

IFI7045	Infoturbe haldus		
Maht:	Kontaktitudide maht: 20	Õppesemester: Kevad 2012	Eksam
Eesmärk:	Anda ülevaade rahvusvaheliselt tunnustatud infoturbemetoodikatest. Luua eeldused teadmiste ja oskuste kujundamiseks infoturbe halduse süsteemi (ITHS) rajamiseks, seireks ja täiustamiseks. Hinnata ITHS kavandamise ja teostamisega seotud organisatsioonilisi vajadusi, eesmärgi, turvanõudeid, äriprotsesse ning organisatsiooni suurust ja struktuuri. Oskus hinnata ITHS teostuse mahtu ja ulatust, arvestades organisatsiooni vajadusi ja võimalusi.		
Aine lühikirjeldus: (sh iseseisva töö sisu kirjeldus vastavuses iseseisva töö mahule)	Sissejuhatus ainesse: Infoturbe ja selle käsitlusala. Infoturbe metoodikad ja standardid ning nende seos teiste IT haldus- ja juhtimisraamistikega (ITIL, Cobit). Kriitilised edutegurid ja infoturbe lähtepunktid. Selgitatakse vajalikud mõisted ja terminid. Teoreetiline osa: Vastavalt ISO 27001 ja ISKE standardile käsitletakse järgmiseid teemasid: riskide haldus, infovarade määratlemine, turbeklasside ja -astme määratlemine, Turbemeetmete ulatuse ja vajalikkuse hindamine. Infoturbepoliitika ulatus ja koostamine. Jätkusuutlikkuse plaani koostamine. ITHS-i seire ja täiendamine. Praktiline osa: Tundides teostatakse praktilisi ülesandeid, mida on võimalik kasutada kodutöös.		
Õpiväljundid:	Üliõpilane on suuteline hindama organisatsiooni infovarade riske, määratlema turbeaspekte, leidma vajalikud vastumeetmed, koostama infoturbepoliitika ja muid regulatsioone. Planeerima ja evitama infoturbe haldussüsteemi, mis baseerub ISO27001 ja/või ISKE standardil.		
Hindamismeetodid:	Eksam (hindeline). Iga üliõpilane koostab ühe individuaalse kodutöö, koostab ja kannab ette gruppitööna valminud arvestustöö, hindab ühte kaasüliõpilaste arvestustööd ning esitleb ettekandena tulemusi.		
Õppejõud:	Hillar Põldmaa, Andro Kull		
Aine ingliskeelne nimetus:	Information Security Management		
Eeldusaine:	Puudub		
Kohustuslik kirjandus:	Loengukonspekt		
Asenduskirjandus: (üliõpilase poolt läbi töötatava kirjanduse loetelu, mis katab ainekursuse)	http://www.iso27001security.com/ http://www.kriso.ee/Information-Security-Risk-Management-Handbook-Handbook/db/9780580607455.html		

loengulist osa)	http://www.ria.ee/iske
Õppetöös osalemise ja eksamile / arvestusele pääsemise nõuded:	Eksam koosneb kirjalikust kodutööst, mis peavad olema esitatud tähtjaks. Kodutöid arvestatakse etteantud järjestuses ja siis, kui eelmine on esitatud. Iga kodutööd võib esitada 2 korda.
Iseseisva töö nõuded:	Iseseisvate tööde loetelu: Kodutöö 1: - Planeeritakse keskmise ettevõtte (10...50 töökohta) infosüsteemid – 10 punkti. - Tehakse nende riskianalüüs – 10 punkti - planeeritakse turvameetmed – 10 punkti - koostatakse jätkusuutlikkuse plaan – 10 punkti Kodutöö 2: - Koostatakse asutuse infoturbe poliitika – 30 punkti Kodutöö 3: - Koostatakse ISKE rakendusplaan – 30 punkti Kodutööde koostamise juhised antakse loengutes
Eksami hindamiskriteeriumid või arvestuse sooritamiseks vajalik miinimumtase:	Hindamiskriteeriumid, millest hindamisel lähtutakse: Esitatud on kõik kolm kodutööd, millede summeeritud punktid annavad järgneva eksami hinde: A – 91-100 punkti B - 81-90 punkti C – 71-80 punkti D – 61-70 punkti E – 51-60 punkti
Informatsioon kursuse sisu kohta, kursuse jaotumine teemade kaupa sh kontaktundide ajad:	I loeng 05.03.2012 1. Sissejuhatus infoturbesse – Infoturbe käsitusala (skoop), terminid, mõisted, määratlused ◦ Mis on info, mida me turvame ◦ Mis on infoturvet ◦ Miks on vaja infoturvet ◦ Infoturbe lähtepunkt ◦ infoturbe seosed üldise juhtimisega ja IT-juhtimisega, turvatunne ja võlts turvatunne ◦ Juhtkonna kohustused ja vastutused infoturbe alal ◦ Infoturbe koordineerimine ja delegeerimine ◦ Infoturvet, kui protsess 2. Riskide kaalutlemine ja käsitus ◦ Kuidas selgitada välja turbe vajadused ◦ Turvariskide kaalutlemine

