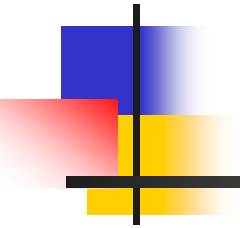


IT audit

Andro Kull

02.10.2010

Tallinna Ülikool

Loengu vorm

- Ajakava:
  - 10.00 – 11.45: loeng (teoreetiline suunitlus)
  - 11.45 – 12.15: paus
  - 12.15 – 14.00: loeng (praktiline suunitlus)
- Materjalid
- Diskussioon

Loengu sisu

- Sissejuhatus;
- IT auditi eesmärk ja A&O, auditi liigitus;
- IT audiitor ja IT auditi organisatsioonid;
- Standardid ja hea tava, mille vastu auditeeritakse;
- IT auditi korraldus ja põhisammud:
  - planeerimine;
  - info kogumine;
  - hinnangute andmine;
  - raporti koostamine.
- Valimikontrolli määratlemine;
- Kontrolli eesmärgid ja IT auditi järeltoimingud;
- ISKE audit;
- IT järelevalve.

IT audit – mis?

Mis ja milleks?

An information technology (IT) audit or information systems (IS) audit is an examination of the controls within an entity's Information technology infrastructure.

/Wikipedia/

IT audit – milleks?

Mis ja **milleks**?

- Kohustuslik: IT audit järelevalve funktsioonis
- Samuti kohustuslik: IT audit siseauditi funktsioonis
- Vabatahtlik: mingil kindlal põhjusel organisatsiooni poolt kolmandatelt osapooltelt tellitud väline audit

IT audit - IT juhile

- IT juht kui kontrollija – oskab ette näha, millele IT audiitor võiks tähelepanu osutada
- IT juht kui kontrollitav – saada aru kuidas IT audit toimub, mida hinnatakse
- IT juht kui IT auditi tellija – auditi eesmärkide ja ülesande püstitamine, auditi tulemuste läbivaatus

IT audit - eesmärk

Vastavuse (*compliance*) ja tegeliku olukorra kontroll:

- Seadused – n. Isikuandmete Kaitse Seadus;
- Määrused – n. ISKE määrus;
- Organisatsiooni sisemised regulatsioonid – n. poliitikad, reeglid, protseduurid;
- Standardid – n. ISO/IEC 27001;
- Soovituslikud juhendid – n. Finantsinspektsiooni juhendid IT valdkonna kohta.

IT audiitor - ettevalmistus

- Sertifitseeritud IT audiitor/IS audiitor omab CISA (*Certified Information Systems Auditor*) sertifikaati
- CISA eksamil on 200 küsimust järgmistest valdkondadest:
  - *IS Audit process*
  - *IT Governance*
  - *Systems and Infrastructure Life Cycle Management*
  - *IT Service Delivery and Support*
  - *Protection of Information Assets*
  - *Business Continuity and Disaster Recovery*
- Veel ISO juhtiaudiitor – Lead auditor

IT audiitor - sõltumatus

- (IT) audiitor ei tohi kuidagi (IT) auditi subjektiga tema (äri)tegevusega seotud olla
- Sõltumatus tagatakse näiteks majanduslike huvide deklaratsiooniga, mida kontrollitakse pidevalt;
- Kui praktikas tuvastatakse et sõltumatus ei ole tagatud, siis ilmselt (Eestis) enam audiitorina tegutseda ei saa.

IT audiitor - eetika

IT audiitor peab:

- Toetama infosüsteemide eeskirjade, protseduuride ja kontrollide väljatöötamist ning nende järgmist.
- Järgima eeskirju.
- Tegutsema hoolikalt, lojaalselt ja ausal viisil oma tööandja, ettevõtte omanike, klientide ja avalikkuse huvides ning teadlikult mitte osa võtma mistahes seadusevastasest või ebasündsast tegevusest.
- Säilitama oma kohustuste täitmise käigus omandatud informatsiooni konfidentsiaalsust. Informatsiooni ei tohi kasutada isikliku kasusaamise huvides ega avaldada asjasse mittepuutuvatele osapooltele.

