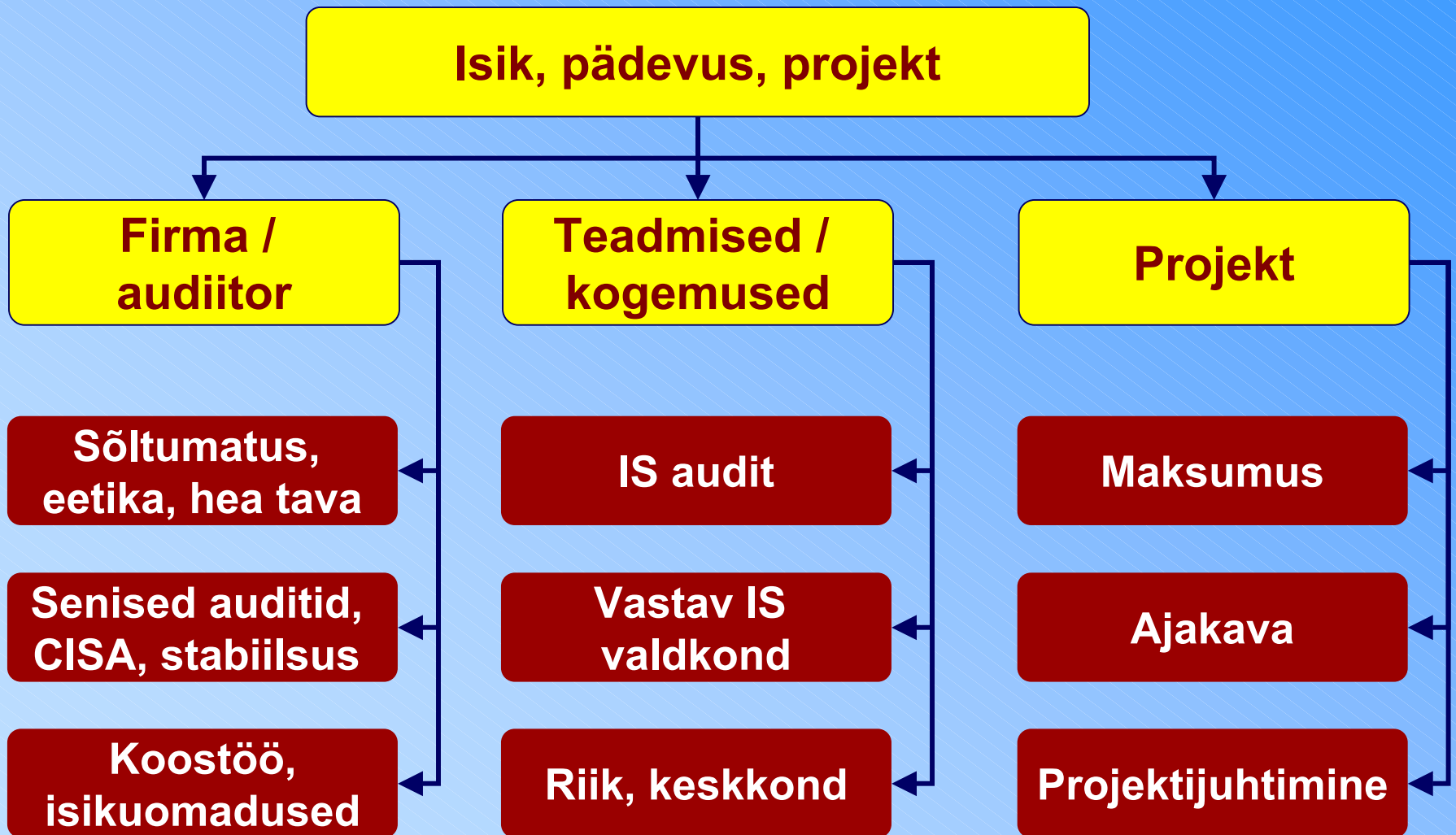


Mida nõuda IS audiitorilt?

