IT audit: lühiülevaade

Jaak Tepandi, CISA

Teemad

Mis?

Kes? - Osalejad – Organisatsioonid – CISA

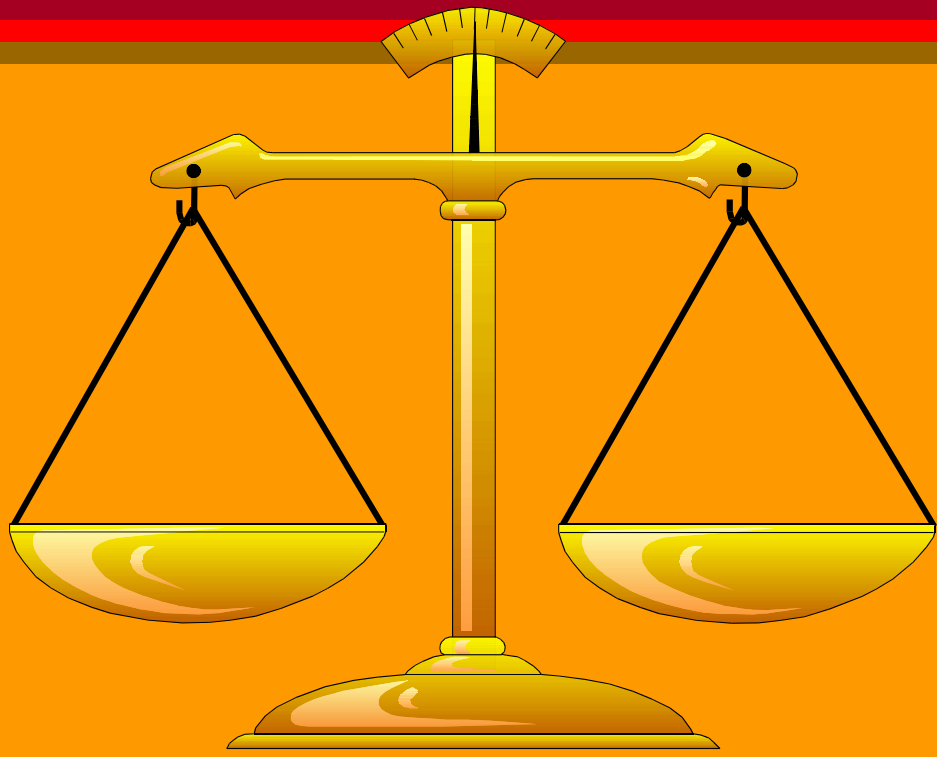
Kuidas? – Auditi loogika – Standardid

COBIT - Ülevaade - Kui juhtimisvahend

IS audit

Ülevaade, hinnang ja nõuanded

- **infosüsteemile (või selle osadele)**
- **süsteemiarendusele**
- **kasutamise tehnoloogiale ja korraldusele**
- **seostele automatiseerimata protsessidega**
- **seostele organisatsioonilise struktuuriga**



IT auditi liike - näited

Spetsiifika

- IT audit
- IT turvaaudit (üldine)
- IT turvaaudit (eriküsimused, detailne)
- IT audit teise auditi koosseisus
- Tarkvara audit
- IT eriküsimused (nt arendus)

Maht / detailsus

- Suur / detailne
- Väike / ülevaade

IS auditis on osalised...

- Tellija
  - omanik, juhtkond, muud volitatud subjektid
- Audiitor
- Auditeeritav (näiteid)
  - kogu organisatsioon, IT-osakond, üks projektirühm, mingi funktsioon kogu organisatsioonis
- Muud (huvitatud) pooled (nt avalikkus)

Auditor

- on sõltumatu auditeeritavast rakendusest
- on sõltumatu auditeeritavast ettevõttest
- on ekspert infosüsteemide auditeerimises
- on ekspert infotehnoloogia (vastavas) valdkonnas
- jälgib auditeerimise head tava ja reegleid
- on tuttav Eesti vastava seadusandlusega
- on tuttav vastavate standarditega
- teab vajalikku metoodikat (nt. COBIT)
- omab sertifikaati

IS Audit and Control Association

- Globaalne liider IT auditeerimises
- >65,000 liiget
- Tütarühingud >140s riigis, sh EISAÜ
- IS Audit & Control Journal
- CISA (>50,000), COBIT
- üle 50 raamatu, konverentsid viiel mandril, koolitus, R&D ...

http://www.isaca.org

Eesti infosüsteemide audiitorühing

- huvitatud isikud
- koolitus, info avalikkusele
- koostöö: ISACA, rahvuslikud ühingud
- auditi standardid
- infosüsteemide audiitorkontrolli eeskirjad
- koostöö IS auditite korraldamisel
- alates 1996

www.eisay.ee

CISA sertifikaat

- CISA eksam
- eetikanormide ja standardite tunnustamine
- töökogemus
- pidevkoolitus ja iga-aastane sertifitseerimine
- aastamaks

Auditi loogika

- Milliseid reegleid on vaja? Kas nad on olemas?
- Reeglid on - kas nad vastavad vajadustele, seadustele jne?
- Reeglid on ja õiged - kas neid täidetakse?
- On õiged reeglid, mida täidetakse - kas nad alati toimivad? Millised on (jääk)riskid?