/EISAÜ/

IT audiitor - eetika

- Täitma oma kohustusi sõltumatult ja objektiivsel viisil ning hoiduma tegevustest, mis ohustaksid või võiksid ohustada tema sõltumatust.
- Säilitama asjatundlikkust auditi ja infosüsteemide alal, arendades oma ametialaseid oskusi ning võttes osa koolitusest.
- Hoolikalt koguma ja dokumenteerima küllaldast faktilist materjali, millel põhjal teha järeldused ja soovitused.
- Informeerima asjassepuutuvaid osapooli enda poolt sooritatud auditist.
- Toetama juhtkonna, klientide ja avalikkuse koolitamist, et laiendada nende arusaamist auditist ja infosüsteemidest.
- Järgima kõrgeid iseloomuomaduste ja käitumise standardeid nii ametialastes kui ka isiklikes toimingutes.

/EISAÜ/

IT audiitor - koolitus

Audiitori koolituse sihid on:

- Säilitada kompetentsuse taset, nõudes pidevat oskuste ja teadmiste täiendamist sellistel aladel nagu infosüsteemid, auditeerimine, juhtimine, raamatupidamine, samuti spetsiifilistel erialadel nagu pangandus, kindlustus, äriseadused jne.;
- Anda võimalus eristada kvalifitseeritud infosüsteemide audiitoreid nendest, kes pole jätkuvsertifitseerimise nõudeid täitnud;
- Pakkuda mehhanism infosüsteemide audiitorite kompetentsustaseme säilitamise jälgimiseks;
- Aidata juhtkonda pädeva auditeerimisfunktsiooni väljatöötamisel, pakkudes kriteeriume personali valikuks ja arendamiseks.

IT audit - organisatsioonid

ISACA - Information Systems Audit and Control Association

- Infosüsteemide valdkonna halduse, juhtimis- ja jälgimistegevuse rahvusvaheliselt tunnustatud liider
- *Previously known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves.*

IT audit - organisatsioonid

EISAÜ

- Eesti Infosüsteemide audiitorite ühing on mittetulundusühing, mille eesmärgiks on toetada infosüsteemide audiitorlust ja propageerida infotehnoloogiaalaseid häid tavasid ning standardeid.
- Propageerimiseks korraldatakse seminare, infopäevi, korralisi koosolekuid ühingu liikmetele jms.

Audit - A&O

Palun anda hinnang, kas on õige suurusega!

Audit - A&O

- Mille suurust tuleb hinnata?
  - Asi ise;
  - Asja komponendid;

  ... ehk piiritleda objekt.
- Mis tähendab suurus?
  - Pikkus;
  - Laius;
  - Kõrgus;

  ... ehk saada aru, mida asja juures tuleb hinnata.

Audit - A&O

- Mis mõõdikuid kasutada?
  - Meeter;
  - Sentimeeter;
  - Mahutavus;

  ... ehk selgitada välja, millisel skaalal mõõta!
- Millisel puhul on õige?
  - 1-2 meetrit;
  - 10-20 sentimeetrit;

  ... ehk selgitada välja hinnangu kriteeriumid!

Auditid - liigitus

- Finantsaudit (*financial audit*)
- Tulemusaudit (*operational audit*)
- Kombineeritud audit (*integrated audit*)
- Haldus audit (*administrative audit*)
- Infosüsteemide audit (*information systems audit*)

Infosüsteemide audit - liigitus

- Vastavusaudit – infotehnoloogia korraldamine toimub vastavuses kehtivate õigusaktidega, standarditega, hea tavaga vms;
- Infoturbe audit – infoturbe riskid on hinnatud adekvaatselt ja riskide maandamiseks on rakendatud piisavad meetmed;
- Infrastruktuuri audit – infrastruktuur on üles ehitatud vastavalt vajadusele ja terviklikult, haldusprotseduurid on juurutatud korrektselt;
- Protsessiaudit – näiteks infosüsteemide arendusprotsess on välja töötatud ja rakendatud, arendusprotsess tagab sobivad lahendused mõistiku ressursikasutusega.

