Mida võetakse aluseks IT auditeerimisel?

Jaak Tepandi, CISA
TTÜ, EVS TK4, Tepinfo
16. 05. 2007

IT auditi meetodeid ja standardeid

- **IT auditi liike**
- **Mida saab kasutada?**
- **Millal mida kasutada?**
- **Mida millega koos kasutada?**

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

Mida saab kasutada?

- **Standardid / Soovitused/ Meetodid**
- **Seadused jm materjalid**
- **Vahendid**
- **Sertifikaadid**
- **Organisatsioonid**

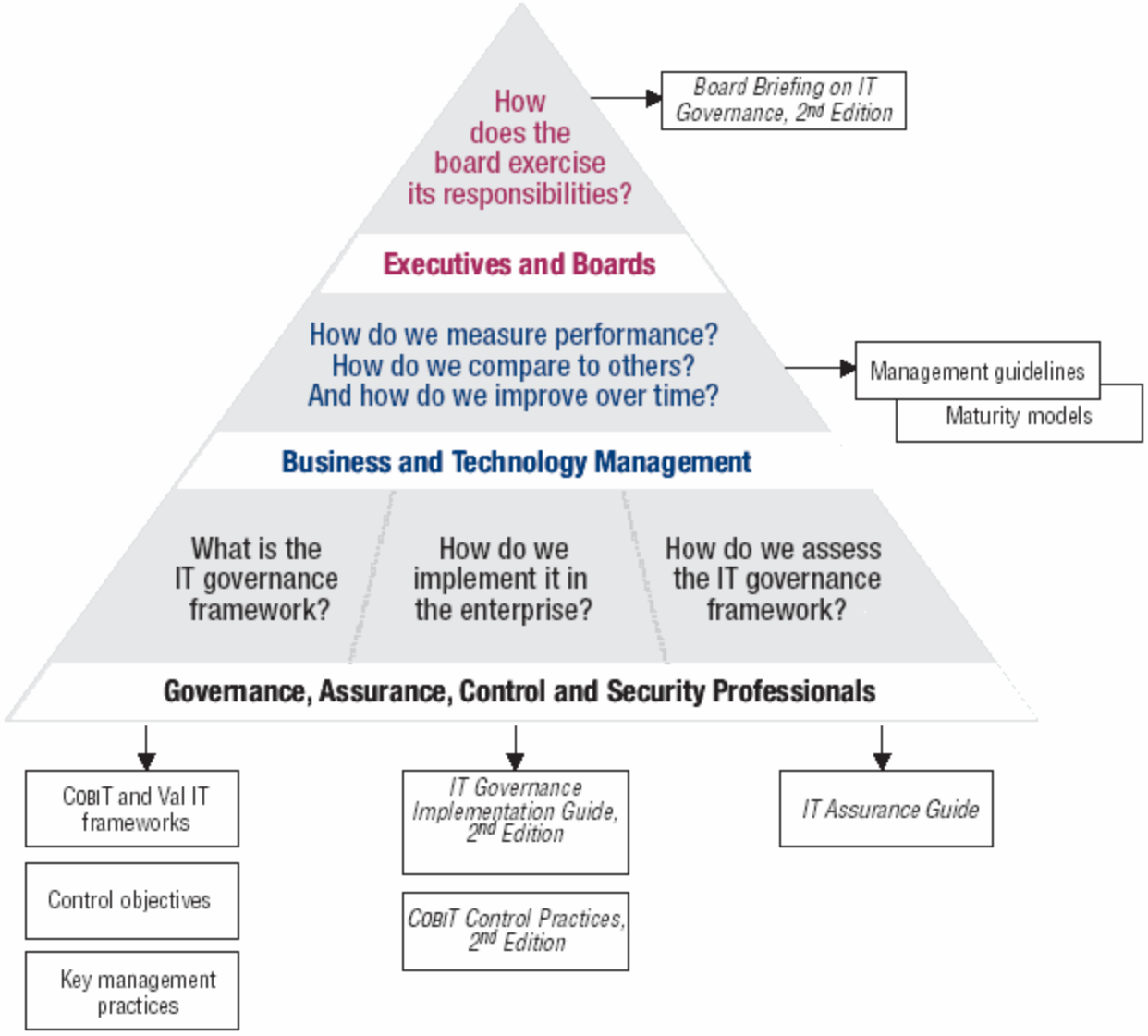
Auditi / IT standardid ja soovitused

IT/IS kohta käivad standardid nt:
ISO/IEC 12207
CMMI, ISO/IEC 15504
ITIL
ISKE, ISO/IEC TR 13335
EVS-EN ISO 9000-3 …

