8. Infosüsteemide audit

2006

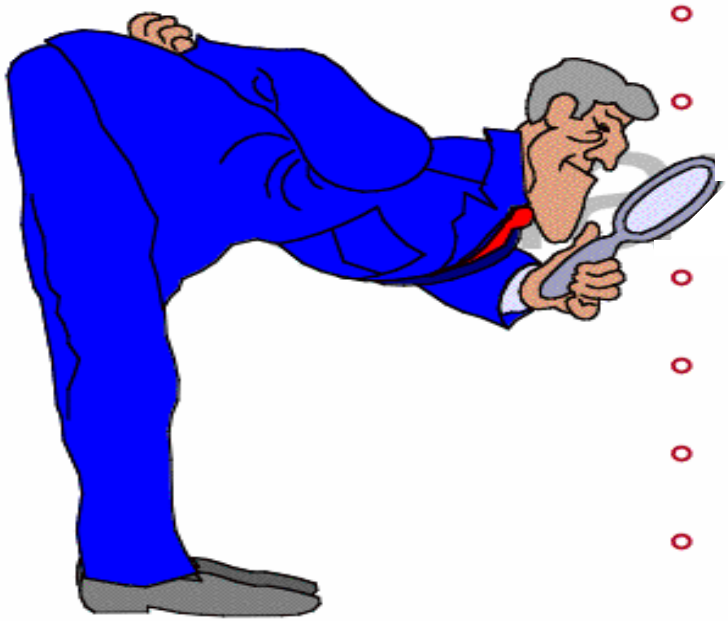
Sissejuhatus

Eriti lühike auditikoodeks

- Auditeerimine pole mõnus –
  eriti auditeeritavale
- Mõlemad osapooled, nii *auditeerija* kui ka *auditeeritav* peavad teadma mitte ainult seda,
  mida teha, vaid ka seda,
  mida **mitte** teha

“Hirm auditi ees”

- **Auditeeritav**:
  Ära lase ennast tabada “püksid rebadel”
- Auditeeritaval on auditist kasu –
  KUI AUDIT ON TEHTUD KORREKTSELT



Protseduurid ja süsteemid

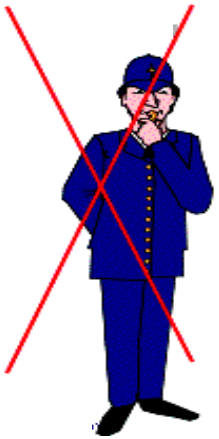
Protseduurid ja süsteemid

Kes on audiitor?

- Ka audiitor on inimene, ta peab valideerima dokumentide, st. veenduma, et töötajad järgivad dokumentatsiooni.

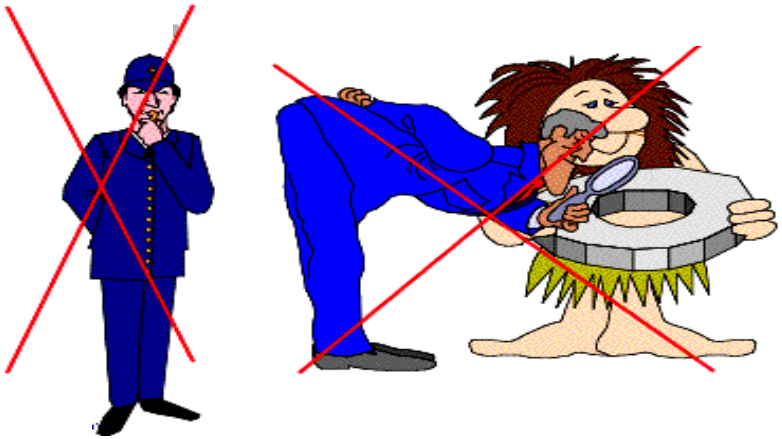
Audiitorid pole

- Ebaausad
- Üliaktiivsed
- Politsei



Audiitorid pole

- Ebaausad
- Üliaktiivsed
- Politsei
- Urgitsejad



Audiitorid pole

- Ebaausad
- Üliaktiivsed
- Politsei
- Urgitsejad
- Inkvisiitorid
- Karistus meie pattude eest

Auditorid vastutavad

- Vastavus auditi nõuetega
- Auditi plaan
- Leidude dokumenteerimine
- Auditi tulemuste raport (aruanne)
- Korrigeerivate tomingute tõhususe verifitseerimine

