

Kursuseprogrammi vorm

IFI 7045	Infoturbe haldus		
Maht EAP	Kontaktitudide maht: 20	Õppesemester: S	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, eesmärke, 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 käsitusala. 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 kodutöodes. Iseseisevtöö: Kodutöö 1 (individuaalne): Vastavalt ISKE metoodikale kaardistatakse infosüsteemid ja selle andmekogud. Määratletakse andmekogude omanikud, turbeklassid ning infosüsteemide SLA. Kodutöö 2 (grupitöö): võttes aluseks kodutöö1 materjalid, teostatakse riskianalüüs ja määratletakse vajalikud meetmed. Koostatakse infoturbe poliitika ja jätkusuutlikkuse plaan. Tehakse ettekanne oma tööst, mida hindavad teised üliõpilased. Kodutöö 3 (individuaalne): kontrollitakse ja hinnatakse ühe grupitööna valminud materjali vastavust ISKE nõuetele. Tuuakse välja puudused ja antakse soovitusel nende parandamiseks. Esitletakse oma töö tulemusi		
Õpiväljundid:	Üliõpilane on suuteline hindama organisatsiooni infovarade riske, määratlema turbeastmeid, leidma vajalikud vastumeetmed, koostama infoturbepoliitikaid ja muid regulatsioone. Planeerima ja evitama infoturbe haldussüsteemi, mis baseerub ISO27001 ja/või ISKE standardil.		
Hindamise meetodid:	Eksam (hindeline). Iga üliõpilane koostab ühe individuaalse kodutöö, koostab ja kannab ette grupitööna valminud arvestustöö, hindab ühte kaasüliõpilaste arvestustööd ning esitleb ettekandena tulemusel.		

Õppejõud:	Margus Kanter
Inglisekeelne nimetus:	INFORMATION SECURITY MANAGEMENT
Eeldusaine:	Puudub
Kohustuslik kirjandus:	Loengukonspekt
Asenduskirjandus: (üliõpilase poolt läbi töötatava kirjanduse loetelu, mis katab ainekursuse loengulist osa)	http://www.iso27001security.com/ http://www.kriso.ee/Information-Security-Risk-Management-Handbook-Handbook/db/9780580607455.html http://www.ria.ee/iske
Õppetöös osalemise ja eksami/arvestusele pääsemise nõuded	Eksam koosneb kolmest kirjalikust kodutööst, mis peavad olema esitatud tähtajaks. Kodutöid arvestatakse etteantud järjestuses ja siis, kui eelmine on esitatud. Iga kodutööd võib esitada 2 korda.
Iseseisva töö nõuded	Iseseisvate tööde loetelu: Kodutöö 1: - Infosüsteemide ja andmekogude kaardistus – 10 punkti - Andmekogude omanike ja turbeklasside määratlemine – 10 punkti - SLA koostamine – 10 punkti Kodutöö 2: - Riskianalüüs – 10 punkti - Meetmete valik – 10 punkti - Infoturbe poliitika – 10 punkti - Jätkusuutlikuse plaan – 10 punkti - Ettekande esitus – 6 punkti Kodutöö 3: - Töö vastavuse hinnang – 10 punkti - Soovitused puuduste likvideerimiseks – 10 punkti - Ettekande esitus – 4 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	I loeng 18.09.2010 1. Sissejuhatus infoturbesse - Mis on info, mida me turvame

kaupa sh kontakttundide ajad	- Mis on infoturve - Miks on vaja infoturvet - Kuidas selgitada välja turbe vajadused - Turvariskide kaalutlemine - Turvameetmete valimine - Infoturbe lähtepunkt - Kriitilised edutegurid - Omaenda suuniste väljatöötamine 2. Infoturbe käsitusala (skoop) 3. Terminid, mõisted, määratlused 4. Infoturbe rakenduse struktuur 5. Riskide kaalutlemine ja käsitus 6. IT turbepoliitika - Infoturbepoliitika dokument - Infoturbepoliitika läbivaatus 7. Infoturbe korraldus - Organisatsiooni sisemine korraldus - Juhtkonna kohustused ja vastutused infoturbe alal - Infoturbe koordineerimine ja delegerimine - Infotöötlusvahendite volitamise protsess - Konfidentsaalsuslepped - Seadustest tulenevad nõuded - Infoturbe sõltumatu läbivaatus (siseaudit) - Turvalisuslepped kolmandate osapooltega - Turvalisus klientidega suhtlemisel 8. Varade haldus - Vastutus varade eest - Varade inventariloend - Varade omanikud (vastutajad) - Varade volitatud kasutamine - Informatsiooni salastatuse liigitus - Teabe märgistamine ja käitus II loeng 02.10.2010 1. Inimressursside turve - Töösuhte algatamisel - Töölepingusätted - Infoturbealased koolitused - Disiplinaarprotsess - Töösuhte lõpetamine või muutmine 2. Füüsiline ja töökeskkonna turve - Turbetsoonid - Sisepääsu/läbipääsu reguleerimine - Sise- ja välisruumide turve - Töötamine turbetsoonides - Avalikud juurdepääsu-, tarnealad - Seadmete turvetehnilised tugiteenused (remont, hooldus) - Võrgu- ja toitekaabeldus - Seadmete turve väljaspool sise- ja välisruume - Seadmete turvaline kõrvaldamine ja/või taaskasutus 3. Suhtlus- ja käitlushaldus - Dokumenteeritud käitlusprotseduurid ja kohustused
---	--