	◦ Infoturbeohud 1. Füüsilised ohud 2. looduslikud ohud 3. Riistvara ohud 4. Koostööpartneri ohud 5. Tarkvara ohud 6. Küberründed 7. Inimese põhustatud ohud ◦ Turvameetmete valimine II loeng 18.03.2012 3. Jätkame riskihalduse ja ohtudega 4. Füüsiline ja töökeskkonna turve ◦ Turbetsoonid ◦ Sissepääsu/läbipääsu reguleerimine ◦ Sise- ja välisruumide turve ◦ Töötamine turbetsoonides ◦ Avalikud juurdepääsu- , tarnealad ◦ Seadmete turvetehtnilised tugiteenused (remont, hooldus) ◦ Võrgu- ja toitekaabeldus ◦ Seadmete turve väljaspool sise- ja välisruume ◦ Seadmete turvaline kõrvaldamine ja/või taaskasutus 5. Intsidendihaldus ja jätkusuutlikus ◦ Intsidendihalduse ja jätkusuutlikuse plaanimine ◦ Intsidendi tuvastamine ja kindlaks tegemine 1. Seire (monitooring) – mida ja millises mahus 2. Seirelogide kaitse 3. Tõrgete logimine ◦ Intsidendi hindamine ◦ Infoturbeintsidendist või -nõrkusest teavitamine 1. erinevad kommunikatsioonistrateegiad ◦ Intsidendi tagajärgede leevendamine ◦ Intsidendi taastamine Iseseisev töö: Kodutöö 1 (grupitöö): Planeeritakse keskmise ettevõtte (10...50 töökohta) infosüsteem(id). Tehakse nende riskianalüüs, planeeritakse turvameetmed ja koostatakse jätkusuutlikkuse plaan. III loeng 01.04.2011 Infoturbe juhtimine ja korraldus - Infovarad ja nende väärtus - Juhtkonna kohustused ja vastutused infoturbe alal - Infoturbe organisatsioon ja rollid - Organisatsiooni sisemine korraldus - Infoturbe koordineerimine ja delegeerimine
--	--

- Seadustest tulenevad nõuded
- Infoturbe väljasttellimisel

IT turbepoliitika

- Infoturbepoliitika dokument
- Infoturbe poliitika rakendamine ja kontroll
- Infoturbepoliitika läbivaatus

Ligipääsu regulatsioon

- Ligipääsupoliitika
- Kasutajate ligipääsuhaldus
- Kasutaja kohustused ja õigused
- Asutuse kohustused ja õigused

Kodutöö 2 (individuealne):

Koostatakse asutuse infoturbe poliitika, tuues välja vähemalt järgmised põhiteemad:

- Eesmärgid
- Korraldus
- Kontroll

IV loeng 15.04.2012

Etalonturbe olemus

- ISKE rakendusjuhend
- Astmeline etalonturbe
- ISKE rakendamise 11 sammu
- Infovarade vajaliku turvaseme määramine
- Infosüsteemide inventuur
- Infosüsteemide spetsifitseerimine
- Infosüsteemide rakenduste ja käideldava info spetsifitseerimine
- Turvalisuse näitajad
- Andmete turvaklassi määramine
- Muude infovarade turvaklassi määramine
- Turbeastme määramine turvaklassi järgi
- Turvaklassita infovarade turbeastme määramine
- Turvameetmete määramine

Kodutöö 3 (individuealne):

Koostatakse ISKE rakendusplaani kolmeaastase perioodi kohta arvestades turbeastet M.

V loeng 29.04.2012

Asutuse riskijuhtimine ja selle seos infoturbe juhtimisega

Turbenõuete vastavus

- Vastavus õigusaktide nõuetele
- Vastavus IT- turvapoliitikale
- Infosüsteemide auditeerimisvajadus
- Infoturbe dokumentide auditeerimine
- Infoturbe korralduse auditeerimine

Infoturbe järelevalve

Äri jätkusuutlikkuse tagamine

ISKE auditi juhend

ISKE auditi sammud