IT audit - metoodikaid

- *COBIT – Control Objectives for Information and Related Technology*
- *ITIL – Information Technology Infrastructure Library*
- *ISKE - Infosüsteemide Kolmeastmeline Etalonturbe süsteem*
- *CAASAM - Computication Audit and Security Analysis Model*
- *GAIT - IT General Controls using a risk-based approach*
- *COSO - Internal Control Framework*
- *PCI/DSS – Payment Card Industry Data Security Standard*
- *...*

IT audit - korraldusest

1. Auditi subjekt
2. Auditi eesmärk
3. Auditi skoop
4. Auditi plaan
5. Auditi protseduurid
6. Hindamine
7. Kommunikatsioon
8. Auditi raport

Annab kokku auditi programmi.

1. Auditi subjekt

- Eesmärk saada ülevaade auditeeritavast valdkonnast;
- Õppida tundma auditeeritava äritegevust ja sellest tulenevaid riske;
- Olenemata aluseks olevatest nõuetest või metoodikast, paralleelne audiitori poolne riskihindamine on vajalik.

2. Auditi eesmärk

- Millistele küsimustele peab audit vastuse andma?
- Auditi tulemus peab aitama kaasa probleemsete kohtade tuvastamisele ja vajalike parendustegevuste planeerimisele;
- Näiteks kindlaks määrata, kas süsteemi muudatused toimuvad piiritletud ja kontrollitud keskkonnas.

3. Auditi skoop

- Millistes raamides auditit teostatakse?
- Kas etteantud skoop võimaldab täita auditi eesmärki?
  - Kui ei aita, tuleb skoopi muuta.
- Näiteks infosüsteem, funktsioon, infrastruktuuri osa, protsess, üksus vms määrab auditi skoobi.

4. Auditi plaan

- Projektina:
  - Eesmärk – vastata küsimusele, anda hinnang, teha ettepanekud...;
  - Tähtajad – määrab paljuski see, millal on võimalus saada hinnangute aluseks olevat lähteinfot;
  - Ressursid – nii ajaline kui inimressurss (panustama peab nii audiitor kui auditeeritav).
- Infoallikad ja asukohad – kelle käest ja kustkohast saab audiitor vajalikku informatsiooni;
- Skoop – millele keskendutakse;
- Tulem – hinnangutele või ettepanekutele orienteeritud;
- Järelaudit – kas ja millistel tingimustel.

5. Auditi protseduurid

- Vastavate materjalide kogumine – tagada et kõik vajalik saaks edastatud;
- Meetod kontrollide testimiseks – off-line, on-line, vaatlus;
- Intervjueeritavate nimekiri – millisel eesmärgil, keda ja millises järjekorra intervjueeritakse;
- Valmistada ette tööriistad ja metoodika protseduuride läbiviimiseks – näiteks analüüsivahendite kasutamine

6. Hindamine

- Kvantitatiivne – eelkõige numbrilise info baasil, midagi mida saab kokku lugeda; võimaldab objektiivset hinnangut;
- Kvalitatiivne – eelkõige audiitori kogemuse, tunnetuse, arvamuse baasil; võimaldab (subjektiivsemat) eksperthinnangut;
- Hindamisskaala – numbriline (1-100), protsentuaalne (% täidetud), madal-keskmine-kõrge;
- Kriteeriumid – vastavalt negatiivne (kui alla 70, alla 50% või madal), positiivne (kui üle)
- Hinnang koos selgitusega (ettepanekuga) – kui hinnang “negatiivne”, siis sellepärast et kriteerium ei ole täidetud (kui teha ..., siis kriteerium täidetud)

