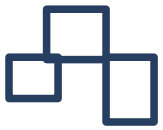
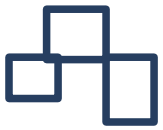


Etika & Profesionalisme TSK

IT Audit dan Forensics

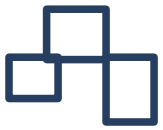
diadopsi dari materi kuliah

Dr. rer.nat. Avinanta Tarigan



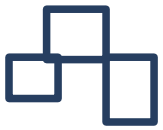
IT Audit

- Latar Belakang:
  - ICT telah dimanfaatkan sedemikian (i) luas dan (ii) dalam, dan banyak institusi / organisasi bergantung pada ICT, sehingga resiko bisnis semakin besar
- Definisi:
  - Penilaian / pengujian kontrol dalam sistem informasi atau infrastruktur teknologi informasi
- Proses IT Audit:
  - Mengumpulkan dan mengevaluasi bukti-bukti bagaimana sistem informasi dikembangkan, dioperasikan, diorganisasikan, serta bagaimana praktek dilaksanakan:
    - Apakah IS melindungi aset institusi: asset protection, availability
    - Apakah integritas data dan sistem diproteksi secara cukup (security, confidentiality)?
    - Apakah operasi sistem efektif dan efisien dalam mencapai tujuan organisasi, dan lain-lain (coba cari pertanyaan2 lain)



IT Audit

- Stakeholders:
  - Internal IT Deparment
  - External IT Consultant
  - Board of Commision
  - Management
  - Internal IT Auditor
  - External IT Auditor
- Kualifikasi Auditor:
  - Certified Information Systems Auditor (CISA)
  - Certified Internal Auditor (CIA)
  - Certified Information Systems Security Professional (CISSP)
  - dll
- Output Internal IT:
  - Solusi teknologi meningkat, menyeluruh & mendalam
  - Fokus kepada global, menuju ke standard2 yang diakui
- Output External IT:
  - Rekrutmen staff, teknologi baru dan kompleksitasnya
  - Outsourcing yang tepat
  - Benchmark / Best-Practices
- Output Internal Audit & Business:
  - Menjamin keseluruhan audit
  - Budget & Alokasi sumber daya
  - Reporting



