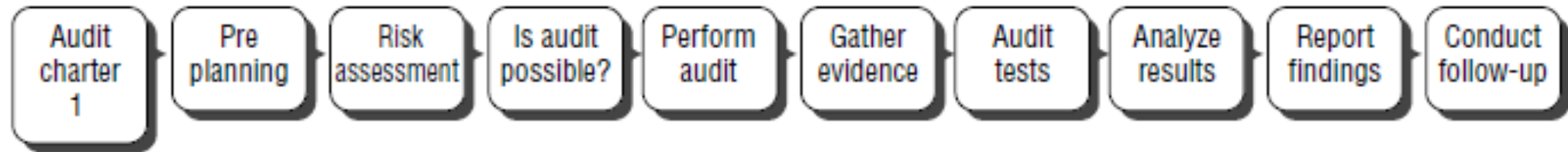


AUDIT PROCESS (CISA Study Guide) -Audit Evidence

Dr. Yeffry Handoko Putra, S.T, M.T,
CISA

Thank's to : Rofi Firdaus (7.51.15.038), Maya Hermawati (7.51.15.033), Sri Anggraeni (7.51.15.040)

- Tugas IS Auditor: memberikan jaminan bahwa sasaran audit dipenuhi menggunakan standar audit professional
- Ada 10 tahap yang harus diperhatikan dalam melaksanakan audit:



1. Establishing and Approving an Audit Charter

- Audit Charter dikeluarkan oleh manajemen eksekutif atau dewan direksi
- Audit Charter berisi mengenai:
 1. Responsibility
 2. Authority
 3. Accountability

Audit Committee

- Audit committee terdiri dari para eksekutif misalnya CEO
- Audit committee menyetujui audit charter dan memberikan wewenang kepada internal dan eksternal audit
- Tujuan audit committee adalah untuk memberikan saran kepada executive mengenai strategi pengendalian internal, prioritas dan jaminan
- Audit committee memiliki wewenang untuk meninjau pengendalian internal yang dilakukan oleh manajemen eksekutif
- Audit committee mengelola kegiatan audit serta hasil audit baik dari internal maupun eksternal auditor.

2. Preplanning Specific Audit

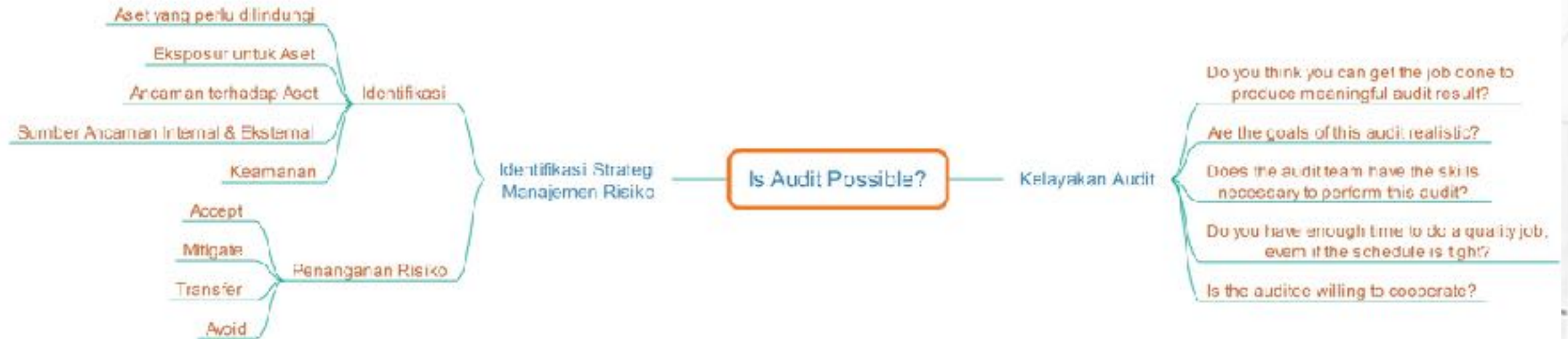
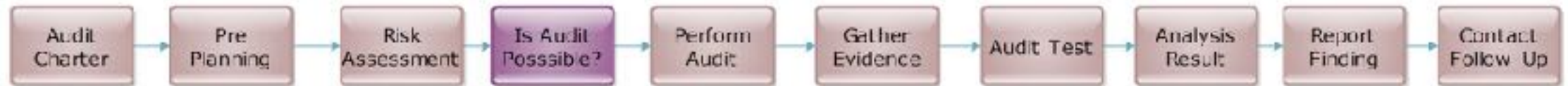
- Menentukan tujuan/sasaran audit
- Menentukan ruang lingkup
- Memahami macam-macam audit
- Mengidentifikasi pembatasan ruang lingkup
- Mengumpulkan kebutuhan audit yang detail
- Menggunakan pendekatan yang sistematis untuk perencanaan

3. Performing an Audit Risk Assessment

Risk assessment dilakukan untuk memastikan bahwa bukti-bukti dapat dikumpulkan selama proses audit

- Inherent Risks
- Detection Risks
- Control Risks
- Business Risks
- Technological Risks
- Operational Risks
- Residual Risk
- Audit Risk

