5. IS audit

2004

Audit

- Audiitortegevuse seadus kehtival kujul ei reguleeri infosüsteemi auditit
- AudS §2 (4) - auditeerimine on raamatupidamisaruande kontrollimine ja sellele hinnangu andmine auditeerimiseeskirjast lähtudes
- Audit - nõuetele vastavuse kontroll ja sõltumatu hinnangu andmine

2

Infosüsteem

- IS - teadmiste, organisatsiooni, meetodite, infotehnoloogiavahendite ja andmete kompleks teabe kogumiseks, säilitamiseks, töötlemiseks ja kasutamiseks.

3

Infosüsteemi audit

- IS audit on nõuetele vastavuse kontroll ja hinnangu andmine auditeeritava organisatsiooni infosüsteemile (või selle osadele), kaasa arvatud selle seostele automatiseerimata protsessidega ja organisatsioonilise struktuuriga.

4

Infosüsteemide audiitor

- IS audiitor:
  - soovitatavalt omades kehtivat IS audiitori sertifikaati
  - auditeerib auditi eesmärgist lähtudes organisatsiooni infosüsteemi
  - vastavalt IS audiitorkontrolli eeskirjadele
  - järgib IS audiitori eetikanormistikku.
- CISA – *Certified Information Systems Auditor.*

5

Informatsiooni turve

Hinnates infoturbega seotud juhtimistegevusi peavad siseaudiitorid kaaluma alljärgnevat:

1. Siseaudiitorid peavad tagama, et juhtkond, nõukogu või mõni teine kõrgem organ omab selget arusaama sellest, et infoturbe tagamine on juhtkonna kohustus (sj. peab olema hõlmatud kogu kriitiline informatsioon sõltumata meedia viisist või andmekandjast).

6

Informatsiooni turve

2. Siseauditi juht peab tagama, et siseaudit omab ise või omab juurdepääsu kompetentsetele ressurssidele hindamaks infoturvet ja sellega seotud nii asutuse siseseid kui väliseid riske.

7

Informatsiooni turve

3. Siseaudit ise peaks kaasa aitama, et nõukogu või mõni teine kõrgem organ nõuaks häirete kohest teatavaks tegemist siseauditile.

8

Informatsiooni turve

4. Siseaudit peab hindama aset leidnud ründeid ennetavate, avastavate ja maandavate kontrollimeetmete tõhusust. Samuti peab siseaudit hindama tulevikus aset leida võivate infoturva alaste juhtumite tõenäosust.

Siseaudit peab olema veendunud, et nõukogu või mõni teine kõrgem organ on vastavalt informeeritud ohtudest, esinenud probleemidest ja korrektiivtegevustest.

9

Informatsiooni turve

5. Siseaudiitorid peavad perioodiliselt hindama asutuse infoturva alast tegevust ja soovitama sobivaid täiustusi ja/või uute kontrollide rakendamist. Hinnangujärgselt peab siseaudit andma kindlustandva raporti nõukogule või mõnele teisele kõrgemale organisatsioonile. Selliseid töid võib siseaudit läbi viia kas eraldiseisvate töödena või integreerituna teistesse auditi projektidesse, mis on osa kinnitatud auditi tööplaanist.

10

Siseauditi mõiste

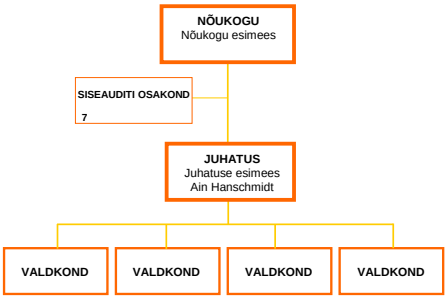
Siseaudit on **SÕLTUMATU** ja objektiivne, kindlustandev ning **KONSULTEERIV** tegevus, mis on suunatud ettevõtte **TEGEVUSE TÄIUSTAMISEKS** ja väärtuse lisamiseks.

Ta aitab kaasa asutuse **EESMÄRKIDE SAAVUTAMISELE**, kasutades süsteemset ja distsiplineeritud lähenemist, hindamaks ja täiustamaks riskide juhtimise, kontrolli ja valitsemiskultuuri efektiivsust.