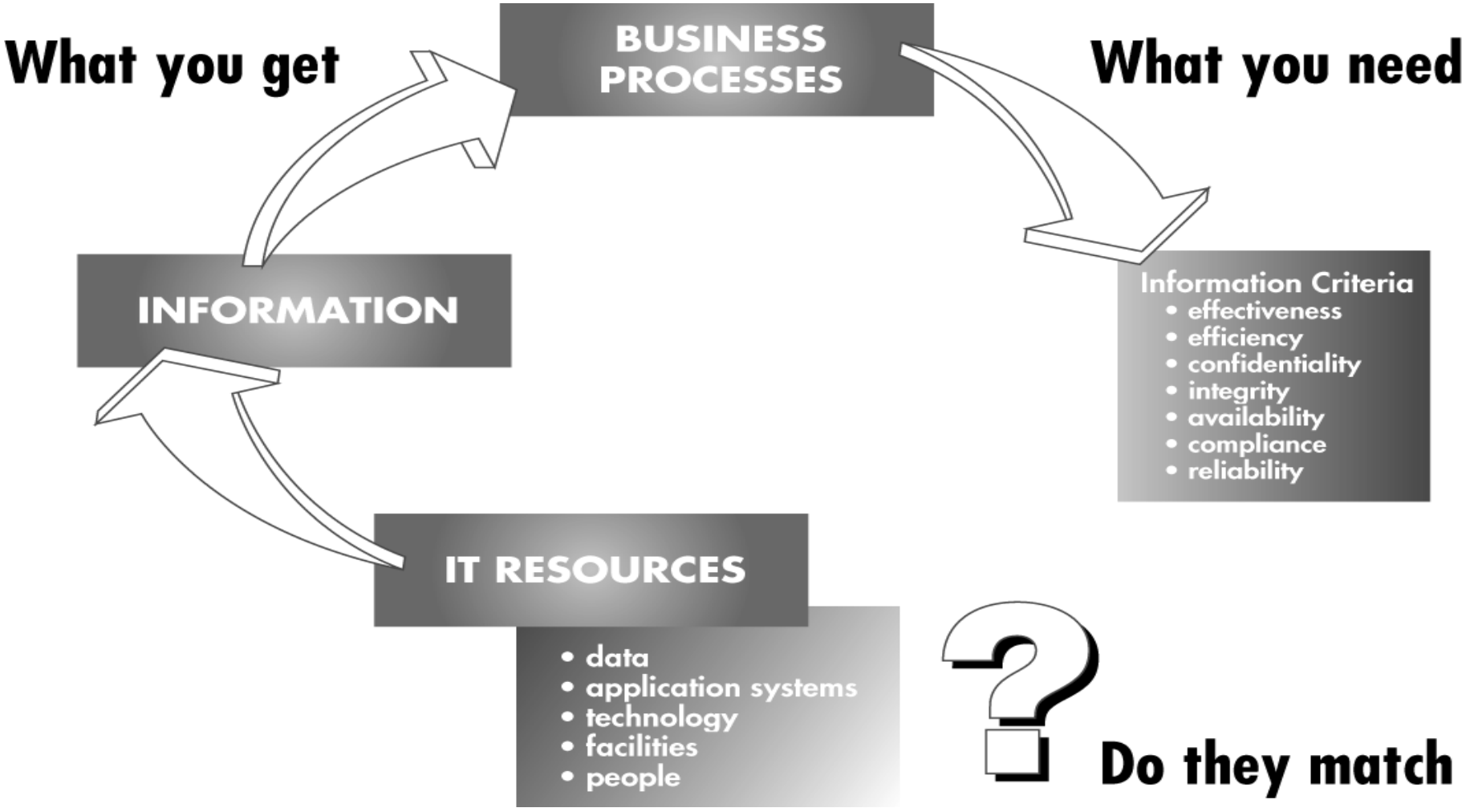
Metodologi & Framework

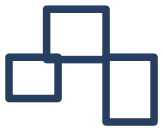
- Framework Besar:
  1. IT Audit
  2. Analisis Resiko berdasarkan hasil audit
  3. Memeriksa "kesehatan" sistem & security benchmarking terhadap sistem yang lain / standard
  4. Hasil dari ketiganya (1,2,3) melahirkan konsep keamanan sistem Informasi
  5. Hasil dari konsep keamanan:
     - panduan keamanan sistem (handbook of system security)

- Metodologi IT Audit:
  - **CobiT**
    - www.isaca.org
  - **BS 7799** - Code of Practice (CoP)
    - www.bsi.org.uk/disc/
  - **BSI** -IT baseline protection manual
    - www.bsi.bund.de/gshb/english/menue.htm
  - **ITSEC**
    - www.itsec.gov.uk
  - **Common Criteria** (CC)
    - csrc.nist.gov/cc/

COBIT

- Dikembangkan oleh ISACA
- (mungkin) cocok untuk self-assesement tapi kurang cocok untuk mengembangkan buku petunjuk keamanan sistem
- Membantu dalam implementasi sistem kontrol di sistem IT
- Dokumentasi detail kurang
- Tidak begitu user-friendly