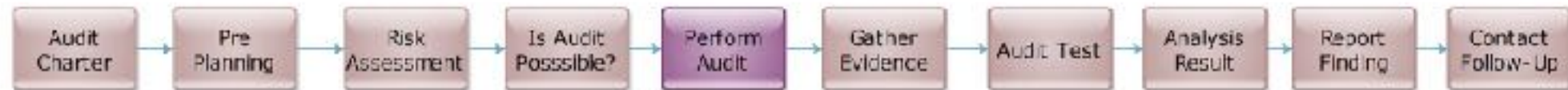
Determining Whether an Audit Is Possible



RISK



Performing the Audit



1. Selecting the Audit Team

- Menentukan personil audit dan menentukan struktur organisasi audit.
- Membuat rencana sumber daya personil
- Mengidentifikasi fungsi khusus dan keahlian yang diperlukan untuk menyelesaikan tujuan audit.



2. Determining Competence and Evaluating Auditors

Dapat menggunakan standar ISO untuk memperjelas apa yang diperlukan untuk menjadi auditor yang kompeten dalam hal pendidikan prasyarat, pengalaman kerja, dan pelatihan



2. Determining Competence and Evaluating Auditors

TABLE 3.2 Competence of auditors and technical experts

	Audit Team Leader	Competent Auditor	Technical Expert
Auditor with experience in at least three complete audits.	X		
Capability to communicate effectively in writing and oral presentations. Should possess good negotiating skills.	X		
Secondary-level education.	X	X	X
4+ years of full-time practical work experience in related to IT.	X	X	X
Successfully completed 5+ days of training covering the subject matter of the audit.	X	X	

2. Determining Competence and Evaluating Auditors

- Membuat Skill Matrix

Tujuan dari matriks keterampilan adalah untuk memastikan bahwa tim memiliki orang yang tepat dengan kualifikasi yang tepat mengerjakan tugas yang tepat

Contoh Skill Matrix

Audit Task	Person	Training or Certification	Related Work Experience
# 8: Review of existing policies and records for PCI user training, all security, system configuration, and incident response.	M. Anderson	IA, CISA	Internal auditor
# 9: PCI section 11 network perimeter analysis.	J.T. Jennings	CISA, Network+, CCNA	PCI and PCI section 11 testing
# 10: Conduct enumeration scan of network hosts and open ports. Exclude "Zeus" server and customer service computers.	R. Martin	CISA	XP admin, BSD Unix admin
# 14: Select logs for review. Supervise and assist in review with B. Goldfield performing task.			
# 15: Catalog system log file data for analysis of past events to forensic-test the incident response.	B. Goldfield	BS computer science	Intern, system analyst

3. Ensuring Audit Quality Control

- Mengenal kualitas, dengan cara:
 1. Mendefinisikan kualitas sebagai kesesuaian dengan spesifikasi.
 2. Perencanaan dan pencegahan menciptakan kualitas.



3. Ensuring Audit Quality Control

Ketika merancang proses Quality Control, auditor harus melakukan hal berikut:

1. Menggunakan metodologi audit (didokumentasikan rencana dan prosedur).
2. Memahami tentang kebutuhan dan harapan auditee.
3. Menyimpan daftar tugas yang harus diselesaikan.
4. Memahami siklus bisnis dan waktu.
5. Wawancara klien.
6. Survei kepuasan pelanggan.
7. Menyetujui kerangka acuan yang digunakan oleh klien, auditee, dan auditor.
8. Membangun metrik kinerja audit.
9. Ukur rencana audit terhadap kinerja aktual.
10. Menanggapi keluhan.

4. Establishing Contact With the Auditee

Agar efektif dalam komunikasi, dapat melakukan hal-hal berikut dengan Audit :

1. Mengidentifikasi tujuan audit, layanan, dan ruang lingkup
2. Fokus dengan masalah dan kendala
3. Menanggapi pertanyaan klien dan keluhan
4. Berurusan dengan isu-isu di luar lingkup audit
5. Memahami waktu dan penjadwalan-mengetahui kapan klien mengharapkan pekerjaan
6. Mengetahui pelaporan kapan dan bagaimana klien ingin mendengar
7. Memperoleh kesepakatan dengan klien
8. Menjaga kerahasiaan
9. Memberikan penanganan khusus untuk bukti penyimpangan atau tindakan ilegal

5. Making Initial Contact with the Auditee

Communication Schedule

auditor profesional akan memberitahu jadwal komunikasi, mengidentifikasi tanggal dan waktu pertemuan, laporan, dan segala sesuatu yang lain yang diperlukan

1. **Mengidentifikasi Stakeholder**
2. **Communication Requirements**
3. **Message Content**
4. **Confidentiality Requirements**
5. **Communication Technology**
6. **Complaint Process**



6. Using Data Collection Techniques

Untuk mengumpulkan data yang berguna, auditor akan menggunakan kombinasi teknik, diantaranya yaitu:



7. Conducting Document Review

Salah satu tahapan dalam audit adalah untuk melakukan review dokumen. Tujuannya adalah untuk memperoleh pemahaman tentang informasi yang dapat digunakan untuk membantu memandu audit. Selain itu untuk menentukan apakah auditee benar-benar mengikuti prosedur.