Jaak Tepandi, CISA
TTÜ, EISAÜ, ISACA, Tepinfo
jaak.tepandi@tepinfo.ee

Mida nõuda audiitori valikul



Auditi standardid ja regulatsioonid

IS standardid: nt
EVS- ISO/IEC 12207
EVS - ISO/IEC 9126
EVS-ISO/IEC 17799
EVS 8 ...

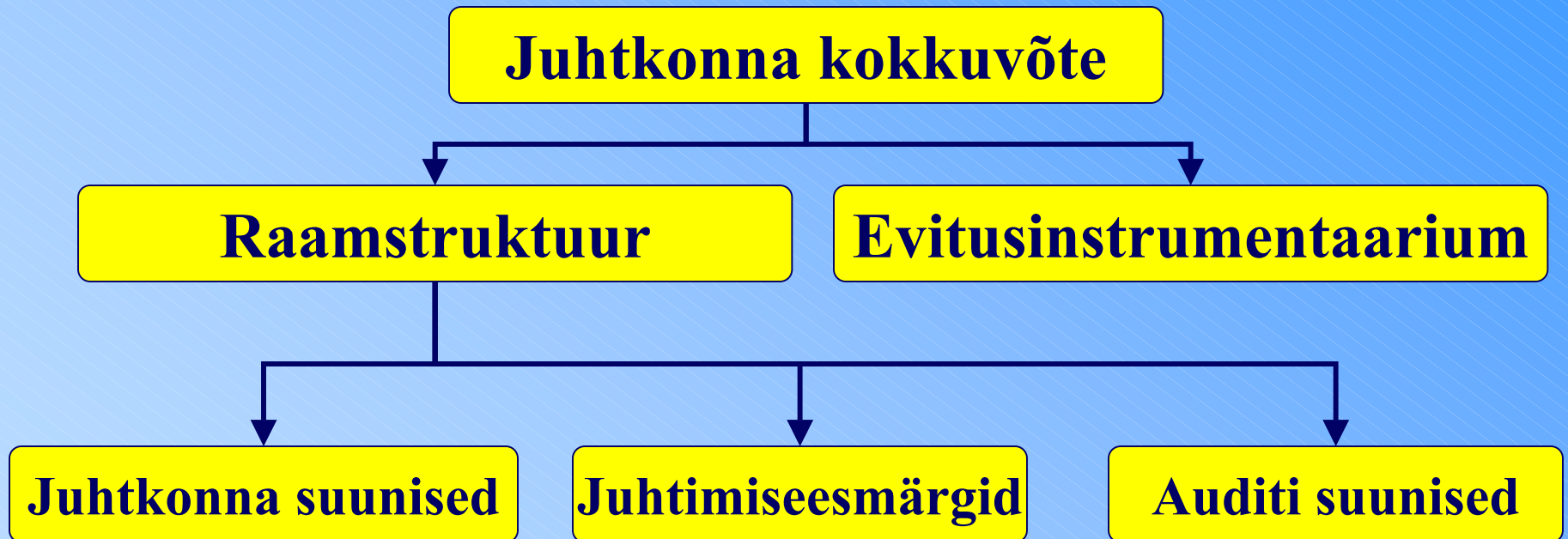
IS auditi standardid: nt
COBIT
ISACA standardid
EISAÜ eeskirjad
Siseauditi standardid
Hea tava nt CISA ...

(Eesti) keskkond nt
Seadused
Muud regulatsioonid
Soovitused ...

ISACA: standardid, juhendid, protseduurid,...

