Kendali dan Audit Sistem Informasi

Catatan: diolah dari berbagai sumber
Oleh: mardhani riasetiawan

Bidang Pekerjaan IT di perusahaan

- System Analyst
- Programmer
- Administrator (Network, system, database)
- Support (workshop, maintenance, helpdesk, dll)
- *Security Officer*
- Auditor

Audit

Systematic, independent and documented
process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Keuntungan Audit

- Menilai keefektifan aktivitas aktifitas dokumentasi dalam organisasi
- Memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan
- Mengukur tingkat efektifitas dari sistem
- Mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidaksesuaian di masa datang
- Menyediakan informasi untuk proses peningkatan
- Meningkatkan saling memahami antar departemen dan antar individu
- Melaporkan hasil tinjauan dan tindakan berdasarkan resiko ke Manajemen

IT Audit Area

- Planning
- Organization and Management
- Policies and procedures
- Security
- Regulation and standard

Jenis Audit (umum)

- Compliance
- Kinerja
- Kecurangan
- Sertifikasi

Jenis Audit (IT)

- System Audit
  - Audit terhadap sistem terdokumentasi untuk memastikan sudah memenuhi standar nasional atau internasional
- Compliance Audit
  - Untuk menguji efektifitas implementasi dari kebijakan, prosedur, kontrol dan unsur hukum yang lain
- Product / Service Audit
  - Untuk menguji suatu produk atau layanan telah sesuai seperti spesifikasi yang telah ditentukan dan cocok digunakan

Siapa yang Diaudit

- Management
- IT Manager
- IT Specialist (network, database, system analyst, programmer, dll.)
- User

Yang Melakukan Audit

Tergantung Tujuan Audit

- Internal Audit (first party audit)
  - Dilakukan oleh atau atas nama perusahaan sendiri
  - Biasanya untuk management review atau tujuan internal perusahaan
- Lembaga independen di luar perusahaan
  - Second party audit
    - Dilakukan oleh pihak yang memiliki kepentingan thd perusahaan
  - Third party audit
    - Dilakukan oleh pihak independen dari luar perusahaan. Misalnya untuk sertifikasi (ISO 9001, BS7799 dll).

Tugas Auditor IT

- Memastikan sisi-sisi penerapan IT memiliki kontrol yang diperlukan
- Memastikan kontrol tersebut diterapkan dengan baik sesuai yang diharapkan

Yang Dilakukan

- Persiapan
- Review Dokumen
- Persiapan kegiatan on-site audit
- Melakukan kegiatan on-site audit
- Persiapan, persetujuan dan distribusi laporan audit
- Follow up audit

Output kegiatan Audit

Hasil akhir adalah berupa laporan yang berisi:

- Ruang Lingkup audit
- Mekanisme Audit
- Temuan-temuan
- Ketidaksesuaian (sifat ketidaksesuaian, bukti2 pendukung, syarat yg tdk dipenuhi, lokasi, tingkat ketidaksesuaian)
- Kesimpulan (tingkat kesesuaian dengan kriteria audit, efektifitas implementasi, pemeliharaan dan pengembangan sistem manajemen, rekomendasi)

Ketrampilan yang dibutuhkan

- Audit skill : sampling, komunikasi, melakukan interview, mengajukan pertanyaan, mencatat
- Generic knowledge : pengetahuan mengenai prinsip2 audit, prosedur dan teknik, sistem manajemen dan dokumen2 referensi, organisasi, peraturan2 yang berlaku
- Specific knowledge : background IT/IS, bisnis, specialist technical skill, pengalaman audit sistem manajemen, perundangan

Prinsip-prinsip Audit

- Ethical conduct
  - Berdasar pada profesionalisme, kejujuran, integritas, kerahasiaan dan kebijaksanaan
- Fair Presentation
  - Kewajiban melaporkan secara jujur dan akurat
- Due professional care
  - Implementasi dari kesungguhan dan pertimbangan yang diberikan
- Independence
- Evidence-base approach

  pendekatan berdasarkan fakta

Peraturan dan Standar yang Biasa Digunakan

- ISO / IEC 17799 and BS7799
- Control Objectives for Information and related Technology (CobiT)
- ISO TR 13335
- IT Baseline Protection Manual
- ITSEC / Common Criteria
- Federal Information Processing Standard 140-1/2 (FIPS 140-1/2)
- The “Sicheres Internet” Task Force [Task Force Sicheres Internet]
- The quality seal and product audit scheme operated by the Schleswig-Holstein Independent State Centre for Data Privacy Protection (ULD)
- ISO 9000