8. Understanding the Hierarchy of Internal Controls

Setiap auditor harus mempertimbangkan dua hal mendasar mengenai pengendalian internal:

Issue 1 : Management Is Often Exempt from Controls, Manajemen Kontrol memiliki tanggung jawab menginstal kontrol untuk organisasi, namun beberapa eksekutif dibebaskan dari kontrol mereka sendiri.

Issue 2 : How Controls Are Implemented Determines the Level of Assurance, Pelaksanaan kontrol yang kuat memberikan kontribusi ke tingkat jaminan, yang dapat dikonfirmasi oleh auditor. Jaminan yang kuat berarti itu merupakan 95 persen atau lebih besar tingkat kebenaran.

9. Reviewing Existing Controls

Tujuan dari pengendalian internal dapat diklasifikasikan ke dalam salah satu dari tiga kategori:

1. **Preventative**, Kontrol pencegahan yang berusaha untuk menghentikan (mencegah) masalah dari terjadi.
2. **Detective**, Kontrol detektif yang dimaksudkan untuk menemukan masalah. Auditing adalah kontrol detektif untuk menemukan informasi.
3. **Corrective**, Kontrol korektif yang berusaha untuk memperbaiki masalah setelah deteksi.

Sedangkan kontrol dari tiga kategori tingkat menengah dilaksanakan dengan menggunakan salah satu dari tiga metode berikut:

1. **Administrative**, Menggunakan kebijakan dan prosedur tertulis (berdasarkan orang)
2. **Technical**, Melibatkan proses software atau hardware untuk menghitung hasilnya (teknologi khusus)
3. **Physical**, pencegahan fisik /visual

Contoh Control dan Metode Implementasi

TABLE 3.4 Controls and methods of Implementation

Control Type	Implementation Method	Some Examples
Preventative "stops"	Administrative	Hiring procedures, background checks, segregation of duties, training, change control process, acceptable use policy (AUP), organizational charts, job descriptions, written procedures, business contracts, laws and regulations, risk management, project management, service-level agreements (SLAs), system documentation
	Technical	Data backups, virus scanners, designated redundant high-availability system ready for failover (HA standby), encryption, access control lists (ACLs), system certification process
	Physical	Access control, locked doors, fences, property tags, security guards, live monitoring of CCTV, human-readable labels, warning signs

10. Preparing the Audit Plan

Ketua tim audit harus mempersiapkan rencana audit termasuk penjadwalan dan koordinasi kegiatan. detail harus sesuai dengan ruang lingkup dan kompleksitas audit dengan fleksibilitas untuk perubahan. Rencana audit selesai harus ditinjau dan diterima oleh klien audit dan disampaikan kepada auditee sebelum kegiatan penukaran dimulai.

Selama audit, harus mempersiapkan catatan untuk menjawab pertanyaan-pertanyaan berikut:

1. Siapa yang terlibat?
2. Apa yang diaudit, bagaimana bukti yang diperoleh, dan apa prosedur tes khusus yang digunakan?
3. Kapan terjadi?
4. Dimana itu terjadi?
5. Mengapa (tujuan audit)?
6. Bagaimana rencana dan prosedur audit dilaksanakan?

Kemudian, kertas kerja akhir auditor harus disimpan ke dalam arsip dokumentasi audit, termasuk salinan dari laporan yang dikeluarkan.

11. Assigning Work to the Audit Team

Contoh tanggung jawab pekerjaan untuk berbagai anggota tim audit

	Lead Auditor	Auditor	Technical Expert	Auditor in Training	Guide
Manage audit team	X	X			
Communicate issues to client or auditee	X			Observe	
Facilitate access to personnel and resources					X
Manage technical experts		X		Observe	
Facilitate escalation assistance	X	X			X
Collect samples		X	Assist	Observe	
Perform testing		X	Assist	Observe	
Analyze results		X	Assist	Observe	
Determine findings		X		Assist	
Prepare reports		X		Assist	
Perform quality control	X			Assist	

12. Preparing Working Documents

Dokumen kerja dibuat dan disimpan dalam bentuk hard copy dan elektronik untuk merekam informasi, catatan dokumen dari pertemuan, katalog bukti pendukung, memastikan konsistensi selama pengujian bukti, dan mencatat temuan audit.

Working Papers Checklist

1. Tujuan Audit
2. Kriteria Audit dan dokumen referensi
3. Lingkup Audit
4. Tanggal dan tempat-tempat di mana kegiatan penukaran yang harus dilakukan
5. Waktu dan durasi kegiatan audit yang diharapkan, termasuk pertemuan dengan pertemuan tim auditee
6. Peran dan tanggung jawab tim audit
7. Alokasi sumber daya ke daerah-daerah kritis audit
8. Identifikasi perwakilan auditee untuk audit
9. Topik laporan Audit
10. Pemeriksaan tindak lanjut