- 12 lühikest standardit, nt sõltumatus, eetika, kompetents, ...
- 24 juhendit standardite rakendamiseks, nt
 - Audit Documentation
 - Enterprise Resource Planning (ERP) Systems Review
- 6 protseduuri, nt. Intrusion Detection, Control Risk Self-assessment
- Seotud COBIT ja selle rakendamisega
- Muud: nt. IT Control Objectives for Sarbanes-Oxley

COBIT 3 tooted

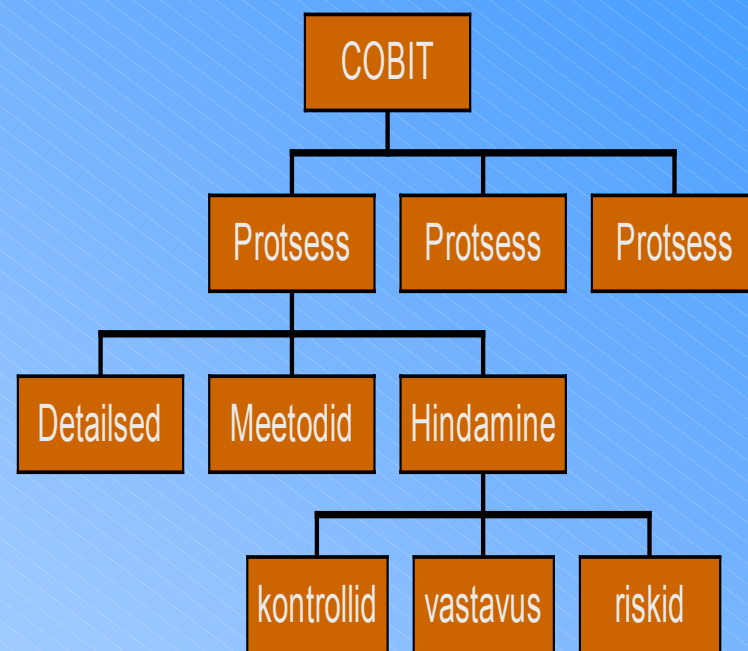


COBIT - kasutamine

- Igapäevases töös - nt juhtkonna suunised
- Auditi ülesande püstitusel - eesmärkide valik
- Auditi läbiviimisel - kas midagi pole unustatud? Soovitused ja juhendid
- Auditi tulemustes - põhjendused, viited

COBIT - sisuline ülevaade

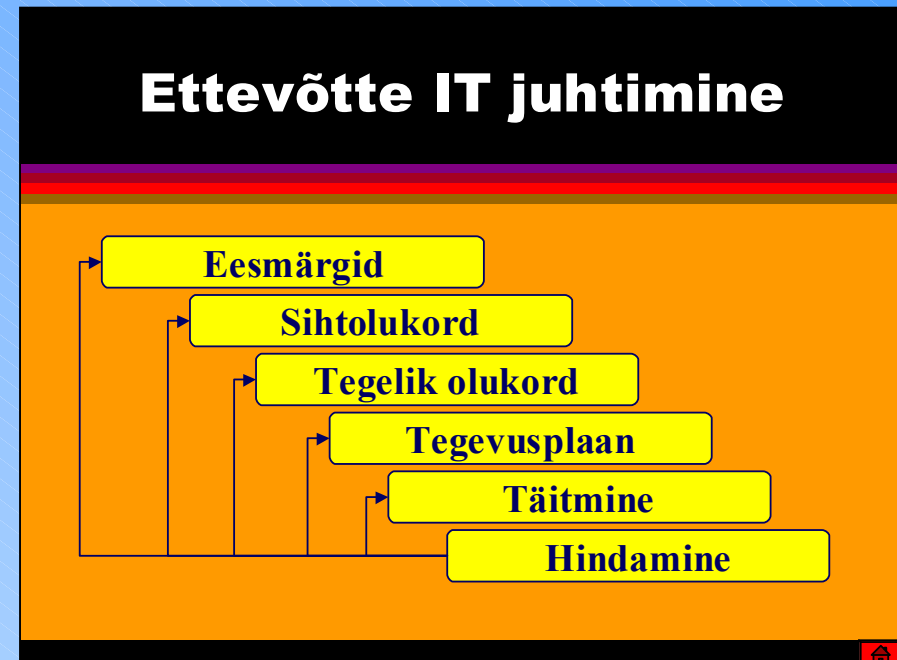
- Neljal alal 34 IT protsessi ja laia juhtimiseesmärki
 - nt: Hallata IT-investeeringuid
- Iga laia juhtimiseesmärgi jaoks
 - detailsed juhtimiseesmärgid (kokku 318)
 - meetodid
 - kontrollide hindamine
 - vastavuse hindamine
 - riskide hindamine