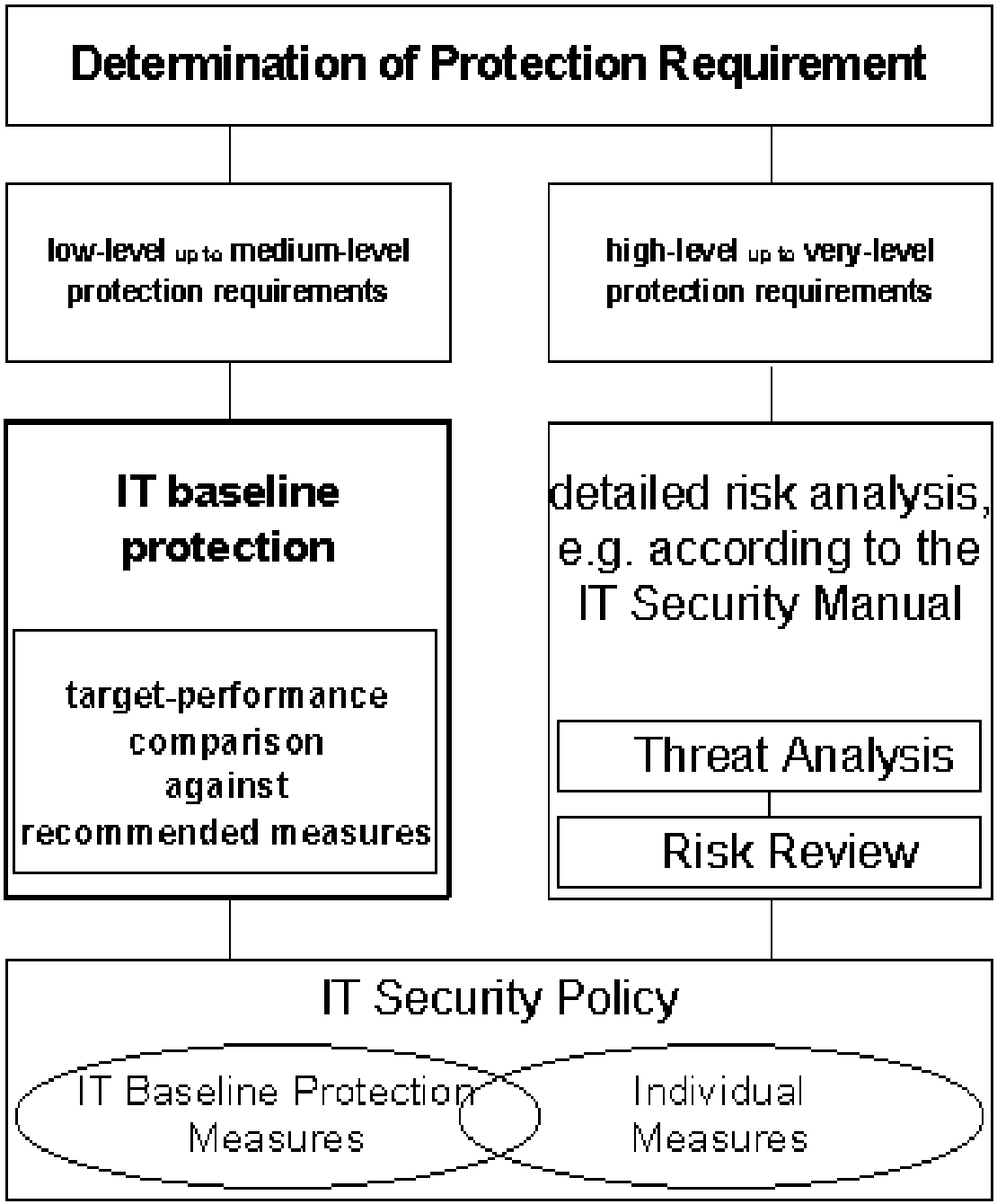




BS 7799 – Code of Practice

- Code of Practice for Inform. Security Management
- Dikembangkan oleh UK, BSI: British Standard
- Security baseline controls:
  - 10 control categories
  - 32 control groups
  - 109 security controls
  - 10 security key controls
- Kategori kontrol:
  - System access control
  - Systems development & maintenance
  - Business continuity planning
  - Compliance
  - Information security policy
  - Security organisation
  - Assets classification & control
  - Personnel security
  - Physical & environmental security
  - Computer & network management
- Digunakan untuk self-assasement:
  - konsep keamanan dan kesehatan sistem
- Tidak ada metodologi evaluasi dan tidak diterangkan bagaimana assemen thd keamanan sistem
- Sangat user-friendly sangat mudah digunakan (menurut yang sudah menggunakan)

BSI (Bundesamt für Sicherheit in der Informationstechnik)