13. Conducting Onsite Audit Activities

Membuat Agenda

1. Konfirmasi rencana tujuan audit
2. Identifikasi kewenangan untuk melaksanakan audit (charter)
3. Mengidentifikasi lokasi dan sumber daya yang diperlukan
4. Membuat ringkasan singkat tentang bagaimana kegiatan audit yang akan dilakukan
5. Konfirmasi melalui komunikasi
6. Konfirmasi jadwal pertemuan (wawancara, semua pertemuan selama audit, ulasan, tanggal dan waktu penutupan rapat)
7. Memberikan kesempatan auditee untuk mengajukan pertanyaan

Gathering Audit Evidence

1. **Using evidence to prove a point**
2. **Understanding types of evidence :**
 - Direct evidence
 - Indirect evidence
3. **Selecting audit samples**
 - Statistical Sampling : Random sampling, Cell sampling, Fixed interval sampling
 - Nonstatistical Sampling
4. **Recognizing Typical Evidence for IS Audit**

Examples of the various types of audit evidence :

 - Documentary evidence
 - Data extraction
 - Auditee Claim
 - Analysis of plan, policies, procedures, and flowchart
 - Result of compliance and substantive audit test
 - Auditor's observation

Gathering Audit Evidence

5. Using Computer-Assisted Audit Tools

Teknik dan kelemahan CAAT :

- Host evaluation tools untuk membaca pengaturan konfigurasi sistem dan mengevaluasi host
- Network traffic dan analisis protocol menggunakan sniffer
- Pemetaan dan pelacakan alat-alat yang menggunakan pendekatan tracer-bullet untuk mengikuti proses melalui aplikasi perangkat lunak menggunakan data uji
- Pengujian konfigurasi perangkat lunak aplikasi tertentu seperti database SQL
- Perhitungan lisensi software di seluruh jaringan
- Pengujian password compliance pada account user login

Gathering Audit Evidence

Menggunakan CAAT untuk Online Audit berkelanjutan :

6 jenis online auditing berkelanjutan :

- Online Event Monitors
- Embedded Program Audit Hooks
- Continuous and Intermittent Simulation (CIS) Audit
- Snapshot Audit
- Embedded Audit M (EAM)
- System Audit Control Audit Review with Embedded Audit Modules

Gathering Audit Evidence

6. **Understanding Electronic Discovery**

7. **Grading of Evidence**

Kriteria dari sebuah bukti :

- Material Relevance
- Evidence Objectivity
- Competency of the Evidence Provider
- Evidence Independence

8. **Timing of Evidence**

9. **Following the Evidence Life Cycle**

7 fase dari evidence life cycle : identifikasi, pengumpulan, awal pelestarian penyimpanan, analisis, postanalysis, presentasi, dan kembalinya bukti kepada pemilik

Conducting Audit Evidence Testing

1. **Compliance Testing**

Compliance testing didasarkan pada salah satu dari jenis sampel pemeriksaan berikut :

- Attribute Sampling
- Stop-And-Go Sampling
- Discover Sampling
- Precision or Expected Error Rate

2. **Substantive Testing**

Substantive testing didasarkan pada salah satu dari jenis sampel pemeriksaan berikut :

- Variable Sampling
- Unstratified Mean Estimation
- Stratified Mean Estimation
- Difference Estimation

Conducting Audit Evidence Testing

3. Tolerable Error Rate

Tolerable error rate digunakan untuk menunjukkan jumlah maksimum kesalahan yang dapat eksis tanpa menyatakan salah saji material.

- Untuk compliance testing, tolerable error rate adalah maksimal deviation dari prosedur yang sudah disetujui oleh auditor.
- Dalam pengujian substantif, auditor menggunakan penilaian mereka mengenai materi relevansi dan menyimpulkan apakah tujuan audit telah tercapai. Prosedur tes dan Hasil harus menunjukkan benar atau gagal. Sebuah auditor yang cerdas akan selalu bersandar ke sisi konservatif untuk keselamatan dalam pengukuran mereka.

Conducting Audit Evidence Testing

4. **Record Your Test Result**

Setiap temuan bukti dapat diklasifikasikan ke dalam salah satu pernyataan pelaporan umum, disajikan dalam urutan yang paling diinginkan untuk paling tidak diinginkan:

- Nothworthy Achievement
- Conformity
- Opportunities for Improvement
- Concern
- Noncomformity

Conducting Audit Evidence Testing

5. **Generate Audit Findings**

Menggunakan rencana audit Anda sebagai peta jalan, saatnya untuk menganalisis sampel bukti. Tujuannya adalah untuk menentukan apakah sampel yang diuji oleh auditor menunjukkan kesesuaian (memenuhi persyaratan atau ketidaksesuaian (gagal persyaratan Kami memiliki dua keprihatinan sebagai auditor terkait dengan pengujian: .kecukupan bukti dan contra directory evidence :

- **Sufficiency of Evidence**
- **Contradictory Evidence**

6. **Detecting Irregularities and Illegal Acts**

Contoh aktivitas ilegal : Penipuan, Pencurian, Menekan, Regulatory Violations

Conducting Audit Evidence Testing

7. Indicators of Illegal or Irregular Activity

Auditor harus memahami bahwa pengendalian organisasi internal tidak akan menghilangkan kemungkinan tidak teratur atau illegal activity. Meskipun bukan pekerjaan auditor untuk mendeteksi kondisi ini, penting untuk waspada terhadap indikator potensial. auditor harus sadar akan gejala berikut:

- Pembayaran yang diragukan
- Unsatisfactory Record Control
- Unsatisfactory Explanation

Conducting Audit Evidence Testing

8. Responding of Illegal or Irregular Activity

Jika anda menemukan aktivitas yang berpotensi iregular atau ilegal, langkah berikutnya adalah untuk mencoba untuk menentukan apakah manajemen menyadari situasi tersebut atau telah berpartisipasi dalam kegiatan yang dicurigai. auditor harus mendokumentasikan semua informasi, bukti, temuan, dan kesimpulan yang menyebabkan penemuan kegiatan dicurigai:

- auditor harus mempertimbangkan hubungan yang tidak biasa atau tak terduga yang dapat menyebabkan salah saji material atau kekeliruan.
- auditor harus mempertahankan posisi skeptisisme profesional.
- Setelah belajar dari penyimpangan materi atau tindakan ilegal, auditor harus segera memberitahukan satu tingkat dari manajemen yang lebih tinggi di mana kegiatan yang diduga mungkin terjadi
- Jika kegiatan melibatkan orang yang dibebankan dengan kontrol internal atau governance, pelaporan harus dilakukan pada tingkat tertinggi .
- auditor tidak harus menghubungi penegak hukum atau regulator sampai disarankan untuk dilakukan oleh penasihat hukum auditor. prosedur penanganan khusus biasanya diperlukan untuk melindungi auditor.
- auditor tidak harus pernah menjadi pihak yang terlibat dalam aktivitas tersebut. Auditor harus mencari nasihat hukum yang kompeten jika tidak yakin tentang apa tindakan untuk mengambil. Anda mungkin disarankan untuk mempersiapkan penghentian audit.

Conducting Audit Evidence Testing

1. Findings Outside of Audit Scope

Setelah melakukan audit, langkah berikutnya adalah mempersiapkan presentasi untuk melaporkan temuan. Pelaporan adalah proses dimana manajemen auditor menyampaikan temuan mereka, termasuk yang berikut:

- Audit scope
- Audit objective
- Methods and criteria used
- Nature of findings
- Extent of work perform
- Applicable dates of coverage

Selain itu, laporan akhir harus menyatakan pembatasan, pemesanan, atau kualifikasi (concems) bahwa auditor memegang kendali dalam dengan audit. Auditor dapat memberikan pendapat akhir atau tidak ada pendapat berdasarkan keterbatasan potensial. Auditor dapat mengeluarkan pendapat yang memenuhi syarat atau wajar tanpa pengecualian:

- A qualified opinion
- An unqualified opinion

Report Findings

Setelah melakukan audit, langkah berikutnya adalah mempersiapkan presentasi untuk melaporkan temuan. Pelaporan adalah proses dimana manajemen auditor menyampaikan temuan mereka, termasuk yang berikut:

- Audit scope
- Audit objective
- Methods and criteria used
- Nature of findings
- Extent of work perform
- Applicable dates of coverage

Selain itu, laporan akhir harus menyatakan pembatasan, pemesanan, atau kualifikasi (concerns) bahwa auditor memegang kendali dalam dengan audit. Auditor dapat memberikan pendapat akhir atau tidak ada pendapat berdasarkan keterbatasan potensial. Auditor dapat mengeluarkan pendapat yang memenuhi syarat atau wajar tanpa pengecualian:

- A qualified opinion
- An unqualified opinion

Report Findings

1. Approving and Distributing the Audit Report

Draft laporan audit harus didistribusikan kepada personil auditee yang berpartisipasi dalam audit. Banyak detail mungkin relatif rahasia atau sensitif. Ketua tim audit dapat menentukan bahwa tindakan terbaik adalah untuk berbagi bagian dari laporan hanya dengan orang yang bertanggung jawab untuk daerah tertentu. Auditee dan klien harus diberi kesempatan untuk setuju atau tidak setuju dengan draft laporan auditor. Komentar mereka harus direkam untuk dimasukkan ke laporan akhir auditor. Ini adalah kontrol kualitas yang sangat penting untuk proses tersebut yang harus terjadi pada setiap audit. Hal ini tidak perlu untuk auditor untuk menyetujuinya, tapi perlu untuk memberikan auditee kesempatan untuk menyuarakan ketidaksesuaian atau keluhan. Banyak masalah hanya kata-kata politik ketimbang perselisihan temuan. Namun, pada akhirnya, laporan audit harus sesuai kebenaran sebagai diverifikasi oleh auditor

