IS 17799

- **"Code of practice for information security management"** (fast track of BS 7799-1; under revision since 2000, now FCD)
- -> security officer
- "... guidelines and principles for initiating, implementing, maintaining, and improving information security management ..." -> what
- ... each area introduced by a description of the goal ("objective") and structured into subchapters ("controls") with different depth
- ... covers several control areas such as policy, organization (*), asset management, personnel (*), physical security (*), operational issues (*), access control, systems aquisistion & development, *incident management*, business continuity, and compliance
  -> checklist without priority/ sequence
- new: *risk assessment and treatment*
- new: *control statement, implementation guidance, other information*
- BUT: no metric defined in order to support the assessment

IS 13335

- **"Management of Information and Communications Technology Security"** (MICTS = the "new" GMITS)
  part 1: concepts and models for ICT security management (now FDIS)
  part 2: techniques for ICT security risk management (now 3rdWD)
- -> security officer
- "... to assist the implementation of information security ..." -> how
- ... covers security elements and relationships, ICT policy, organizational aspects, security management functions, risk management process, safeguards categories and approaches for selecting safeguards
- ... contains techniques for ICT risk management which can be used to assess security requirements and risks, and help to initiate and follow-up appropriate safeguards
- -> concepts/models, and techniques without pre-scribing
- BUT: no metric defined to check whether the techniques are "in place"

BS 7799-2

- **"Information security management systems - Specification with guidance for use"**
- ... covers ISMS liefecycle, management responsibility (incl. Management review of ISMS) within 10 pages
- -> senior management
- ... based on the PDCA-model (by Deming) -> management system
- ...defines key elements such as general requirements, establishing an maintaining ISMS, documentation requirements, management commitment, resource management, general review requirements, review input, review output, internal audits, continual improvements, corrective and prevention action
- ... emphasises systematic approach to risk assessment
- -> mingles operative and management processes
- BUT: no parameter/ indicators to "measure" performance/ effectiveness