Tee ise: IT juhtimise COBIT lahendus

Juhtkonna suunised

- Ärisiht
- Juhtimiseesmärgid
- Kriitiliste sihtide meetrikad
- Jõudluse meetrikad
- Kriitilised edufaktorid
- Küpsustasemed
 - 0 - olematu, 1 - esialgne, 2 - korratav, 3 - defineeritud, 4 - mõõdetav, 5 - optimeeritud



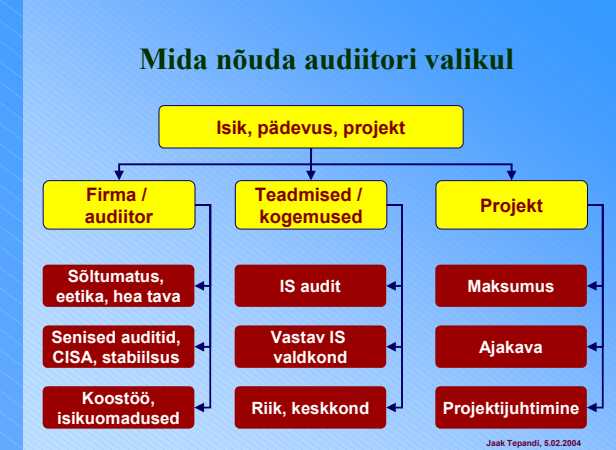
Juhtkonna suunised: +/-

- Paras maht
- Tasemed, mille järgi ennast orienteerida - ühilduvad CMMI-ga
- Eestis kogemus
- Pole üldlevinud
- Pole sertifitseerimist
- Tasemete adekvaatsust pole lihtne hinnata

Mida jälgida auditi käigus? Kuidas seda ära tunda (näited)?

- Audiitor tegutseb ka tegelikult hea tava kohaselt
- Auditis rakendatakse teadmisi ja kogemusi (IS, audit, keskkond)
- Projekt läheb kavakohaselt
- Tulemused on kasulikud

- Erapooletus
- Märkab nii head kui vead
- Konfidentsiaalsus - nii see kui eelmised projektid
- Metoodika on jälgitav
- Standardid (kui vaja) ära toodud ja kasutatud
- Tehnilised vahendid (kui vaja)
- Ajakava, maksumus



Nõudmised auditi väljundile

- Sihid, saavutamine / mittesaavutamine
- Kasutatud standardid, kõrvalekaldumised
- Auditi ulatus - laad, maht, ala, periood, piirangud
- Leiud, selgitused
- Järeldus - hinnang auditeeritavale alale. Mõõndused
- Loogiline, organiseeritud, piisavalt informatsiooni, vormistatud korralikult, korrektne terminoloogia
- Õigeaegselt, vajadusel leiud enne raporti koostamist
- Vajadusel konfidentsiaalsuse deklaratsioon

Üleandmine ja järeltegevused: kas audit on olnud piisav?

Põhilised tunnused:

- ülesanded täidetud
- küsimustele vastatud
- saadud kindlustunne ja kohe rakendatavaid ideid
- vastused õigel tasemel üle antud ja selgitatud
- jätkutegevused kokku lepitud

Kaudsed tunnused:

- rakendatud metoodika
- tehtud tegevused
- kontakt: isikud ja aeg, kohtumiste piisavus
- aruande ulatus / maht
- tähtajad