IFI7085	**IT riskijuhtimine**		
Maht: 4 EAP	***Kontakttundide maht:*** 16	***Õppesemester:*** sügis	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)***	IT riskijuhtimise kursus baseerub IT riskijuhtimise standarditel ja headel tavadel ning seostel teiste infoturbe juhtimissüsteemidega (ISMS – Information Security Management Systems). Kursusel läbitavate teemadena käsiltetakse ISO 27005 standardit, IT riskijuhtimise organisatsiooni ja protsesse ning IT riskijuhtimise tegevusi. Konkreetsemate IT riksijuhitmise 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. Loengute käigus analüüsitakse praktilisi juhtumeid läbi riskistsenaariumite. Praktilise tööna koostavad üliõpilased kodutööd IT riskijuhtimise teemal konkreetse asutuse näitel ja kaitsevad seda seminaril.		
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:	Andro Kull PhD		
Aine ingliskeelne nimetus:	IT Risk Management		
Eeldusaine:	-		
Kohustuslik kirjandus:	Loengukonspekt, viited konkreetsete teemade kohta antakse loengute käigus.		
Asenduskirjandus:	Information Technology Risk Management in Enterprise		

(üliõpilase poolt läbi töötatava kirjanduse loetelu, mis katab ainekursuse loengulist osa)	Environments (Jake Kouns and Daniel Minoli); IT Risk: Turning Business Threats Into Competitive Advantage (George Westerman, Richard Hunter); The Risk IT Framework (ISACA).
Õppetöös osalemise ja eksamile / arvestusele pääsemise nõuded:	Iga üliõpilane osaleb grupitööna valmivas arvestustöös ja selle kaitsmisel seminaris. Kõik ühes rühmas osalenud üliõpilased saavad arvestustöö eest sama tulemuse.
Iseseisva töö nõuded:	Iseseisvate tööde loetelu: Arvestustöö rühmatööna: • kaardistatakse ettevõtte riskid; • kirjeldatakse riskijuhtimise korraldust ja tegevusi; • hinnatakse riskide monitoorimise ja reageerimise võimekust; • hinnatakse kontrollide rakendamist ja nende mõju riskidele; • tuuakse välja jääkrisk ja koostatakse ettepanekud IT riskijuhtimise parendamiseks. Arvestustöö koostamise täpsemad juhised antakse loengutes.
Eksami hindamiskriteeriumid või arvestuse sooritamiseks vajalik miinimumtase:	Hindamiskriteeriumid, millest hindamisel lähtutakse: Arvestatud - esitatud ja kaitstud on nõuetele vastav arvestustöö.
Informatsioon kursuse sisu kohta, kursuse jaotumine teemade kaupa sh kontakttundide ajad:	**I loeng 21. septembril kell 14.00-18.00: Andro Kull** IT riskijuhtimise kursuse kirjeldus ja korraldus. Sissejuhatus IT riskijuhtimisse: • Terminid ja seosed nii üldise riskijuhtimisega kui ka infoturbe haldusega; • Rahvusvahelised standardid ja head tavad, sh ISO 31000, ISO/IEC 27005, RiskIT jm; • IT riskijuhtimise korraldus ja protsess; • Väliste teenusepakkujate riskide haldus; • IT riskijuhtimise meetodid ja vahendid; • Riskikontroll ja riskipõhine auditeerimine. **II loeng 30. novembril kell 14.00-18.00: Andro Kull, välislektor** Riskijuhtimise tegevused enne riski realiseerumist: • Riskide monitoorimise vajaduse väljaselgitamine; • Mõõdikud, sh KRI, KPI jm; • Informatsiooni kogumine ja töötlemine;

	• Monitooringu põhimõtted ja vahendid; • Logide analüüs; • Alarmeerimine. **III loeng 13. Detsembril kell 10.00-14.00: Andro Kull, välislektor** Riskijuhtimise tegevused peale riski realiseerumist: • Intsidentide halduse protsess; • Esmased tegevused riski realiseerumise negatiivse mõju vähendamiseks; • Riskikommunikatsioon; • Tõendusmaterjali säilitamise vajadus ja ekspertiis; • Raporteerimine. **IV seminar 14. detsembril kell 14.00-18.00: Andro Kull** Arvestustööde ettekandmine ja kaitsmine. Täpsemad arvestustöö nõuded ja seminari kirjeldus antakse loengute käigus!