7. Kommunikatsioon

- Auditi tulemuste kommunikeerimine – kes peavad tulemustest teadma (nõukogu, juhtkond, töötajad) ja kes ei peaks tulemustest teadma (ajakirjandus)?
- Auditeeritava kommentaarid – võimalus selgitada, lisada täiendavaid kontrolle kui on jäänud auditi skoobist välja jms;
- Lõppjäreldused – audiitor tutvub auditeeritava kommentaaridega ja kujundab lõpphinnangu.

8. Auditi raport

- Auditi kulg – auditi metoodika, auditi plaani täitmine jms;
- Järeldused – kokkuvõttev hinnang auditeeritud valdkonnale ja peamistele puudustele;
- Märkused – konkreetsed märkused auditeeritava valdkonna kohta koos selgitustega;
- Ettepanekud – kui vajalik, siis pakutakse välja võimalikud lahendused olukorra parandamiseks;
- Järeltegevused – teatud ajavahemiku pärast läbiviidav väiksemamahuline audit ettepanekute rakendamise või puuduste kõrvaldamise kohta.

IT auditi meetodid

- Informatsiooni (dokumentatsiooni) analüüs – vastab küsimusele kuidas peab olema, hinnang näiteks kas piisav/puudulik vms;
- Vaatlus – vastab küsimusele kuidas on;
- Intervjuu – vastab küsimusele kuidas on või kuidas võiks olla;
- Testimine – reaalselt tehakse pistelisi teste näiteks kontrollide olemasolu kohta, protseduuri järgimise kohta vms.

ISACA - valimikontroll auditeerimisel

- Auditi valimkontroll määratletakse kui auditiprotseduuride rakendamine vähemale kui 100 protsendile üldkogumist, nii et IS audiitoril oleks võimalik hinnata auditi asitõendeid valitud objektide mingi omaduse järgi ja et see kujundaks või aitaks kujundada järeldust kogu üldkogumi kohta.
- Et valim oleks üldkogumi suhtes representatiivne, peaksid kõigil valimiüksustel üldkogumis olema võrdne või teadaolev valimisse sattumise tõenäosus, st tuleks kasutada statistilisi valimivõtu meetodeid.
- Statistilised valimivõtu meetodid:
  - juhuslik valimivõtt – tagab, et kõigil valimiüksuste kombinatsioonidel üldkogumis on ühesugune võimalus sattuda valimisse;
  - süstemaatiline valimivõtt – seisneb valimiüksuste võtus mingi ettemääratud vahemiku järel, kusjuures esimese vahemiku algus on juhuslik.

ISACA - valimikontroll auditeerimisel

- Kihitamine - valimi tõhusa ja toimiva kavandamise soodustamiseks võib olla kasu kihitamisest. Kihitamine on protsess, millega üldkogum jagatakse ühesuguste selgelt määratletud omadustega alamkogumiteks, nii et iga valimiüksus saab kuuluda ainult ühte kihti.
- Valimi maht - valimi mahu määramisel peaks IS audiitor arvestama valimiriski, aktsepteeritavat vea suurust ja oodatavate vigade ulatust.
- Valimirisk - valimirisk tekib võimalusest, et IS audiitori järeldused võivad erineda järeldustest, milleni jõutaks sama auditiprotseduuri rakendamisel kogu üldkogumile.

Tõendusmaterjal

- Tõendusmaterjali sõltumatus – peab olema tagatud;
- Tõendusmaterjali esitaja kvalifikatsioon – kui ei vasta, tuleb otsida sobilik;
- Tõendusmaterjali objektiivsus – faktid arvamustest ja hinnangutest lahus hoida;
- Tõendusmaterjali ajakohasus – veenduda et auditeerimisel viimane kehtiv seis;

Tõendusmaterjali hoidmine peab olema turvaline (käideldavus, terviklus ja konfidentsiaalsus).