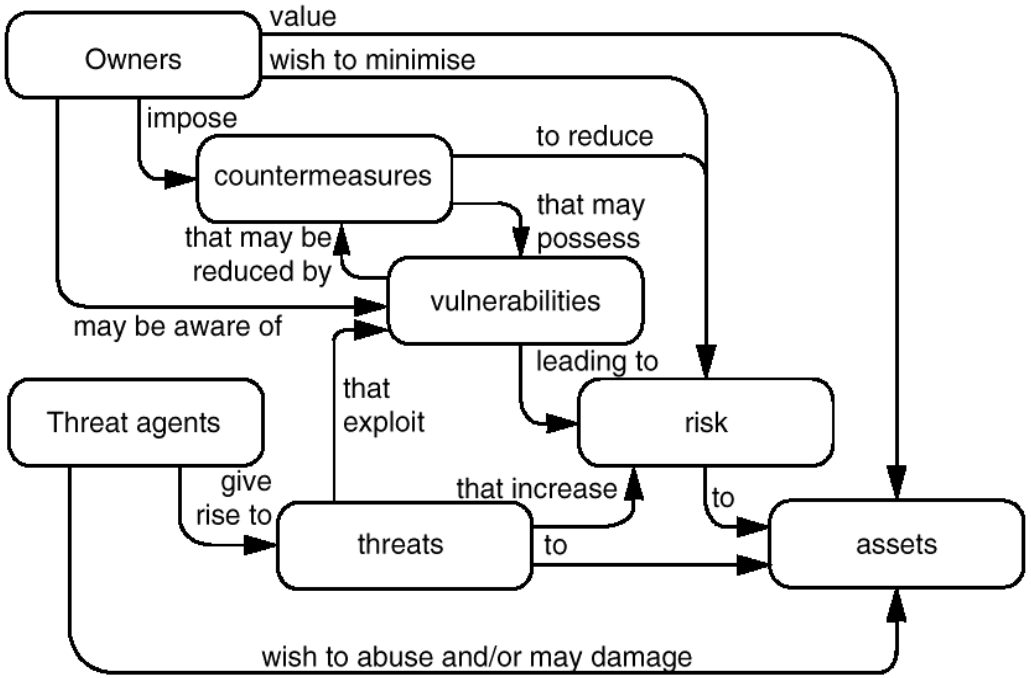
- IT Baseline Protection Manual (IT- Grundschutzhandbuch)
- Dikembangkan oleh GISA: German Information Security Agency
- Digunakan: evaluasi konsep keamanan & manual
- Metodologi evaluasi tidak dijelaskan
- Mudah digunakan dan sangat - detail - sekali
- Tidak cocok untuk analisis resiko
- Representasi tdk dalam grafik yg mudah dibaca

BSI (...cont'd)

- IT security measures
  - 7 areas
  - 34 modules (building blocks)
- Safeguards catalogue
  - 6 categories of security measures
- Threats catalogue
  - 5 categories of threats
- Security Measures (example):
  - Protection for generic components
  - Infrastructure
  - Non-networked systems
  - LANs
  - Data transfer systems
  - Telecommunications
  - Other IT components