IT auditi standardid nt COBIT
Siseauditi standardid
Soovitused nt AKI
Seadused

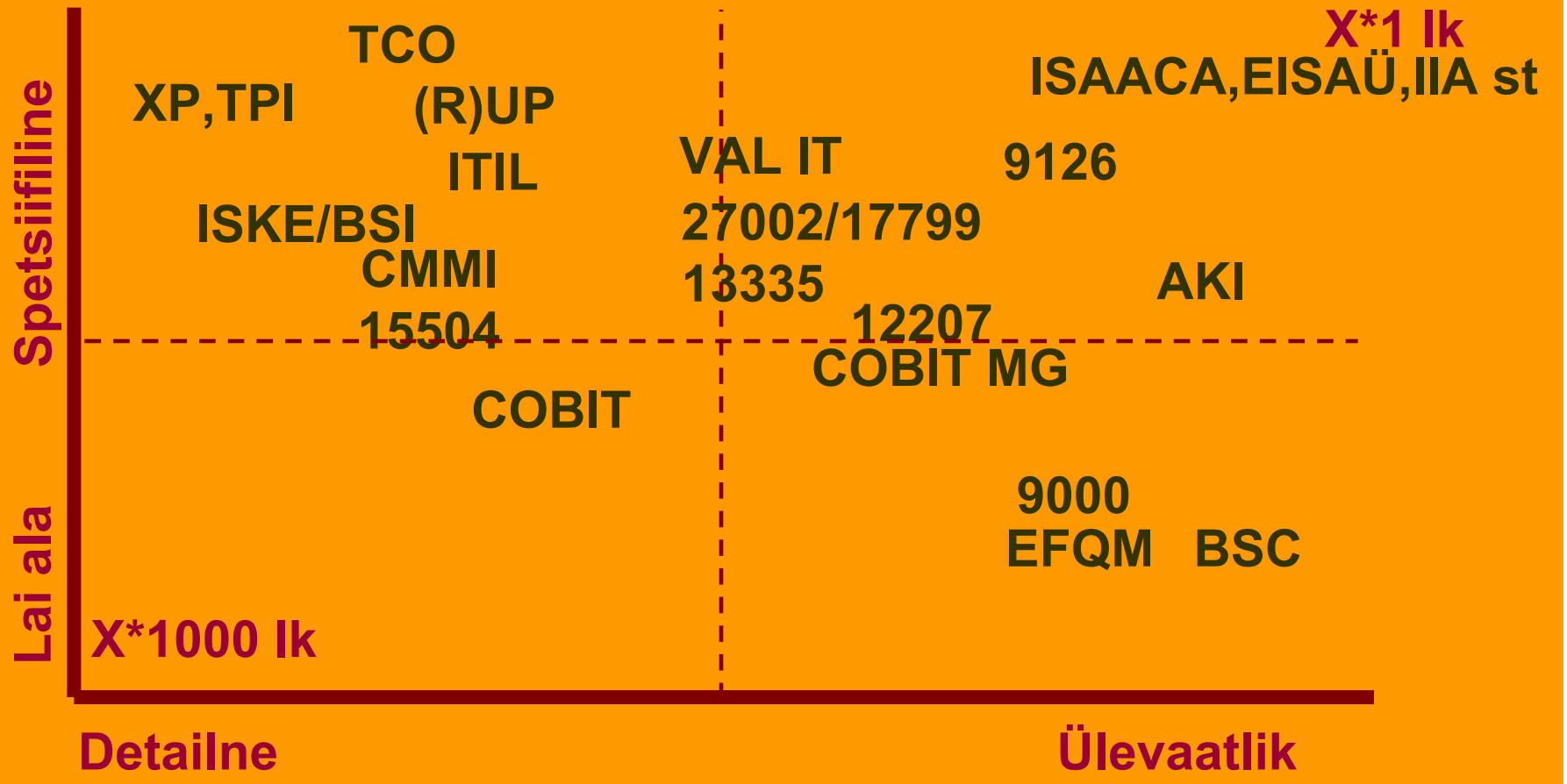
COBIT 4.1. IT Governance Institute, 2007

Figure 3—COBIT Content Diagram



This COBIT-based product diagram presents the generally applicable products and their primary audience. There are also derived products for specific purposes (*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*), for domains such as security (COBIT *Security Baseline* and *Information Security Governance: Guidance for Boards of Directors and Executive Management*), or for specific enterprises (COBIT *Quickstart* for small and medium-sized enterprises or for large enterprises wishing to ramp up to a more extensive IT governance implementation).

Spetsiifiline/lai vs detailne/üldistatud



Mida kasutada?

- Seadustes, määrustes ... nõutud
- Lepingus nõutud
- Dokumentides nõutud
- ...kui ikka veel vabadus?

Vastavalt asukohale

Üldine IT audit =>

- **Cobit / IT raamistikud**
- **eriotstarbelised standardid**
- **auditi üldstandardid**

Kitsam IT audit =>

- **eriotstarbelised standardid**
- **Cobit / IT raamistikud**
- **auditi üldstandardid**

Näide: paroolihaldus

- COBIT 500 lk: 34 ala, neist infoturbe komponendid: Primary 7-s, Secondary 22-s
- Password policy 5 lõiku
- ISKE / IT-Grundschutz-handbuch 3100 lk: infoturve. Meetmeid 1000, ohte 400
- Paroolide üldteema 2 lk + paljudes meetmetes
- ISO 17799/ISO 27002 60 lk: infoturbe haldus
- Paroolid u 1 lk

Üldauditis? Üldises IT turbe auditis? Detailses IT turbe auditis?

Tänan!

www.tepinfo.ee/IT_audit_Tepandi.pdf

LISA: IT / auditi standardeid

- COBIT
- IS audiitorkontrolli eeskirjad (EISAÜ), ISACA standardid, muud audiitorkontrolli eeskirjad (RM, IIA/ESAÜ)
- ISO/IEC 12207, EVS-EN ISO 90003
- ISKE, ISO/IEC TR 13335, EVS - ISO/IEC 17799->ISO 27002, AKI
- ITIL, CMMI, ITSEC, TCSEC, ISO/IEC 15504 (SPICE), TickIT
- (Eesti audiitortegevuse standardid)