Auditeeritavad vastutavad

- Töötajate informeerimine auditi eesmärkidest ja skoobist
- Vastutavate isikute määramine audiitoritega kohtumiseks
- Ressurside eraldmine audiitoritele nende töö toimivuse ja tõhususe tagamiseks
- Tagada audiitorite ligipääs kõigile vajalikele materjalidele ja isikutele
- Koostöö audiitoritega auditi eesmärkide saavutamiseks
- Korrigeerivate toimingute määratlemine ja algatamine

Käitumine auditi ajal

- Ole rahulik. Oota, kuni audiitor esitab küsimuse.
- Kuula tähelepanelikult küsimust, enne kui vastad. Kui sa ei saanud küsimusest aru, palu audiitoril küsimust korrata. Kui küsimus pole ikka arusaadav, siis ütle seda audiitorile.
  lialgi ära vasta küsimusele, millest sa aru ei saanud.
- **Räägi alati tõtt.** Ära püüa midagi varjata. Kui sa arvad, et varjates sa aitad kedagi, siis tea – sa ei aita. Pea meeles, et üks vale võib hävitada usalduse – ja ka kogu auditi.
- Usaldus kaotatakse hetkega, selle tagasivõitmine võtab aastaid.

Mida mitte teha

- Kui sa ei tea audiitori küsimusele vastust, siis ütle seda audiitorile. Ära püüa vastust võltsida/välja mõelda.
- Ära varja midagi. Kõik mida audiitor teada tahab, on see, mis tööd sa teed ja kuidas sa seda teed. Kuna seda sa tead, siis saad sa sellest ka vabalt audiitorile rääkida.
- Ära anna vastuseid teiste isikute eest. Kui sa tead, kes seda tööd teeb, siis teata seda audiitorile.
- Ära anna vastuseid teiste poolt tehtava töö kohta. Eeldatakse, et audiitor esitab küsimusi ainult sinu töö kohta. Kui audiitor siiski küsib teiste töö kohta, tuleb vastata: *“see pole minu töö/kohustus/vastutus”.*

Mida audiitorid teevad?

- Audiitorid analüüsivad dokumente ja poliitikaid (verifitseerimine)
- Seejärel audiitorid selgitavad, kuidas töötajad tomivad. Nad teevad kindlaks, kas kõik töötajad täidavad dokumenteeritud protseduure ja poliitikaid (valideerimine)
- Audiitorid selgitavad, kas kõik töötajad on koolitatud oma ülesannete täitmiseks

Verification:
are we building *the thing right?*

Validation:
are we building *the right thing?*

Audiitor leiab probleemi

- Kui audiitor leiab probleemi, siis ta teavitab sellest koheselt – mitteteavitamine on välistatud.
- Leiu kohta võetakse asjasse puutuvalt töötajalt allkiri.
  - Allkiri ei tähenda probleemi tunnustamist, vaid ainult fakti kinnitust
  - Kas probleem on või polnud, selgitatakse päevalõpu kohtumistel või lõppkohtumisel (*final meeting*)
- Kui audiitor ei teavita töötajat leiust, siis leidu polnud. Audiitorid ei teavita juhtkonda probleemist ilma seda eelnevalt probleemiga seotud töötajatega arutamast – "*fair play*" põhimõttest peetakse alati kinni.

Definitsioonid: “**mis**”

- **Tähelepanek** – väide auditeerimisel leitud mittevastavuste kohta
- **Tõendus** – informatsioon auditeeritava objekti kohta, mida on võimalik tõestada
- **Mittevastavus** – auditeeritava objekti erinevus nõuetest

Mittevastavus eksisteerib kuna ...

- Süsteem ei vasta standardi(te)le, protseduuridele või teistele nõuetele
- Teostus ei vasta süsteemile
- Teostus pole tõhus

Mittevastavuste gradatsioon

- Olulised (*major*)
  - Standardi mingit osa on ignoreeritud
  - Võib põhjustada mittevastava toote/teenuse väljastamise
  - Protseduur, mida regulaarselt on ignoreeritud
- Väheolulised, sekundaarsed (*minor*)
  - 3 kuni 5 VÄHEOLULIST ühes süsteemis/protsessis *võib* anda OLULISE mittevastavuse
- Leiud (*findings*)
  - Väheoluline probleem, üksik intsident
  - Leiule peab auditeeritav reageerima