Report Findings

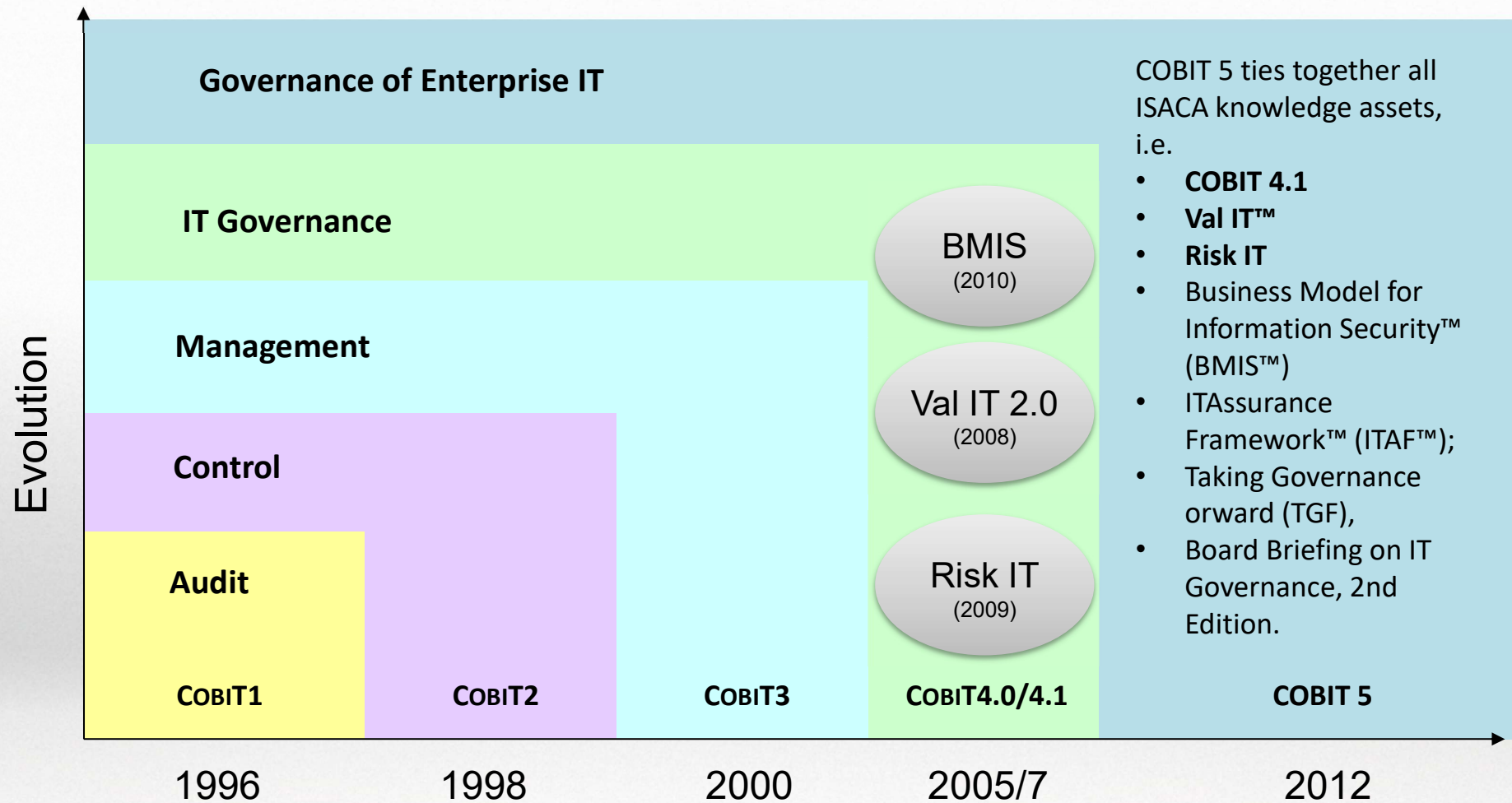
2. Identifying Omitted Procedures

Pada kesempatan yang langka auditor setelah menentukan mengeluarkan draft atau finalreport bahwa satu atau lebih prosedur audit telah dihilangkan, mungkin perlu untuk peninjauan beberapa alternatif audit untuk mengimbangi kelalaian, Jika lubang prosedur dihilangkan materi hadir bantalan pada hasil, dan alternatif audit tidak dapat mengimbangi efisiensi, membatalkan laporan dan penerbitan kembali laporan baru (jika sesuai) mungkin diperlukan. Jika prosedur dihilangkan maka akan memiliki bukti yang nyata pada hasil, auditor harus berkonsultasi dengan pengacara mereka untuk saran conceming setiap jalan yang mungkin atau tindakan hukum yang potensial

Conducting Follow-Up (Closing Meeting)