The Institute of Internal Auditors (1999.a)

11

Näide: *Eesti Ühispank*



12

Siseauditi tegevuse alused

A. KREDIIDIASUTUSTE SEADUS

- **Krediidiasutuse sisekontrolli süsteemi osana moodustatakse sõltumatu siseauditi üksus, mis jälgib kogu krediidiasutuse tegevust.**
- **(1) Siseauditi üksus tegutseb krediidiasutuse** NÕUKOGU **poolt kinnitatud põhimääruses sätestatud korras.**
- **(2) Siseauditi üksuse töötajatel on** ÕIGUS JÄLGIDA **piiranguteta krediidiasutuse tööd ning osaleda juhatuse ja krediidiasutuse põhikirja alusel moodustatud komiteede koosolekutel.**
- **(3) Siseauditi üksusel on** ÕIGUS NÕUDA **krediidiasutuse töötajatelt nende tegevuses ilmnenud puuduste ja eksimuste kohta kirjalikke seletusi ning ilmnenud puuduste kõrvaldamist.**

13

Sisekontroll ja siseauditi osa selles

KREDIIDIASUTUSTE SEADUS (**§55**)

- Krediidiasutuse juhatus (LOE: JUHTKOND) on kohustatud
  - töötama välja ning **RAKENDAMA** asutuse tegevuse kontrollimise süsteemid, tagama nende järgimise, **PIDEVALT HINDAMA** nende piisavust ning vajadusel neid **TÄIUSTAMA**;
  - korraldama sisekontrolli süsteemi tõhusa toimimise;
- Sisekontrolli süsteem **peab hõlmama kõiki krediidiasutuse juhtimistasandeid, et tagada tegevuse** EFEKTIIVSUS**, finants-aruandluse** USALDATAVUS **ning** VASTAVUS **seadustele ja krediidiasutuse juhtkonna poolt kinnitatud dokumentidele.**
- Krediidiasutuse sisekontrolli süsteemi osana **moodusta-takse sõltumatu** SISEAUDITI ÜKSUS**, mis jälgib kogu asutuse tegevust.**

14

COSO sisekontrolli definitsioon

Sisekontroll on protsess, mis on loodud tagamaks piisavat kindlust järgmiste eesmärkide saavutamisel:

- **Äriprotsesside toimivus ja efektiivsus**
- **Finantsaruandluse usaldusväärsus**
- **Vastavus seadustele ja muudele normatiivaktidele**

Võtmekontseptsioonid:

- **Sisekontroll on protsess. See on vahend eesmärgi saavutamiseks, mitte eesmärk ise.**
- **Sisekontrolli viivad läbi inimesed. See ei koosne ainult poliitikatest ja kordadest, vaid** INIMESTEST **igal organisatsiooni tasandil.**
- **Sisekontroll ei taga eesmärgi saavutamisel absoluutset kindlust**

15

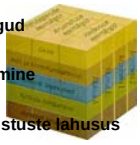
Sisekontrolli süsteem

- COSO (http://www.coso.org/) kuubik sisekontrolli süsteemi komponentidest

16

Sisekontrolli süsteemi komponendid

- KONTROLLIKESKKOND
  Seadusandlus, tööjõupoliitika, väärtushinnangud
- RISKIDE HINDAMINE
  Keskendumine olulisele, ressursside planeerimine
- KONTROLLTEGEVUSED
  Kinnitused, autoriseerimised, võrdlused, kohustuste lahusus
- INFO JA KOMMUNIKATSIOON
  Regulaarne info kontrolltegevuste toimumise, protsessi- ja keskkonna-muudatuste ning erandite kohta. Info liikumine organisatsioonis ülevalt alla ja alt üles. Kommunikatsioonis väljendub iga töötaja arusaamine tema osast sisekontrollisüsteemis.
- SEIRE
  Sisekontrollisüsteemi sõltumatu hindamine - audit



17

Sisekontrollide liigid ja tehnikad

Liigitamine ajalises dimensioonis

- Suunavad kontrollid (korrad, reeglid)
- Ennetavad kontrollid (süsteemsed kontrollid, eelmisest tegevusest sõltuvad kontrollid, kohustuste lahusus)
- Järelkontrollid (aruandlus, inventuurid, auditi jälje analüüsid)

