Notes on IT audit

Jaak Tepandi
Tallinn University of Technology
Institute of Informatics
Moodle: „Software Quality (Tarkvara kvaliteet)”
Alternate download: tepandi.ee
Version 21.12.2016


Information technology audit

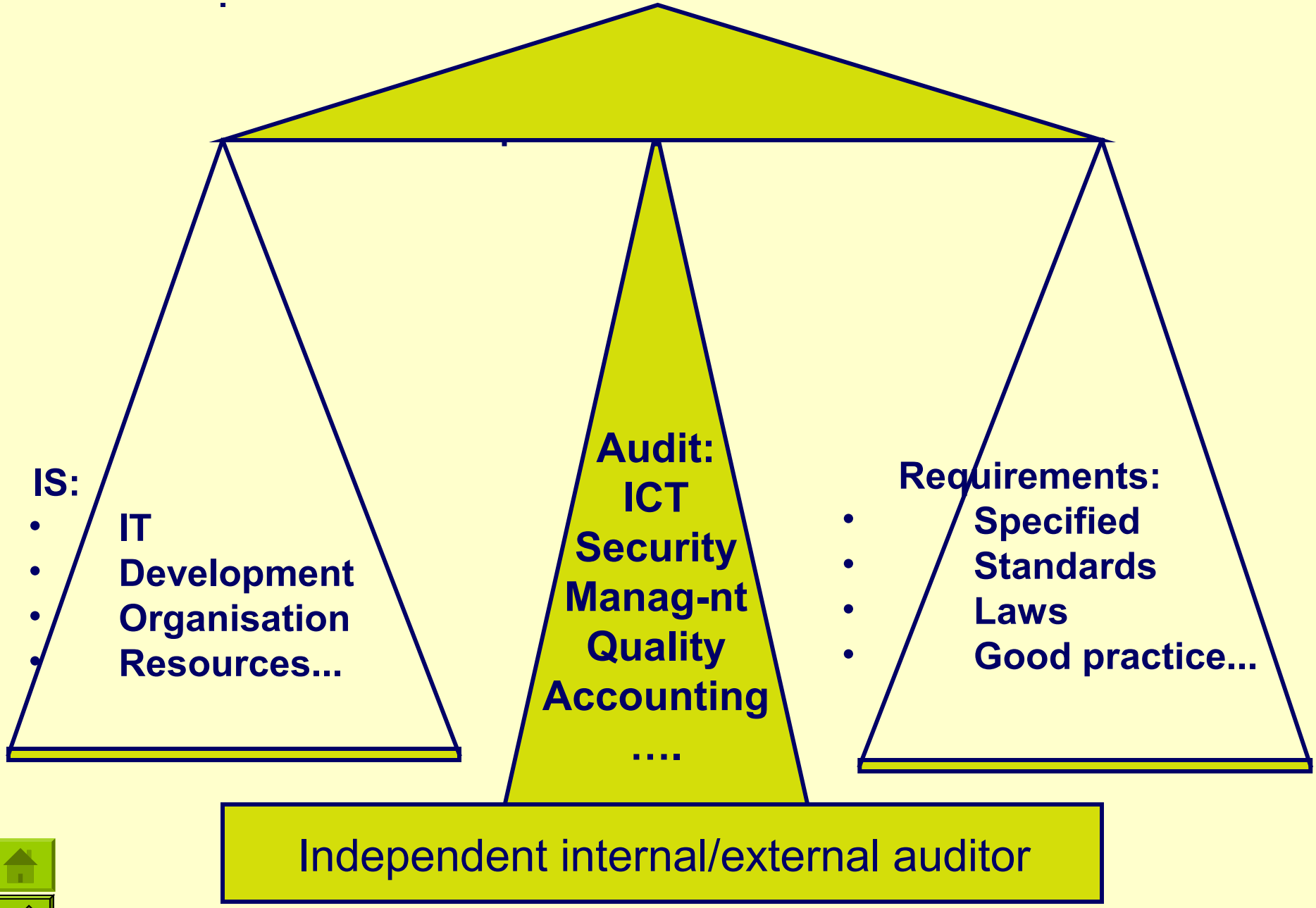
Contents

- Why? Concept, idea
- What? Content
- Who? Participants. Organisation behind. Who might implement?
- When? When to use it, when not? Advantages, disadvantages?
- Where? Relationship to other methods
- How?
  - How can my organisation benefit? How to implement?
  - Standards
  - COBIT

Main materials about audit, COBIT etc: www.isaca.org

Concepts

- IT audit
- ISACA
- COBIT
- CISA


IS:
IT
Development
Organisation
Resources...
Audit:
ICT
Security
Manag-nt
Quality
Accounting
....
Requirements:
Specified
Standards
Laws
Good practice...
Independent internal/external auditor