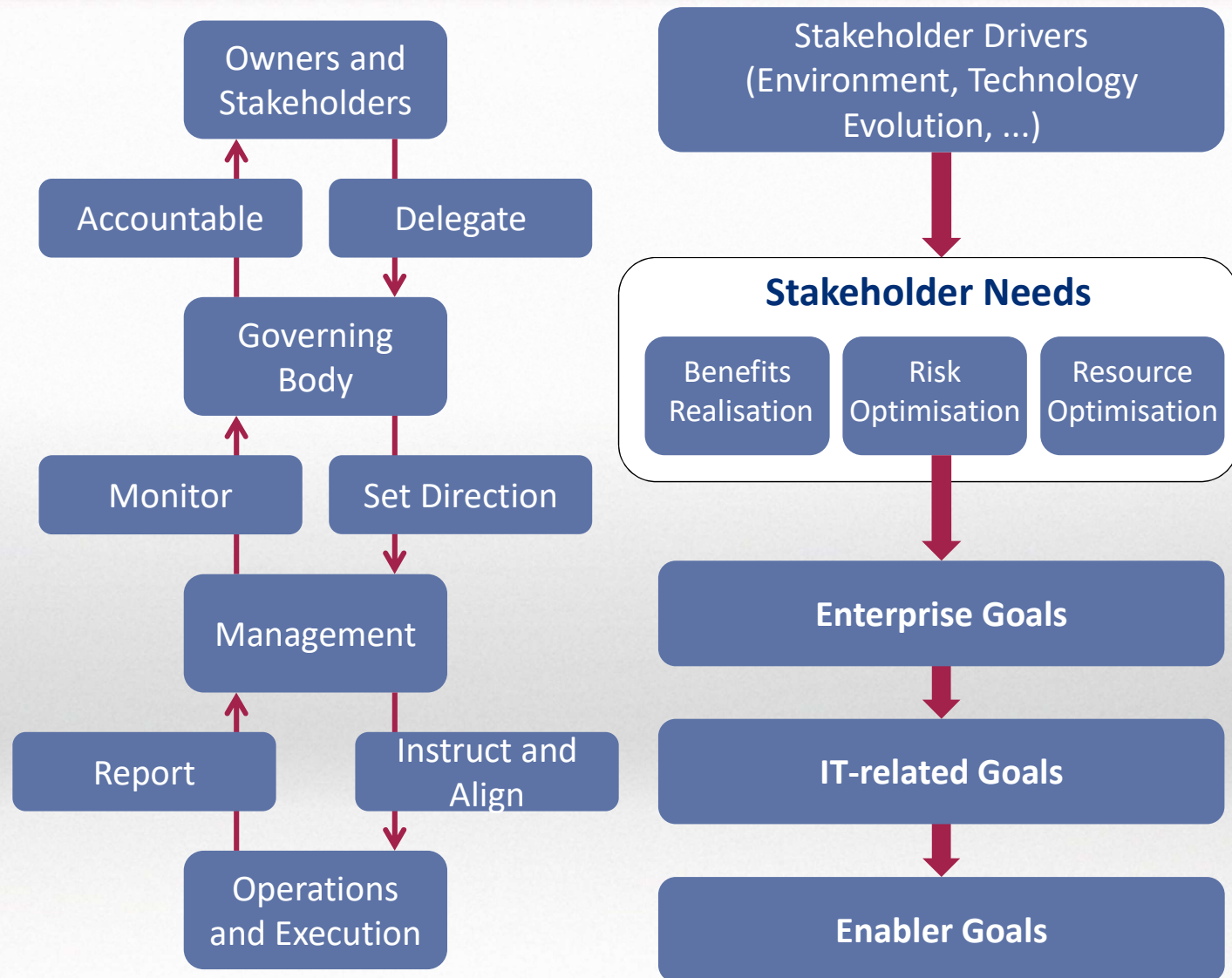
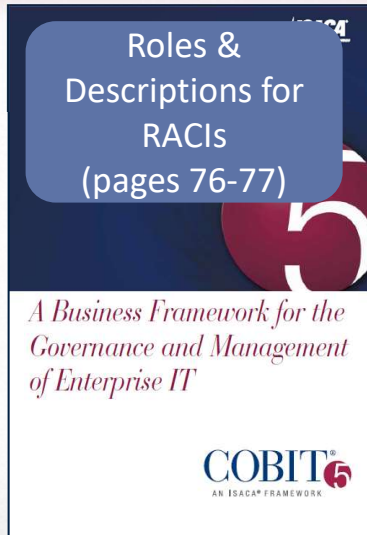
Setelah mengeluarkan laporan, auditor melakukan sebuah exit interview dengan manajemen untuk mendapatkan komitmen untuk rekomendasi yang dibuat dalam audit. Manajemen bertanggung jawab atas akuisisi rekomendasi, dan menunjuk apapun tindakan korektif akan diambil, termasuk tanggal-tanggal perkiraan tindakan. Dalam audit berikutnya, Anda akan memeriksa apakah manajemen menghormati komitmen mereka untuk memperbaiki atau memulihkan kekurangan yang ditemukan dalam audit sebelumnya. Kadang-kadang, kekurangan dibiarkan tidak dikoreksi karena perubahan dalam desain atau praktek organisasi telah menghilangkan kondisi kelemahan kontrol sebelum ini. Temuan tertentu mungkin berlaku untuk peristiwa yang tidak lagi relevan. Jika tidak, Anda berharap manajemen untuk bertindak pada waktu yang tepat untuk memperbaiki kekurangan sebagai awalnya dilaporkan.

The Evolution of COBIT 5



© 2013 ISACA. All Rights Reserved.

The People and the Process



COBIT 5 Enterprise Goals				
BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

© 2013 ISACA. All Rights Reserved.