Auditi standardid ja regulatsioonid

IT/IS standardid, nt:
ISO 27000 seeria,
ISO/IEC 12207,
EVS-EN ISO 9000-3,
ISO/IEC TR 13335…

IS auditi standardid:
nt COBIT.
Audiitortegevuse standardid,
http://www.eisay.ee/2938.
Siseauditi standardid.
Regulatsioonid:
nt ISKE, AKI.
Seadused

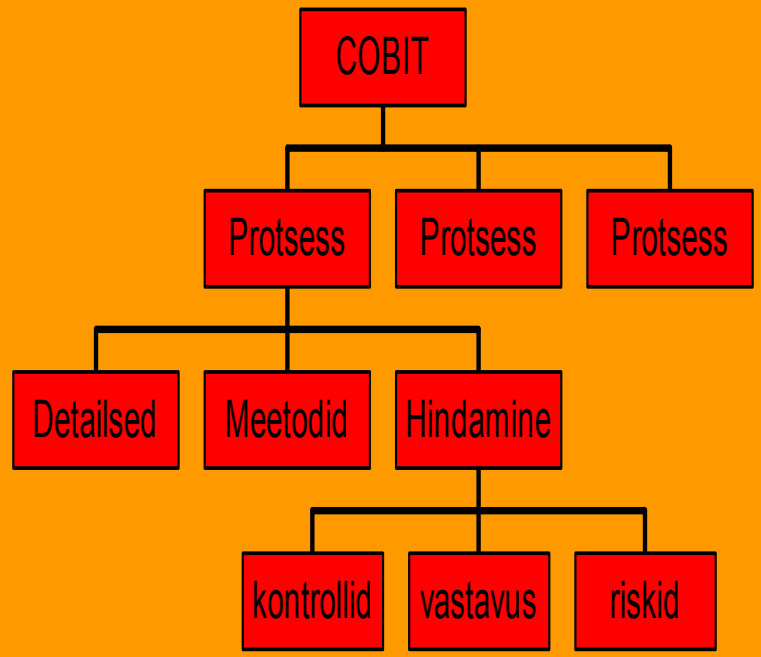
COBIT - metoodika IS haldamiseks, juhtimiseks ja auditiks

- **Info- ja sidustehnoloogia haldamine, juhtimine ja audit, Control Objectives for Information and Related Technology**
- **Kolm kihti tooteid:**
  - **Tipjuhtkonnale**
  - **IT-juhtkonnale**
  - **IT spetsialistidele**