Kontrolli eesmärgid

- Infovarade kaitse meetmed;
- Vastavus siemiste/väliste nõuetega;
- Sisendite kinnitused;
- Operatsioonide täielikkus;
- Väljundite läbivaatus;
- Protsessi usaldusväärsus;
- Varundamine;
- Operatsioonide efektiivsus.

Kontrolli meetmed - ennetavad

Näiteid:

- Ainult kvalifitseeritud tööjõu värbamine
- Kohustuste lahutamine (arendus, haldus, kontroll)
- Ruumidele ligipääsu piiramine
- Dokumenteerimise standardid
- Süsteemsed kontrollid
- Ligipääsuõiguste haldus

Kontrolli meetmed - avastavad

Näiteid:

- Kontrollsummade arvutamine
- Vahetulemuste ülevaatamine
- Automaatsed veateated
- Teistkordne ülearvutamine
- Erisuste tuvastamine
- Tähtaegade jälgimine
- Siseauditi funktsioon

Kontrolli meetmed - parandavad

Näiteid:

- Erakorraliste juhtumite lahenduse planeerimine
- Varukoopiate protseduurid
- Tagasilükkamise (*roll-back*) või ületegemise (*re-run*) protseduurid

ISACA - aruandlus

- Pärast käsitlusobjekti kontrollimise hetke või perioodi, kuid enne IS audiitori aruande tähtaega võivad mõnikord leida aset sündmused, millel on kaalukas mõju käsitlusobjektile ning mis seetõttu vajavad korrigeerimist või avaldamist käsitlusobjekti esituses või kinnituses. Selliseid juhtumeid nimetatakse järgnevateks sündmusteks.
- Kinnitusülesande täitmisel peaks IS audiitor arvestama teavet talle teatavaks saanud järgnevate sündmuste kohta. IS audiitor ei ole aga kohustatud avastama järgnevaid sündmusi.
- IS audiitor peaks küsitlema juhtkonda selle kohta, kas juhtkonnale on teada mingid sellised järgnevad sündmused ajavahemikul enne IS audiitori aruande tähtaega, millel võiks olla kaalukas mõju käsitlusobjektile või kinnitusele.

ISACA - järeltoimingud

- Audiitorid peaksid taotlema asjakohast teavet eelmiste leidude, järelduste ja soovituste kohta ning hindama seda, et otsustada, kas on õigeaegselt rakendatud sobivaid meetmeid.“
- IS audiitori ja auditeeritava organisatsiooni vaheliste arutamiste ühe osana peaks IS audiitor vajadusel saavutama kokkuleppe auditiülesande tulemuste kohta ja tegutsemist täiustavate meetmete plaani kohta.
- Kui probleemiteate soovitused on ellu viidud, võib lõpparuandesse selle soovituse juurde märkida "lõpetatud" või "teostatud". "Lõpetatud" või "teostatud" soovitustest tuleks teatada.

ISACA - järeltoimingud

- Suureriskilisi probleeme puudutavate kokkulepitud tulemuste järeltoimingud tuleks sooritada peatselt pärast meetmete tähtpäeva ja neid tulemusi võib seirata progresseeruvalt.
- Kuna järeltoimingud on IS auditi protsessi lahutamatu osa, tuleks nad ajakavastada koos muude läbivaatuse sooritamiseks vajalike sammudega. Spetsiifilisi järeltoiminguid ja nende ajastust võivad mõjutada läbivaatuse tulemused ja need tuleks määrata ala juhtkonnaga nõu pidades.