Liigitamine eesmärgi alusel

- Andmete käideldavusele
- Andmete terviklikkusele
- Konfidentsiaalsusele suunatud kontrollid

Liigitamine toimimis-keskkonna alusel

- Manuaalsed kontrollid
- Süsteemsed kontrollid

18

Siseauditi töökorraldus

1. **Siseaudiitorid töötavad juhatusega ja välisaudiitoritega kooskõlastatud ja nõukogu poolt kinnitatud** TÖÖPLAANI ALUSEL
2. **Auditite eesmärk on testida oluliste** SISEKONTROLLIDE TOIMIMIST **läbi erinevate organisatsiooni tasandite, kontrollides grupi töötajate toimingute vastavust kehtestatud reeglitele ja grupi huvidele**
3. **Auditid lõpetatakse** RAPORTIGA**, mis on läbi arutatud ja allkirjastatud auditeeritud valdkonna eest vastutava juhiga.**
4. **Auditite käigus tehtud** TÄHELEPANEKUTE **kõrvaldamiseks lepitakse kokku tähtajad ning määratakse töötajad, kes vastutavad lahenduste leidmise ja rakendamise eest**
5. **Siseaudit viib läbi** JÄRELKONTROLLE **tähelepanekutele reageerimise tulemuste fikseerimiseks**

19

Siseauditi tööplaan

- Siseauditi osakonna tööplaani aluseks on auditeeritava valdkonna tegevuse riskianalüüs
- Riskianalüüsi koostamisel
  a) Moodustatakse loetelu valdkonna protsessidest
  b) Hinnatakse iga üksiku protsessi riski vastavalt kehtivale metoodikale
  c) Omistatakse protsessidele riskitasemed: kõrge, keskmine ja madal
- Tööplaan koostamisel järgitakse põhimõtet, et
  a) Kõrge riskiga protsesse auditeeritakse 1x aastas
  b) Keskmise riskiga protsesse auditeeritakse vähemalt 1x kahe aasta jooksul
  c) Madala riskiga protsesse auditeeritakse vähemalt 1x kolme aasta jooksul

20

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

21

IS audit: auditi sammud

- Tundmaõppimine
- Juhtimismeetmete hindamine
- Vastavuse hindamine
- Riski tõendamine

22

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 keksete sooritusnäitajate (KSN) ja juhtimisjärelduste mõistmisele näiteks protsessi mõttelise läbikäimisega.**

23

IS audit: juhtimismeetmete hindamine

09.06

- ***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..**

24

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.**

25

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.

27

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

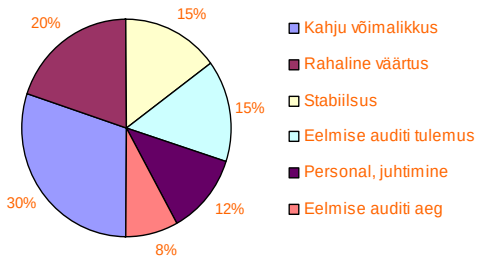
28

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

29

Riskifaktorid (2)



30

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

31

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**

32

Näide: SEB grupi hindamismetoodika

- 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

33

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)**

34

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

35

Järeldused: kuidas parandada IS olukorda?
Üks võimalustest

- Teha esmane valiku COBIT 34 protsessist – näiteks 10 protsessi
- Määrata neile protsessidele omanikud/vastutajad, kes mooduvad töögrupid ja töötavad välja tööplaanid protsesside COBITile vastavuse hindamiseks – ja ettepanekute tegemiseks nende protsesside muutmiseks/täiustamiseks
- ***Kokkuvõttes: tuntud riskijuhtimise metoodika "kui ei jõua kogu rehkendust teha, siis tee pool"***

36

Lisainfo

- *The Institute of Internal Auditors (**IIA**)*
Web http://www.theiia.org

- MTÜ Eesti Siseaudiitorite Ühing
Web: http://www.siseaudit.ee
siseaudit@siseaudit.ee

37