- Muudatuste haldus
- Kohustuste lahusus
- Kolmanda osapoole teenustarnete haldus ja seire
- Infosüsteemide plaanimine ja vastuvõtmine
- Mahuhaldus (suutlikuse haldus)
- Kahjur- ja mobiilkooditõrje haldus
- Varundus - mida, millest ja millises mahus
- Võrguturbe haldus
- Infokandjate käitlus ja haldus
- Infovahetuslepped
- Elektrooniline sõnumivahetus (IM)
- Seire (monitooring) – mida ja millises mahus
- Seirelogide kaitse
- Tõrgete logimine

4. Ligipääsu regulatsioon

- Tööalane ligipääsu regulatsioon (ligipääsupoliitika)
- Kasutajate ligipääsuhaldus
- Kasutaja kohustused ja õigused
- Võrgu ligipääsu regulatsioon
- Operatsioonisüsteemi ligipääsu regulatsioon
- Rakenduste ja teabe ligipääsu regulatsioon
- Mobiil- ja kaugtöö

5. Infosüsteemide väljatöötamine, hankimine ja hooldus

- Infosüsteemide turvanõuded
- Rakenduste õige käsitus
- Krüptograafia
- Süsteemifailide turve
- Turve arendus- ja tugiprotsessides
- Tehniliste nõrkuste haldus

6. Infoturbe intsidentide haldus

- Teavitamine infoturbeintsidendist või -nõrkusest
- Infoturbeintsidentide ja –täiustuste haldus
- Kohustused ja protseduurid

7. Jätkusuutlikuse haldus

- Jätkusuutlikuse infoturbeaspektid
- Jätkusuutlikuse ja riski kaalutlemine
- Jätkusuutlikuse planeerimine
- Teenuskvaliteedi nõuded (SLA)

8. Turbenõuete vastavus

- Vastavus õigusaktide nõuetele
- Vastavus IT- turvapoliitikale ja – normidele
- Tehniline vastavus
- Infosüsteemide auditeerimisvajadus
- Infoturbe dokumentide auditeerimine

III loeng 16.10.2010

9. ISKE meetoodika

10. Etalonturbe olemus

- Astmeline etalonturve
- ISKE rakendusjuhendi struktuur
- ISKE rakendamise 10 sammu
- Etalonturbe täiendamine

	- Infovarade vajaliku turvataseme määramine 11. Infosüsteemide analüüs - Infosüsteemide inventuur - Infosüsteemide spetsifitseerimine - Infosüsteemide rakenduste ja käideldava info spetsifitseerimine - Turvalisuse näitajad - Andmete turvaklassi määramine - Muude infovarade turvaklassi määramine 12. Nõutava turbeastme ja turvameetmestiku määramine - Turbeastme määramine turvaklassi järgi - Turvaklassita infovarade turbeastme määramine - Turvameetmete määramine IV loeng 13.11.2010 2.kodutöö esitlemine ja hindamine 13. Intoturbe auditi põhimõtete tutvustamine - Auditeerimise raamistik ja küsimused - 3.kodutöö koostamise juhised V loeng 12.12.2010 3. Kodutööde esitlemine ja hindamine
--	---

Õppeainet kureeriv üksus:	Informaatika instituut
Kursuseprogrammi koostaja	Margus Kanter
Allkiri:	
Kuupäev:	06.09.2010

Kursuseprogramm registreeritud akadeemilises üksuses

Kuupäev	06.09.2010
Õppeassistendi nimi	Jaanika Meigas
Allkiri	