) kā lietot risku analīzi, ņemot vērā uzņēmuma vērtības un intereses b) ieguldījumu atdevi salīdzinājumā ar riska nepieļaušanu c) labo praksi (metodoloģijas) un standartus risku analīzē	a) izstrādāt riska pārvaldības plānu, lai identificētu nepieciešamās profilakses darbības b) komunicēt un veicināt organizācijas risku analīzes iznākumus un risku pārvaldības procesus c) izstrādāt un dokumentēt risku analīzes un pārvaldības procesus d) veikt ietekmi mazinošas un sistēmas rīcībspējas nodrošināšanas darbības e) pārraudzīt drošības kontroles f) pievienot rādītājus, lai novērtētu drošības kontroles
B.2.14. **Attiecību pārvaldība** (e-CF E4)		
Izveido un saglabā pozitīvas biznesa attiecības starp ieinteresētajām pusēm (iekšējām vai ārējām), izmantojot un ievērojot organizatoriskos procesus. Uztur regulāru komunikāciju ar klientu/ partneri / piegādātāju, un ir empātiski vajadzību izpildē, izmantojot vidi un pārvaldot piegādes ķēdes komunikāciju. Nodrošina, ka ieinteresēto pušu vajadzības, bažas un sūdzības tiek izprastas un risinātas saskaņā ar organizatorisko politiku.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Atbild par savām un citu darbībām, pārvaldot ierobežotu	a) organizācijas procesus, tai skaitā lēmumu	a) ar empātisku attieksmi pildīt klientu vajadzības

skaitu ieinteresēto pušu. Komunicē ar personālu. Sniedz visiem darbiniekiem nepieciešamo drošības informāciju. Pēc pieprasījuma sniedz nepieciešamo drošības informāciju.	pieņemšanu, budžetu un pārvaldības struktūru b) paša un citu ieinteresēto pušu uzņēmējdarbības mērķus c) kā noteikt un izmantot resursus, lai tiktu izpildītas ieinteresēto pušu prasības d) uzņēmējdarbības izaicinājumus un riskus	b) noteikt reālus sagaidāmos rezultātus, lai veicinātu savstarpējās uzticēšanās veidošanos c) informēt par labām un sliktām ziņām, lai izvairītos no pārsteigumiem d) ziņot par drošības prasībām citiem departamentiem e) izskaidrot drošības darbību nepieciešamību
B.2.15 **Informācijas drošības pārvaldība** (e-CF E8)		
Ievieš informācijas drošības politiku. Pārrauga un veic darbības pret ielaušanos, krāpniecību un drošības pārkāpumiem vai informācijas noplūdi. Nodrošina, ka tiek analizēti un pārvaldīti drošības riski uzņēmuma datu un informācijas jautājumos. Pārskata drošības incidentus, pauž ieteikumus par drošības politiku un stratēģiju, lai nodrošinātu nepārtrauktu drošības normu uzlabošanu.		
Apraksts	Papildu zināšanas Zina:	Prasmes Spēj:
Sistemātiski pārrauga vidi, lai identificētu un definētu vājās vietas un draudus. Reģistrē un eskalē neatbilstības. Novērtē drošības pārvaldības pasākumus un indikatorus un nolemj, vai tie atbilst informācijas drošības politikai. Izpēta un ievieš korektīvus pasākumus, lai novērstu jebkādus drošības pārkāpumus.	a) organizācijas drošības pārvaldības politiku un tās ietekmi saziņā ar klientiem, piegādātājiem un apakšuzņēmējiem b) labāko informācijas drošības pārvaldības praksi un standartus c) kritiskos informācijas drošības pārvaldības riskus d) IKT iekšējās revīzijas pieeju e) drošības problēmu atklāšanas paņēmienus, tai skaitā mobilus un digitālus f) kiberuzbrukumu paņēmienus un pasākumus, lai no tiem izvairītos g) datortehnisko ekspertīzi h) drošības struktūras principus i) pierādījumu dzīves cikla pamatus j) pierādījumu savākšanas pamatus k) tīmekļa, mākoņa un mobilo tehnoloģiju un vides prasības	a) dokumentēt informācijas drošības pārvaldības politiku, veidojot saikni starp to un uzņēmējdarbības stratēģiju b) analizēt uzņēmuma nozīmīgos aktīvus un identificēt to trūkumus un vietas, kuras nav pilnībā aizsargātas pret ielaušanos vai uzbrukumu c) izstrādāt risku pārvaldības plānu, lai pievienotu un izveidotu profilakses darbības plānus d) veikt drošības revīzijas e) izmantot pārraudzības un testēšanas paņēmienus f) izstrādāt atjaunošanas plānu g) krīzes gadījumā īstenot atjaunošanas plānu

	l) organizācijas resursu vājās vietas	

B.2.16. **STARPDISCIPLINĀRĀS PRASMES UN KOMPETENCES**
1. Komunikācija
2. Sadarbība
3. Iniciatīva un radošums
4. Plānošanas un organizēšanas darbs
5. Problēmu risināšana
6. Mācīšanās mācīties
7. Rakstpratība un valodu zināšanas
8. Informācijas pārvaldība
9. Personīgā attieksme un vērtības (pašdisciplīna, godīgums, atklātums, rūpība)