Audit

Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met. May be carried out by internal or external groups. [ISACA]

Motivation

- Problems
- Management
- Customers
- Legislation
- Public concern

Late Middle English: from Latin auditus ‘hearing’, from audire ‘hear’, in medieval Latin auditus (compoti) ‘audit (of an account)’, an audit originally being presented orally - http://www.oxfordlearnersdictionaries.com/definition/english/audit_1?q=audit

Examples of standards useful for IT audit

- ISACA standards, COBIT
- ISO/IEC 12207, ISO 9001, ISO/IEC ISO 27000 series, ISO /IEC 20000 series, ISO/IEC 25000 series,...
- ITIL, IT Baseline Protection Manual, ISKE
- Professional standards in internal control and auditing
- Professional standards in internal control and auditing: COSO report, IFAC, IIA, AICPA, GAO, PCIE, ISACA standards, etc.
- Emerging industry specific requirements such as from banking, electronic commerce and IT manufacturing

Example: IT security audit may be based on ...

- ISKE framework
- IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals
- IT Baseline Protection Manual
- COBIT
- ISO/IEC 27000 series
- Security audit tools
- Other

Participants

- Customer
- Auditor
- Auditee
- Other

Auditor requirements

- Professional Independence
- Organisational Independence
- Reasonable Expectation
- Due Professional Care
- Proficiency, certification
- Legislation
- Standards, methods, frameworks

Who might be the customer? Auditee?

- Our IS does not satisfy our needs
- Do we waste money on information technology?
- We had a data leakage problem - what can be done?
- Are our communications secured?
- Is the IS department properly based in the organisation?
- Is our IS infrastructure developing in a right direction?
- Our project is delayed - what can be done?

ISACA, COBIT, CISA

- ISACA (previously Information Systems Audit and Control Association, http://www.isaca.org)
- COBIT (originally Governance, Control and Audit for Information and Related Technology). Current version: COBIT 5
- Certified Information Systems Auditor + Certified Information Security Manager (CISM) + Certified in the Governance of Enterprise IT (CGEIT) + Certified in Risk and Information Systems Control (CRISC) designations
- Other professional resources

ISACA

Engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems.

- >140,000 members
- 180 countries
- >200 Local Chapters in >80 countries, incl EISAÜ
- ISACA Journal
- CISA (>118,000 since 1978)
- COBIT, books, journal, conferences, R&D...
- http://www.isaca.org

COBIT

A complete, internationally accepted framework for governing and managing enterprise information and technology (IT) that supports enterprise executives and management in their definition and achievement of business goals and related IT goals [ISACA]

- Starting from IT audit (COBIT 1) to IT Governance (COBIT 5)
- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT
  - Meeting stakeholder needs
  - Covering the enterprise end-to-end
  - Applying a single, integrated framework
  - Enabling a holistic approach
  - Separating governance from management

Please download and read materials from www.isaca.org/cobit

CISA

- CISA examination
  - simultaneously in over 50 countries
  - 200/150 questions, 4 hours
- ethics and standards
- experience
- life-long education
- Domains:
  1— The Process of Auditing Information Systems (21%)
  2— Governance and Management of IT (16%)
  3— Information Systems Acquisition, Development and Implementation (18%)
  4— Information Systems Operations, Maintenance and Service Management (20%)
  5— Protection of Information Assets (25%)

Successful use of auditing frameworks implies

- careful setting of objectives
- recognizing the roles of all stakeholders
- selection of criteria to be audited
- prioritisation of audit findings

Best practice: Arranging an IT audit

- Agreement
  - analysis of the problems and situation
  - scope of the audit
  - the contract
- Audit
  - requirements, documentation, procedures
  - compliance testing
  - substantive testing
  - risk evaluation
- Reporting and presentation

Audit logic

A system full analysis is usually not possible

- **Do rules exist?**
- **Yes: are they adequate?**
- **Yes: are they fulfilled?**
- **Yes: are they working, is it possible to go around?**
- **What are the residual risks? Have they been accepted?**

Summary / Outcomes

- Understanding of the idea, purpose and application areas of ICT audit
- Understanding of the concepts of ISACA, COBIT, CISA
- Given an organisation and a system - ability to set up an objective and task for an ICT audit

Useful to IT auditor, manager, maintainer, and other stakeholders

Additional reading (examples)

ISACA, http://www.isaca.org

COBIT, http://www.isaca.org/cobit

CISA, http://www.isaca.org/cisa

ISACA Estonian Chapter, http://eisay.ee/

Software quality, processes, and standards: some challenges

- Testing across different platforms
- Internet of things
- Big data
- Data quality
- Data analysis
- Mobile systems
- Human body systems
- Intelligent systems
- Security
- ...

Course and Part 3: Summary