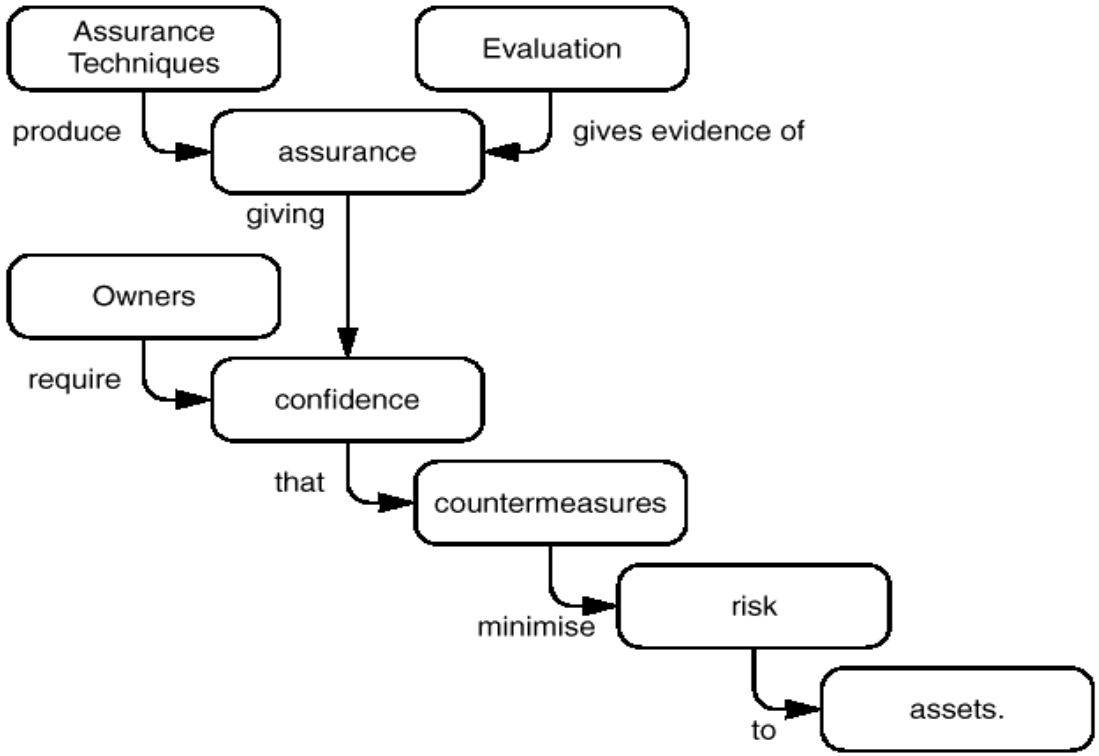
- Komponen generik:
  - Organisation
  - Personnel
  - Contingency Planning
  - Data Protection
- Infrastruktur:
  - Buildings, Cabling, Rooms, Office, Server Room, Storage Media Archives, Technical Infrastructure Room, Protective cabinets, Home working place
- Human error .....