Eel-audit ja järel-audit

- Eel-audit (*pre-auditing*) – auditi vajaduse, objekti, skoobi, hindamine: tulemuseks otsus auditi käivitamise kohta, skoobi kohta või edasilükkamise kohta
- Järel-audit (*post-auditing*) – väiksem skoop, põhitähelepanu puuduste kõrvaldamisele, vajadusel täiendav riskianalüüs, täiendav audit

Auditi riskid

- Sisemine risk (*inherent risk*) – sõltumatu auditist, auditeeritava äritegevusest tulenev;
- Kontrolli risk (*control risk*) – olemasoleva materjali baasil ei jõua teha põhjalikke järeldusi, näiteks logide läbivaatus
- Tuvastuse risk (*detection risk*) – mõni oluline aspekt järelduste tegemiseks võib jääda kahe silma vahele
- Üldine auditi risk (*overall audit risk*) – kombinatsioon eelmistest

Andmeanalüüsi vahend

- CAAT (*Computer Assisted Audit Techniques*), lisavad auditile andmeanalüüsi;
- Kasutamise eelised:
  - Auditi riskide maandamine;
  - Erapooletuse suurendamine;
  - Auditi ulatuse suurendamine;
  - Info kiirem esitamine;
  - Efektiivne erisuste tabamine;
  - Paindlikkus andmete analüüsiks;
  - Kvantitatiivsete hinnangute kujundamine;
  - Tõhus proovide võtmine;
  - Auditi kulude kokkuhoid.
- Näiteks ACL, IDEA, SAS, SESAM jms.

IT auditi valdkonnad – IT korraldus

- Indikaatorid – hilinenud projektid, kaadri voolavus, madal jõudlus, kõrged võtmeisiku riskid jms;
- Dokumentatsioon – IT strateegia, plaanid, eelarve, infoturbe poliitika, organisatsiooniskeem, raportid, protseduurid jms;
- Intervjuud – IT töötajad, juhid, ülevaatajad;
- Lepingud – riist- ja tarkvara, arendus ja haldus.

IT auditi valdkonnad – IT infrastruktuur

- Riistvara ülevaatus;
- Operatsioonisüsteemide ülevaatus;
- Andmebaaside ülevaatus;
- Andmesidevõrgu ülevaatus;
- Operatsioonide ülevaatus;
- Probleemilahenduse ülevaatus;
- Käideldavuse ja kasutuse ülevaatus;
- Halduse ülevaatus.

IT auditi valdkonnad – infoturve

- Infoturbe juhtimise audit
- Loogilise ligipääsu auditeerimine
- Kaitsemehhanismide auditeerimine
- Võrguturbe auditeerimine
- Füüsilise turbe auditeerimine
- Füüsilise juurdepääsu auditeerimine
- Kaugligipääsu auditeerimine

IT auditi valdkonnad – talitluspidevus

- Talitluspidevusplaani läbivaatus
- Vastavate testide läbivaatus
- Varuasukoha läbivaatus
- Võtmepersonali intervjueerimine
- Varuasukoha turvalisus
- Varulepingute läbivaatus
- Kindlustuse läbivaatus

IT auditi valdkonnad – süsteemiarendus

- Projektijuhtimine;
- Teostatavus;
- Nõuete püstitamine;
- Tarkvara tellimise protsess;
- Detailanalüüs, disain ja arendamine;
- Testimine;
- Rakendamine;
- Pilootkasutus
- Muudatused ja migreerimine.

IT auditi valdkonnad – süsteemsed kontrollid

- Sisendi kontrollid – süsteem väldib vigaste andmete kandmist;
- Töötluskontrollid – süsteem väldib andmete tervikluse rikkumist;
- Väljundi kontrollid – väljundi läbivaatus ja võimalikud lisatestid.