Auditi järelkontroll

- Hinnang korrigeerivale toimingule
- Vastus: **kes, mida, millal, kuidas**
- Vastuse hinnang
- Dokumentatsiooni ülevaatus
- Korrigeeriva toimingu kinnitus
- Järeldus

IS audit

Auditi tüübid

- **Siseaudit**
- **Välisaudit**
  - Teine osapool:
    - Klient auditeerib teenuse pakkujat
  - Kolmas osapool:
    - Audiitoriks on sõltumatu organisatsioon

Auditi faasid

- Auditi plaanimine ja ettevalmistamine
- Auditi läbiviimine
- Auditi tulemuste aruanne (raport)
- Korrigeerivate toimingute määratlemine

IS audit

määratleda auditi käsitlusala	- käsitletav äriprotsess - protsessi toetavad platvormid, süsteemid ja nende ühenduvus - rollid, vastutused ja organisatsiooniline struktuur
selgitada välja äriprotsessi puutuvad infonõuded	- asjakohasus äriprotsessi jaoks
selgitada välja olemuslikud IT-riskid ja üldine juhtimistase	- hiljutised muudatused ja intsidendid ärilises ja tehnoloogilises keskkonnas - auditite, enesehindamiste ja sertifitseerimiste tulemused - juhtkonna rakendatud seiremeetmed
valida auditeerimiseks protsessid ja platvormid	- protsessid - ressursid
otsustada auditi strateegia	- juhtimismeetmed × risk - sammud ja tööd - otsustuspunktid

IS audit: auditi sammud

- Tundmaõppimine
- Juhtimismeetmete hindamine
- Vastavuse hindamine
- Riski tõendamine

IS audit: tundmaõppimine

- ***Auditi sammud, mis tuleb sooritada juhtimiseesmärkidele alluvate tegevuste dokumenteerimiseks ning teatatud juhtimismeetmete või protseduuride olemasolu väljaselgitamiseks*.**

- **Küsitlege asjaomast juhtkonda ja personali, et saada teada**
  - **ärinõuded ja nendega seotud riskid**
  - **organisatsiooni struktuur**
  - **rollid ja vastutused**
  - **poliitikad ja protseduurid**
  - **seadused ja eeskirjad**
  - **kehtestatud juhtimismeetmed**
  - **aruandlus juhtkonnale (seis, sooritus, tegutsemist nõudvad asjaolud)**

- **Dokumenteerige protsessiga seotud IT-ressursid, mida vaatlusalune protsess eriti mõjutab. Leidke kinnitust läbivaadatava protsessi, protsessi kesksete sooritusnäitajate (KSN) ja juhtimisjärelduste mõistmisele näiteks protsessi mõttelise läbikäimisega.**

IS audit: juhtimismeetmete hindamine

- ***Auditi sammud, mis tuleb sooritada kehtestatud juhtimismeetmete tõhususe või juhtimiseesmärgi saavutamise määra hindamiseks. Põhiliselt otsustamine, mida, kas ja kuidas testida.***

- **Hinnake juhtimismeetmete sobivust vaatlusalusele protsessile, arvestades väljaselgitatud kriteeriume, ala standardpraktikaid ja juhtimismeetmete kriitilisi edutegureid (KET) ning rakendades audiitori professionaalset hinnangut.**
  - **Dokumenteeritud protsessid on olemas.**
  - **Asjakohased väljastatavad saadused on olemas.**
  - **Vastutus ja jälitatavus on selged ja toimivad.**
  - **Vajalikes kohtades on olemas kompenseerivad juhtimismeetmed.**

- **Järeldage, mil määral juhtimiseesmärk saavutatakse.**.