ITSEC, Common Criteria

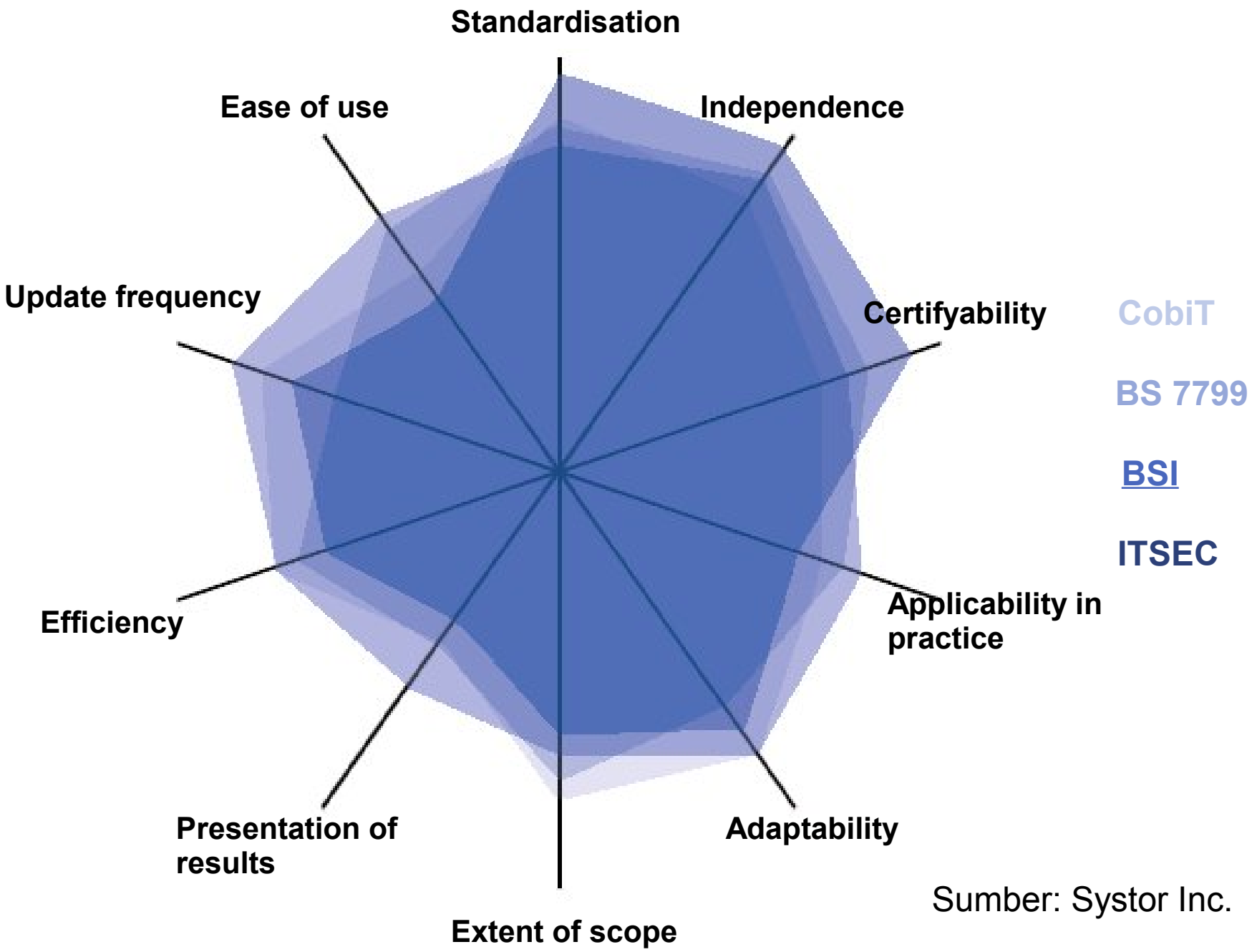


- ITSEC: IT Security Evaluation Criteria
- Developed by UK, Germany, France, Netherl. and based primarily on USA TCSEC (Orange Book)
- Based on systematic, documented approach for security evaluations of systems & products

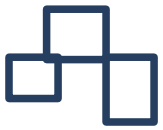
- Common Criteria (CC)
- Developed by USA, EC: based on ITSEC
- ISO International Standard
- Evaluation steps:
  - Definition of functionality
  - Assurance: confidence in functionality



Komparasi Metodologi

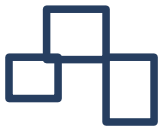


Sumber: Systor Inc.



19 Langkah Umum Audit TSI

- Kontrol lingkungan:
  1. Apakah kebijakan keamanan (security policy) memadai dan efektif ?
  2. Jika data dipegang oleh vendor, periksa laporan ttg kebijakan dan prosedural yg terikini dr external auditor
  3. Jika sistem dibeli dari vendor, periksa kestabilan finansial
  4. Memeriksa persetujuan lisen (license agreement)
- Kontrol keamanan fisik
  5. Periksa apakah keamanan fisik perangkat keras dan penyimpanan data memadai
  6. Periksa apakah backup administrator keamanan sudah memadai (trained,tested)
  7. Periksa apakah rencana kelanjutan bisnis memadai dan efektif
  8. Periksa apakah asuransi perangkat-keras, OS, aplikasi, dan data memadai
- Kontrol keamanan logikal
  9. Periksa apakah password memadai dan perubahannya dilakukan reguler
  10. Apakah administrator keamanan memprint akses kontrol setiap user

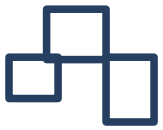


19 Langkah Umum Audit TSI (2)

11. Memeriksa dan mendokumentasikan parameter keamanan default
12. Menguji fungsionalitas sistem keamanan (password, suspend userID, etc)
13. Memeriksa apakah password file / database disimpan dalam bentuk tersandi dan tidak dapat dibuka oleh pengguna umum
14. Memeriksa apakah data sensitif tersandi dalam setiap phase dalam prosesnya
15. Memeriksa apakah prosedur memeriksa dan menganalisa log memadai
16. Memeriksa apakah akses kontrol remote (dari tempat yang lain) memadai: (VPN, CryptoCard, SecureID, etc)