Riskipõhine audit

- Info kogumine ja auditi planeerimine – ärist arusaamine, eelmiste auditite tulemused, finantsnäitajad, regulatiivsed nõuded, sisemise riski analüüs
- Sisemised kontrollid – kontrolli keskkond ja protseduurid, riskihindamise väljaselgitamine ja kontroll, kogurisk ja jääkrisk
- Vastavustestide läbiviimine – poliitikate ja protseduuride järgimine, kohustuste lahususe tagamine, jms
- Sisuliste testide läbiviimine – analüüsi läbiviimine, kontrollsummade arvutamine jms
- Kokkuvõte – soovituste ja auditi raporti koostamine

ISKE auditeerimine – ISKE rakendamine

I. Infovarade inventuur ja spetsifitseerimine
II. Andmekogude turvaklasside määramine
III. Muude infovarade turvaklasside määramine
IV. Turvaklassiga infovarade turbeastme määramine
V. Tsoonide vajaduse analüüs, asutuse tsoneerimine vajadusel
VI. Tüüpmoodulite märkimine infovarade spetsifikatsioonidesse
VII. Turbehalduse meetmete loetelu koostamine
VIII. Turvameetmete rakendamise plaani koostamine
IX. Turvameetmete rakendamine
X. Tegeliku turvaolukorra kontroll, ohtude hindamine, vajadusel täiendavate meetmete rakendamine

ISKE auditeerimine - ülevaade

Auditeerimise käigus tuleb teha järgmised tööd:

I kontrollida teostatud infovarade inventuuri vastavust nõuetele;
II kontrollida turvaklasside ja turbeastmete määramist;
III kontrollida rakendamisele kuuluvate turvameetmete valimist;
IV kontrollida kõigi rakendamisele kuuluvate turvameetmete rakendamist.

ISKE auditeerimine - ülevaade

- 10-st sammust keskenduda pooltele ISKE rakendamise sammudest ehk 1, 2, 4, 7 ja 9
- Auditeerimisel jälgida:
  - ISKE rakendamise juhend: mida auditeeritav pidi tegema?
  - Reaalne seis: mis on tehtud?
  - ISKE auditi juhend: mida ja kuidas hinnata?

IT järelevalve - ülevaade

- IT järelevalve = IT riskide monitooring+ IT audit;
- Riskide monitooring – vastavuskontroll (compliance) soovituslike juhenditega, tegelike intsidentide esinemine ja muud riskide mõjutajad (siseauditi raport, ...);
- IT audit – off site: dokumentide analüüs, küsimustikud ja on-site: auditi tegevused kohapeal, intervjuud, vaatlus.

IT järelevalve - valdkonnad

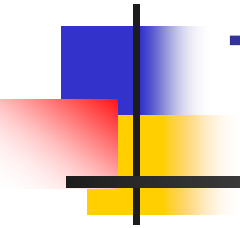
- IT korraldus (*IT governance*) – IT juhtimine, organisatsioon, arendus, haldus jms, nõuded on järelevalve subjektile teada;
- Infoturve (*information security*) – infoturbe juhtimine ja korraldamine, riskide haldus, intsidentide haldus jms, nõuded on järelevalve subjektile teada;
- Talitluspidevus (*business continuity*) – vastutus ja kohustused, talitluspidevuse plaan, taasteplaanid, testimine jms, nõuded on järelevalve subjektile teada;

IT järelevalve - jätkupidevus

- Kogu sektori monitooring – pangad, kindlustus, fondivalitsejad, investeerimisühingud
- Kvantitatiivsed ja kvalitatiivsed hinnangud – monitooringu tulemused (vastavus) numbrilisele skaalale ja põhjendused kirjeldusena;
- Kõikide olulisemate valdkondade katmine – IT juhtimine/haldus (*governance*), infoturbe haldus ja talitluspidevus (continuity);
- Võrdne kohtlemine – üks nõue erineva suurusega ettevõtetele erinevalt kohalduv;
- IT auditi eelneva väljaselgitamise vajadus.

Täiendavat lugemist

- http://www.isaca.org
- http://www.eisay.ee/
- http://www.ria.ee/iske
- http://www.fi.ee/index.php?id=2897



Tänan!

Küsimusi?