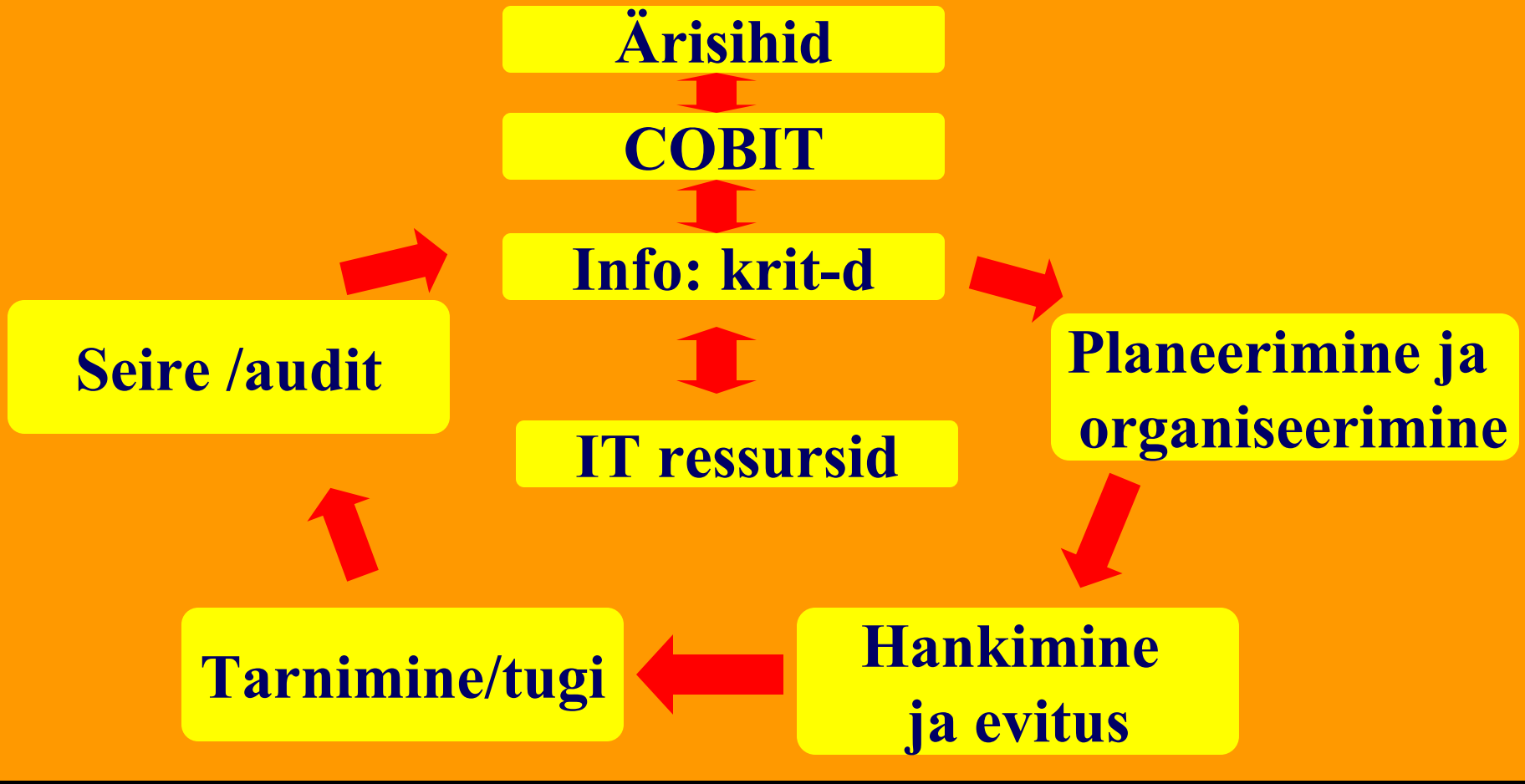
IT_Assurance_Guide_Research.pdf

Raamstruktuur ja juhtimiseesmärgid

- **Raamstruktuur**
- **Kriteeriumid**
- **Ressursid**
- **Alad**
- **Juhtimis-eesmärgid**



Raamstruktuur

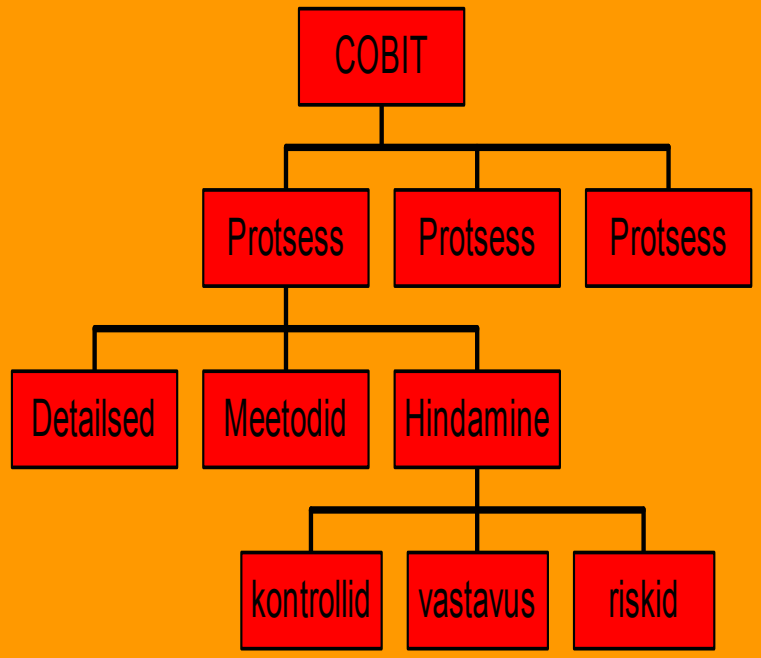


COBIT - teemad

- 4 ala
  - planeerimine ja organiseerimine
  - hankimine ja evitus
  - tarnimine ja tugi
  - seire

COBIT - sisuline ülevaade

- 4-l alal 34 IT protsessi ja laia juhtimiseesmärki
- iga laia juhtimiseesmärgi jaoks
  - 318 detailset juhtimiseesmärki
  - meetodid
  - kontrollide hindamine
  - vastavuse hindamine
  - riskide hindamine



COBIT on abiks

- **Auditil**
- **Ettevõtte IS juhtimisel**
- **Enesehindamisel**
  - **juhtkond**
  - **töötajad**
  - **IT**

Tänan!

Ettekanne on kättesaadav aadressilt www.tepinfo.ee