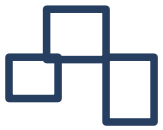
- Menguji Kontrol Operasi

17. Memeriksa apakah tugas dan job description memadai dalam semua tugas dalam operasi tsb
18. Memeriksa apakah ada problem yang signifikan
19. Memeriksa apakah kontrol yang menjamin fungsionalitas sistem informasi telah memadai



IT Forensic

- Bertujuan untuk mendapatkan fakta-fakta obyektif dari sebuah insiden / pelanggaran keamanan sistem informasi
- Fakta-fakta tersebut setelah diverifikasi akan menjadi bukti-bukti (evidence) yang akan digunakan dalam proses hukum
- Metodologi umum dalam proses pemeriksaan insiden sampai proses hukum:
  1. Pengumpulan data/fakta dari sistem komputer (harddisk, usb-stick, log, memory-dump, internet, dll) – termasuk di dalamnya data yang sdh terhapus
  2. Mendokumentasikan fakta-fakta yang ditemukan dan menjaga integritas data selama proses forensik dan hukum dengan proteksi fisik, penanganan khusus, pembuatan image, dan menggunakan algoritma HASH untuk pembuktian / verifikasi
  3. Merunut kejadian (chain of events) berdasarkan waktu kejadian
  4. Memvalidasi kejadian2 tersebut dengan metode “sebab-akibat”
  5. Dokumentasi hasil yang diperoleh dan menyusun laporan
  6. Proses hukum (pengajuan delik, proses persidangan, saksi ahli, dll)

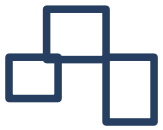


Kebutuhan

- Hardware:
  - Harddisk IDE & SCSI kapasitas sangat besar, CD-R, DVR drives
  - Memori yang besar (1-2GB RAM)
  - Hub, Switch, keperluan LAN
  - Legacy hardware (8088s, Amiga, …)
  - Laptop forensic workstations
- Software
  - Viewers (QVP http://www.avantstar.com/, http://www.thumbsplus.de/
  - Erase/Unerase tools: Diskscrub/Norton utilities)
  - Hash utility (MD5, SHA1)
  - Text search utilities (dtsearch http://www.dtsearch.com/)
  - Drive imaging utilities (Ghost, Snapback, Safeback,…)
  - Forensic toolkits
    - Unix/Linux: TCT The Coroners Toolkit/ForensiX
    - Windows: Forensic Toolkit
  - Disk editors (Winhex,…)
  - Forensic acquisition tools (DriveSpy, EnCase, Safeback, SnapCopy,…)
  - Write-blocking tools (FastBloc http://www.guidancesoftware.c) untuk memproteksi bukti-bukti

Forensik

- Prinsip:
  - Forensik bukan proses Hacking
  - Data yang didapat harus dijaga jgn berubah
  - Membuat image dari HD / Floppy / USB-Stick / Memory-dump adalah prioritas tanpa merubah isi, kadang digunakan hardware khusus
  - Image tsb yang diotak-atik (hacking) dan dianalisis – bukan yang asli
  - Data yang sudah terhapus membutuhkan tools khusus untuk merekonstruksi
  - Pencarian bukti dengan: tools pencarian teks khusus, atau mencari satu persatu dalam image



Kesimuplan

- CobiT: Metode audit untuk semua proses IT
- ITSEC, CC: Pendekatan evaluasi yang sistematik
- BS7799, BSI:
  - Evaluasi yang detail dan digunakan sebagai dokumentasi “best-practice”
  - Detailed audit plans, checklists, tools for technical audits (operating systems, LANs, etc.)
- IT Forensik:
  - Ilmu yang berhubungan dengan pengumpulan fakta dan bukti pelanggaran keamanan sistem informasi serta validasinya menurut metode yang digunakan (misalnya metode sebab-akibat)
  - Memerlukan keahlian dibidang IT (termasuk diantaranya hacking) – dan alat bantu (tools) baik hardware maupun software
- Auditor dan Dokter-komputer-forensik: penuh dengan tanggungjawab dan harus independen, diasses secara formal