Dunia Industri

- CobiT

  Control Objectives for Information and Related Technology

- BS7799

CobiT

Control Objectives for Information and Related Technology

CobiT

- Dibuat oleh organisasi ISACA (Information Systems Audit and Control Association) dan dikembangkan oleh IT Governance Institute

focus on audit, control and security issues

Badan (Indonesia)

- ISACA Indonesian Chapter (isaca.or.id)
- ISSA (Information System Security Association) Indonesian Chapter

Sertifikasi

- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- CISSP (Certified IS Security Professional)
- CIA (Certified Internal Auditor)

Kualifikasi :

Pengalaman dan pengetahuan untuk mengidentifikasi, mengevaluasi, dan memberikan rekomendasi berupa solusi untuk mengurangi kelemahan sistem IT

> Mengeluarkan sertifikasi untuk personal auditor

Misi CobiT

Melakukan penelitian, pengembangan, publikasi dan promosi terhadap control objective dari teknologi informasi yang secara umum diterima di lingkungan internasional untuk pemakaian sehari-hari oleh manager dan auditor

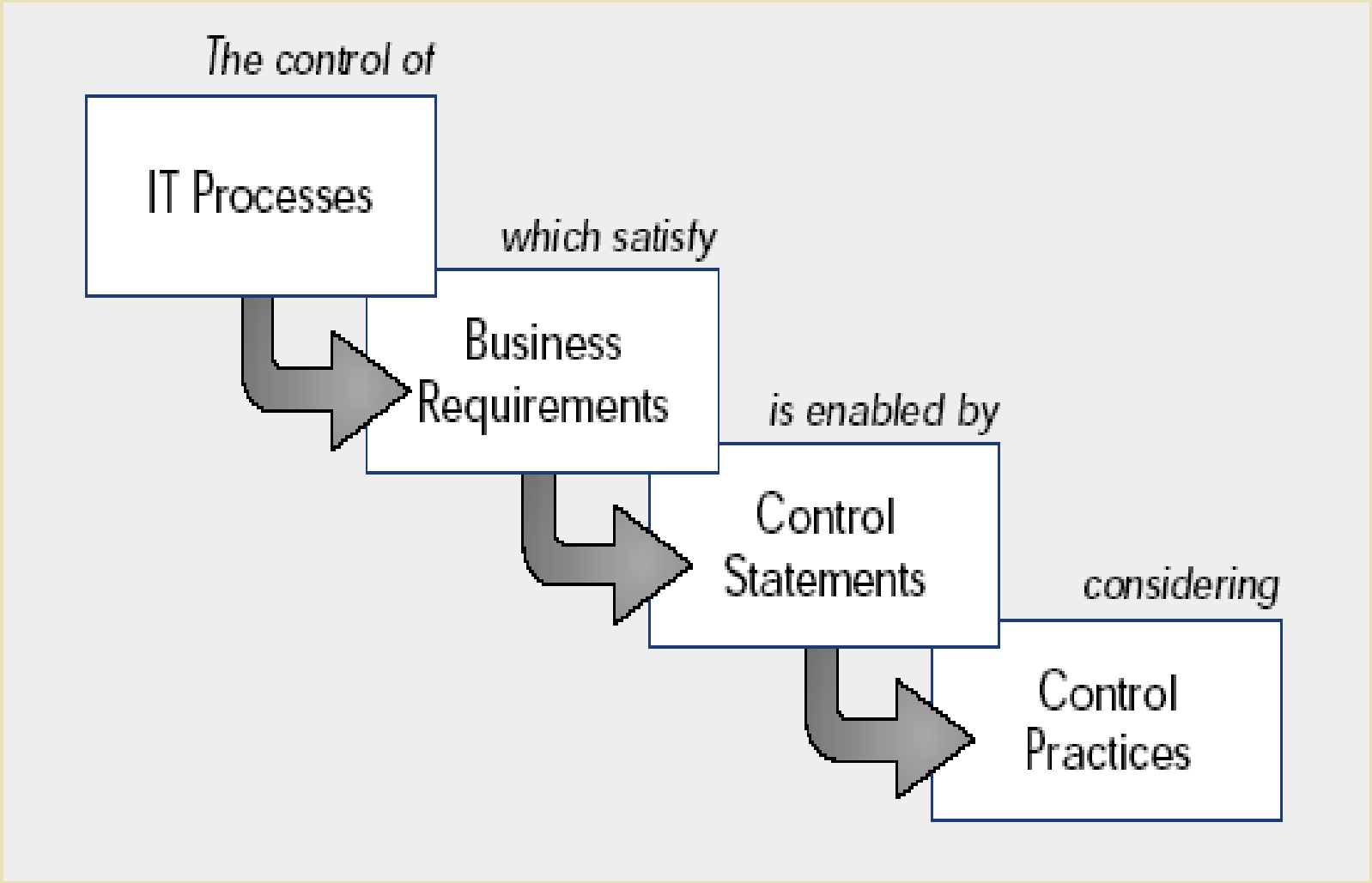
Lingkup CobiT
4 domains

- Planning & Organization
- Acquisition & Implementation
- Delivery & Support
- Monitoring

