

## Kursuseprogrammi vorm

Ainekood IFI7085.DT	NIMETUS IT riskijuhtimine		
Maht EAP 4.0	Kontaktundide maht: 16	Õppesemester: S	Eksam/Arvestus Arvestus
Eesmärk:	Vastavalt infotehnoloogia juhi kutsestandardile kuulub IT juhi põhioskuste ja –teadmiste hulka kõrgtasemel infoturbe põhimõtete tundmine. Kursuse eesmärgiks on anda ülevaade rahvusvaheliselt tunnustatud IT riskijuhtimise standarditest ja headest tavadest ning näidata, kuidas neid praktikas rakendada. Samuti aitab kursus selgitada IT riskijuhtimist kui pidevat protsessi, selle protsessi eesmärke ja vajalikkust ning seotust teiste juhtimistegevustega, sh strateegilise juhtimisega, IT juhtimisega ja infoturbe haldamisega.		
Aine lühikirjeldus:  (sh iseseisva töö sisu kirjeldus vastavuses iseseisva töö mahule)	<p>IT riskijuhtimise kursus baseerub IT riskijuhtimise standarditel ja headel tavadel ning seostel teiste infoturbe juhtimissüsteemidega (ISMS – Information Security Management Systems). Kursusel läbitavate teemadena käsitletakse ISO 27005 standardit, IT riskijuhtimise organisatsiooni ja protsesse ning IT riskijuhtimise tegevusi. Konkreetsemate IT riskijuhtimise tegevuste hulka kuuluvad riskide jälgimine, riskide hinnastamine ja meetmete hinnastamine, IT monitooring, infoturbe intsidentide haldus ja puudutatakse ka logide analüüsi ning tõendusmaterjalide haldust. Täiendavate teemadena leiavad kajastust kontrollide monitoorimine, IT teenuselepingute (SLA) haldus, riskikommunikatsioon, selgitatakse koolituse ja dokumenteerimise vajadus ja üldisemat riskikeskkonna seiret ning tutvustatakse riskipõhise auditeerimise põhiprintsiipe.</p> <p>Loengute käigus analüüsitakse praktilisi juhtumeid läbi riskistsenaariumite.</p>		
Õpiväljundid:	Üliõpilane on suuteline hindama organisatsiooni IT riske, välja töötama ja rakendama riskide juhtimise tegevusi ning analüüsima nende tegevuste mõju.		
Hindamismeetodid:	Arvestus – arvestuse saamiseks on vaja koostada nõuetele vastav iseseisev töö ning kaitsta seda seminaril.		
Õppejõud:	Hillar Põldmaa, MSc, CISA, CISM		
Ingliskeelne nimetus:	IT Risk Management		

Eeldusaine:	Puudub
Kohustuslik kirjandus:	ISKE riskide kataloog
Asenduskirjandus: (üliõpilase poolt läbi töötatava kirjanduse loetelu, mis katab ainekursuse loengulist osa)	COBIT 5 ISO 27005
Õppetöös osalemise ja eksamile/arvestusele pääsemise nõuded	Kursusel osalejatena on eelistatud infotehnoloogia juhtimise ja infoteaduse magistriõppe üliõpilased
Iseseisva töö nõuded	Iseseisev töö peab käsitlema riskihalduse kõiki etappe. Lõpptulemus esitatakse töö kaitsmisel. 20 minuti jooksul on vajalik esitada kõik olulised riskid ning nende vähendamise meetmed ning vähendamiseks vajalik ressurss. Soovitav on töö koostada reaalse asutuse näitel.
Eksami hindamiskriteeriumid või arvestuse sooritamiseks vajalik miinimumtase	Arvestuse sooritamiseks vajalik miinimumtase:  Arvestuse saamiseks on vaja koostada nõuetele vastav iseseisev töö ning kaitsa seda seminaril. Kaitsmisel välja toodud riskid on aktuaalsed ja põhjendatud. Riskide vähendamiseks pakutud meetmed vastavad riski olemusele. Töö kaitsmine on läbimõeldud ja ettevalmistatud. Üliõpilane esitab kaitsmisel hea ülevaate oma tööst.
Informatsioon kursuse sisu kohta, kursuse jaotumine teemade kaupa sh kontakttundide ajad	23.09.2017 k 10:00 – 4h - sissejuhatus, üldine riskihalduse protsess, riskihalduse standardid 18.11.2017 k 10:00 – 4h - riskide jälgimine, riskide hinnastamine, IT monitooring, infoturbe intsidentide haldus 02.12.2017 k 10:00 – 4h - riskistsenaariumite koostamine 16.12.2017 k 10:00 – 4h - vähendusmeetmete valik ja nende hinnastamine; - riskianalüüsi dokument, kui tervik.

Õppeainet kureeriv üksus:	Digitehnoloogiate instituut
Kursuseprogrammi koostaja	Hillar Põldmaa
Kuupäev:	21.08.2017

Kursuseprogramm registreeritud akadeemilises üksuses

Kuupäev	22.08.2017
Õppenõustaja ja -spetsialisti nimi	Ingrid Sander