09. oktoober " Uued tehnoloogiad, küberriskid ja infoturve"
Ats Onemar, CISA, Infoturbe analüütik, Security Software OÜ

1. Sissejuhatus teemasse: mida siseaudiitor peab teadma küberturvalisusest ja infoturbest.

Räägime lühidalt ja anname tausta teema edasiseks käsitlemiseks. Mis on infoturve, mis on küberturvalisus ja kuidas need on seotud siseauditi tööga - kas ainult auditi tellimine.

2. Millised ohud kaasnevad uute tehnoloogiate kasutuselevõtuga.

Mis need uued tehnoloogiad siis on ja kuidas nad organisatsiooni aitavad ja mis ohud nendega kaasnevad. Mida ja kes tegema peaks, et need tehnoloogiad oleks ohutud kasutada.

3. Infoturbe auditeerimine ja vahendid (kompetentsid, töövahendid, praktilised näited)

Miks ja mida infoturbe vallas auditeerida? Millised kompetentsid mängivad infoturbe vallas sh ka auditi läbiviimisel olulist rolli? Võimalikud töövahendid auditi toetamiseks või sellega alustamiseks.

4. Organisatsiooni infoturbealane küpsus.

Infoturvalisuse tagamine on protsess ja areng. Ootused infoturbealaseks võimekuseks ei saa olla igale organisatsioonile samaväärsed. Kuidas antud olukorras aru saada, millised ootused on põhjendatud ja kuhu suunas organisatsioon liigub.

5. Mida siseaudiitor saab teha, et kaitsta oma organisatsiooni. Teadlikkuse tase organisatsioonis ja selle mõõtmine.

Avatum arutelu teemal, kuidas siseaudiitor saab toetada infoturbe arengut ja ka kaitsta organisatsiooni nii töötaja kui audiitori rollis. Räägime ka laiemast teadlikkuse tõstmisest, mis vahenditega ja kuidas aru saada, kas tehtud on piisavalt.

6. Milliseid teste võiks organisatsioonis teha (näited, soovitused, õppetunnid).

Organisatsiooni juhtimine, selles toimivad protsessid ja töötavad inimesed sõltuvad igapäevaselt tehnoloogilistest vahenditest ja nende kättesaadavusest. Kui varem toimetasime hunniku paberite, lauatelefoni ja kalkulaatoriga laua peal, siis täna on seal enamasti sülearvuti ja nutitelefon. Kusjuures, nutitelefon on tihtilugu asendamatu töövahend. Praegune kiire muutuste periood ja uued tehnoloogiad on endaga kaasa toonud ka uued ohud.

Uued tehnoloogiad: nutitelefonid ja nende rakendused, pilvetehnoloogiad, suurenevad andmemassiivid ja nende töötlemine, krüptoaheldamine jpm. Tehnoloogiad muudavad meid produktiivsemaks, annavad paremat infot otsuste langetamiseks, sh vajalik info on alati käepärast – see on positiivne pool. Aga sellest ka meie järjest suurem sõltuvus nende tehnoloogiate kasutamisel, meie sõltuvus nende tehnoloogiate olemasolust.

Tekivad küsimused: kui turvaline see uus tehnoloogia on? Kas minu andmetest on varukoopia olemas? Kellele andmed kuuluvad? Kuidas ma toimetan siis, kui andmed ei ole kättesaadavad? Mida ma teen, kui minu organisatsiooni andmed on lekkinud?

Seminar räägibki uutest ohtudest ja kuidas organisatsioon end nende eest kaitsmiseks ette valmistama peaks. Seminaril käsitletakse teemasid lähtuvalt siseaudiitori vaatest.