CobiT Control Objectives

- Defining controls that should be in place
- 34 processes
- 3-30 detailed IT Control Objectives

Pola Pikir


The control of
IT Processes
which satisfy
Business Requirements
is enabled by
Control Statements
considering
Control Practices

PO1 Planning & Organisation
Define a Strategic Information Technology Plan

COBIT

Control over the IT process of

defining a strategic IT plan

that satisfies the business requirement

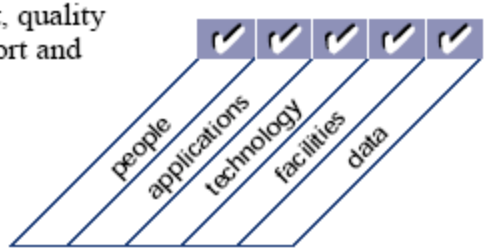
to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

is enabled by

a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals

and takes into consideration

- enterprise business strategy
- definition of how IT supports the business objectives
- inventory of technological solutions and current infrastructure
- monitoring the technology markets
- timely feasibility studies and reality checks
- existing systems assessments
- enterprise position on risk, time-to-market, quality
- need for senior management buy-in, support and critical review



Control Domain Planning & Organisation

DOMAIN		PROCESS
Planning & Organisation	PO1	Define a strategic IT plan
	PO2	Define the information architecture
	PO3	Determine technological direction
	PO4	Define the IT organisation and relationships
	PO5	Manage the IT investment
	PO6	Communicate management aims and direction
	PO7	Manage human resources
	PO8	Ensure compliance with external requirements
	PO9	Assess risks
	PO10	Manage projects
	PO11	Manage quality

Control Domain Acquisition & Implementation

Acquisition & Implementation	AI1	Identify automated solutions
	AI2	Acquire and maintain application software
	AI3	Acquire and maintain technology infrastructure
	AI4	Develop and maintain procedures
	AI5	Install and accredit systems
	AI6	Manage changes

Control Domain Delivery & Support

Delivery & Support	DS1	Define and manage service levels
	DS2	Manage third-party services
	DS3	Manage performance and capacity
	DS4	Ensure continuous service
	DS5	Ensure systems security
	DS6	Identify and allocate costs
	DS7	Educate and train users
	DS8	Assist and advise customers
	DS9	Manage the configuration
	DS10	Manage problems and incidents
	DS11	Manage data
	DS12	Manage facilities
	DS13	Manage operations

Control Domain Monitoring

Monitoring	M1	Monitor the processes
	M2	Assess internal control adequacy
	M3	Obtain independent assurance
	M4	Provide for independent audit

BS7799

What's BS7799

- Sebuah pendekatan berbasis 'resiko' dalam mendefinisikan kebijakan dan prosedur serta untuk memilih kontrol yang memadai untuk mengelola resiko
- ISO/IEC 17799
  - Information technology – code of practice for information security management
- BS 7799
  - Information security management systems – Specification with guidance for use

ISO/IEC 17799:2000 Information Technology – Code of Practice for Information Security Management

- Contents identical to BS7799-1:1999
- Contains a comprehensive listing of approved procedures and information security measures
- Recommendation of measures structured in 10 sections
- This code of practice serves a basis for the understanding of the requirements as contained in BS7799-2
- Is not suited to serve as sole basis for certifications

BS7799-2:2002 Information Security Management Systems – Specification with guidance for use

- Based on BS7799-1:1999, but ISMS is based on the selection of measures as contained in BS7799-2:2002
- Is a suitable basis for ISMS system certification
- Contains requirements for ISMS (new:PDCA-Cycle and continuous Improvement)
- 127 controls structured in :
  - 10 detailed control clauses containing
  - 36 control objectives

Lain-lain

Kebutuhan auditor IT

- Internal Audit -> setiap perusahaan memerlukan
- Perusahaan penyedia layanan audit
- Perusahaan penyedia sertifikasi

Peluang

- Ketergantungan terhadap IT semakin besar sehingga muncul kebutuhan untuk melakukan audit IT
- Auditor IT yang sekarang banyak yang berasal bukan dari bidang IT
- Banyak permasalahan (bisnis) dalam pengelolaan IT