IS audit: vastavuse hindamine

- ***Auditi sammud, mis tuleb sooritada veendumiseks, et kehtestatud juhtimismeetmed toimivad vastavalt ettekirjutusele, järjekindlalt ja pidevalt ning järelduse tegemiseks juhtimiskeskkonna sobivuse kohta.***

- **Hankige valitud objektide või perioodide kohta otsest või kaudset tõendmaterjali veendumiseks, et vaatlusalusel perioodil on protseduure järgitud; tõendage seda nii otsese kui ka kaudse materjaliga.**

- **Sooritage protsessi saaduste adekvaatsuse piiratud läbivaatus.**

- **Määrake IT-protsessi adekvaatsuses veendumiseks vajaliku tõendava testimise ja lisatöö tase.**

IS audit: riski tõendamine

Riskihindamise metoodika

- **Operatsiooniriski definitsioon -** Kahju võimalikkus nii väliste (nagu loodusõnnetused, väline kuritegevus) kui sisemiste tegurite (nagu katkestus IT süsteemides, pettus, seadustest ja sisemistest protseduuridest mitte-kinnipidamine ning muud sisekontrolli puudujäägid) tõttu
- **Operatsiooniriski mõõtmisel** vaadeldakse, kui suur on kindlaksmääratud ajahorisondil, kindlaksmääratud tõenäosusega, negatiivsete sündmuste kokkulangemisel ettevõtte maksimaalne kaotus.

Riskihindamise metoodika (2)

RISK

Ühekordne oodatav kahju riski realiseerumisel	X	Tõenäosuslikke riski realiseerumisi perioodis

Riskikomponendid:

Protsessi (käsitletava vara) väärtus	Ohud, nõrkused, vastu-meetmed

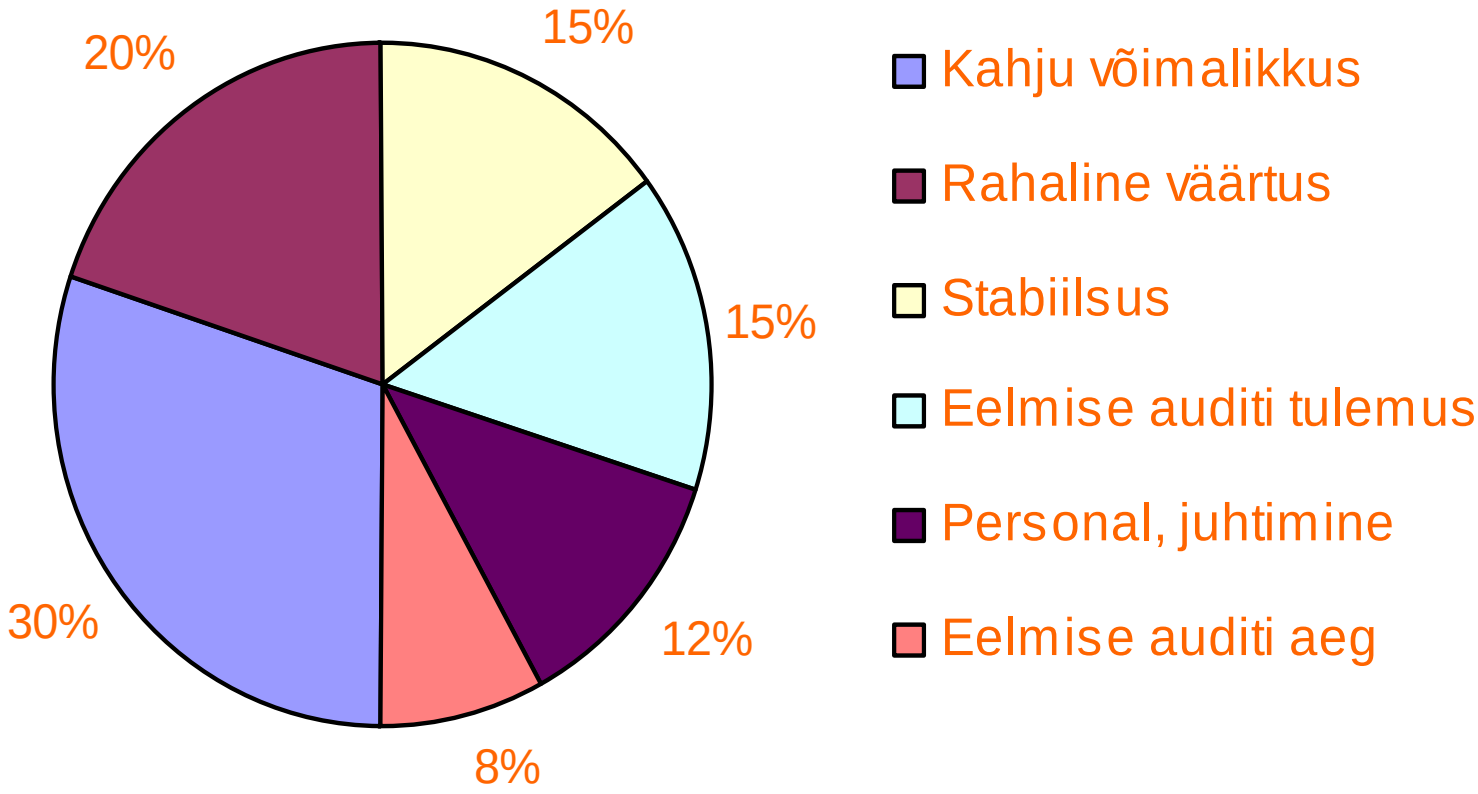
Riskifaktorid siseauditi metoodikas:

1. Kahju võimalikkus
2. Rahaline väärtus
3. Stabiilsus
4. Eelmise auditi tulemus
5. Personal, juhtimine
6. Eelmise auditi aeg

Riskifaktorid

- **Kahju võimalikkus –** iseloomustab protsessi tundlikust otsese kahju tekkele.
- **Rahaline väärtus –** iseloomustab käsitletava protsessi rahalist väärtust.
- **Stabiilsus –** iseloomustab teostatud tegevuste stabiilsust käsitletava protsessi raames
- **Eelmise auditi tulemus –** põhineb eelmise, samas valdkonnas läbiviidud auditi hinnangutel**.**
- **Personal, juhtimine –** iseloomustab juhtimise ja personali kvaliteeti
- **Eelmise auditi aeg –** arvestab kontrollide vähenemist aja möödudes

Riskifaktorid (2)



Riskitase

RISKITASE	PUNKTID	TÖÖPLAAN
Kõrge	67 - 100 punkti	Protsessi auditeeritakse vähemalt üks kord aastas
Keskmine	38 - 66 punkti	Protsessi auditeeritakse vähemalt üks kord kahe aasta jooksul
Madal	25 - 37 punkti	Protsessi auditeeritakse vähemalt üks kord kolme aasta jooksul

Siseauditi hindamismetoodika ja aruandlus

KREDIIDIASUTUSTE SEADUS

- Siseauditi üksus HINDAB krediidiasutuse tavapärast majandustegevust ja sise-eeskirjade ja protseduurireeglite vastavust ja piisavust krediidiasutuse tegevusele ning kontrollib pidevalt nõukogu ja juhatuse kehtestatud eeskirjadest, protseduurireeglitest, limiitidest ja muudest normidest kinnipidamist ning jälgib Finantsinspektsiooni ettekirjutuste täitmist

Näide hindamismetoodikast

- Lähtuvalt auditeeritud PROTSESSI OLULISUSEST ning auditi käigus TUVASTATUD PUUDUSTEST sisekontrolli süsteemis, omistatakse protsessile auditi reiting – A, B, C või D
- Protsessile omistatud reiting EI OLE SAMASTATAV valdkonna reitinguga

Siseauditi hindamismetoodika

REITINGU VÕTI:

A. **Sisekontrolli süsteem on efektiivsed**
B. **Märkused on seotud mõningaste nõrkustega sisekontrolli süsteemis**
C. **Olulised märkused seoses kõrge riskiga, vajalikud on kohesed muudatused töökorralduses ja sisekontrollide selge fikseerimine (näidetega kinnitatud protseduurireeglite rikkumine)**
D. **Kriitiline risk, sisekontrolli süsteem on puudulik (esineb olulisi kõrvalekaldeid firma poliitikast, puuduliku sisekontrolli süsteemi tõttu oht turvalisusele, tõsine oht sissetulekute vähenemiseks, varade raiskamine)**

Aruandlus

- **Siseauditi aruandlus tehtud tööst toimub vastavalt** FIRMA NÕUKOGU **poolt kinnitatud aruandlusprotseduurile.**
- **Aruandluse eesmärgiks on tagada informatsiooni olemasolu grupi sisekontrolli süsteemist ja selle toimimisest ning leida lahendused tekkinud küsitavustele riskide kontrollitusest lähtuvalt**
- **Plaanilise töö raportid edastatakse auditi lõpetamisel auditeeritud** VALDKONNA JUHTIDELE
- **Kord kvartalis annab siseaudit tehtud tööst aru** FIRMA JUHATUSELE **ja** AUDITI KOMITEELE**, vähemalt kord poolaastas** NÕUKOGULE