COBIT 5 Enterprise Goals		
ITBSC Dimension	Information and Related Technology Goal	
Financial	01	Alignment of IT and business strategy
	02	IT compliance and support for business compliance with external laws and regulations
	03	Commitment of executive management for making IT-related decisions
	04	Managed IT-related business risk
	05	Realised benefits from IT-enabled investments and services portfolio
Customer	06	Transparency of IT costs, benefits and risk
	07	Delivery of IT services in line with business requirements
	08	Adequate use of applications, information and technology solutions
	09	IT agility
	10	Security of information, processing infrastructure and applications
Internal	11	Optimisation of IT assets, resources and capabilities
	12	Enablement and support of business processes by integrating applications and technology into business processes
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards
	14	Availability of reliable and useful information for decision making
	15	IT compliance with internal policies
Learning and Growth	16	Competent and motivated business and IT personnel
	17	Knowledge, expertise and initiatives for business innovation

© 2013 ISACA. All Rights Reserved.

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting
and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

APO01 Manage the IT Management Framework

APO02 Manage Strategy

APO03 Manage Enterprise Architecture

APO04 Manage Innovation

APO05 Manage Portfolio

APO06 Manage Budget and Costs

APO07 Manage Human Resources

APO08 Manage Relationships

APO09 Manage Service Agreements

APO10 Manage Suppliers

APO11 Manage Quality

APO12 Manage Risk

APO13 Manage Security

Monitor, Evaluate and Assess

MEA01 Monitor,
Evaluate and Assess
Performance and
Conformance

MEA02 Monitor,
Evaluate and Assess
the System of
Internal
Control

MEA03 Monitor,
Evaluate and Assess
Compliance With
External
Requirements

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Change Acceptance
and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI010 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process
Controls

Processes for Management of Enterprise IT

Enterprise Goal Mapping

Enterprise Goal Mapping:
1. Stakeholder value of business investments

Benefits Realisation	Primary
Risk Optimisation	
Resource Optimisation	Secondary

Delegate Activity 1 (45 mins)

Process Name

Area:

Domain:

Process Description

Process Purpose Statement



Process Purpose Reality Check

Compare – Where do we do this? How do we do this?

Contrast – What do we do that isn't covered? What is covered that we don't do?


Challenge – What can we learn from this? What and how can we do this better?

Ask yourself "Have we got the right people involved?" (RACI) and "Are we optimising our resources?" (Enablers)

Summarise your thoughts on the back page "+" for strengths, "-" for room for improvement and "?" for need to re-visit

1. EVALUATE, DIRECT AND MONITOR (EDM)	Compare – Contrast - Challenge
EDM01 Ensure Governance Framework Setting and Maintenance Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.	
EDM02 Ensure Benefits Delivery Secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.	
EDM03 Ensure Risk Optimisation Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.	
EDM04 Ensure Resource Optimisation Ensure that the resource needs of the enterprise are met in the optimal manner IT costs are optimised, and there is an increased likelihood of benefit realization and readiness for future change.	
EDM05 Ensure Stakeholder Transparency Make sure that the communication to stakeholders is effective and timely and the basis for reporting is established to increase performance, identify areas for improvement, and confirm that IT-related objectives and strategies are in line with the enterprise's	

Process Name		Area:	
		Domain:	
Process Description			
Process Purpose Statement			
The process supports the achievement of a set of primary IT-related goals:			
IT-related Goal		Related Metrics	
Process Goals and Metrics			
Process Goal		Related Metrics	
RACI Chart:			
Management Practices	Inputs		Outputs
	From	Description	From
Activities			
Related Guidance			
Related Standard	Detailed Reference		

Process Name			Process Name:DSS04 Manage Continuity	
Process Description			Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.	
Process Purpose Statement				
The process supports the ...				
IT-related Goal				
			Process Purpose Statement Continue critical business operations and maintain availability of information at a level acceptable to the enterprise in the event of a significant disruption.	
Process Goals and Metrics				
Process Goal				
			Management Practices DSS04.01 Define the business continuity policy, objectives and scope. DSS04.02 Maintain a continuity strategy. DSS04.03 Develop and implement a business continuity response. DSS04.04 Exercise, test and review the BCP. DSS04.05 Review, maintain and improve the continuity plan. DSS04.06 Conduct continuity plan training. DSS04.07 Manage backup arrangements. DSS04.08 Conduct post-resumption review.	
RACI Chart:				
Management Practices	Inputs	Outputs		
Activities				
				
Related Guidance				
Related Standard & Reference				

COBIT 5 Outputs		
Outputs to all Processes		
From Key Practices	Output Description	Destination
APO13.02	Information security risk treatment plan	EDM; All APO; All BAI; All DSS; All MEA
Outputs to all Governance Processes		
From Key Practices	Output Description	Destination
EDM01.01	Enterprise governance guiding principles	All EDM
EDM01.01	Decision-making model	All EDM
EDM01.01	Authority levels	All EDM
EDM01.02	Enterprise governance communications	All EDM
EDM01.03	Feedback on governance effectiveness and performance	All EDM
Outputs to all Management Processes		
From Key Practices	Output Description	Destination
APO01.01	Communication ground rules	All APO; All BAI; All DSS; All MEA
APO01.03	IT-related policies	All APO; All BAI; All DSS; All MEA
APO01.04	Communications on IT objectives	All APO; All BAI; All DSS; All MEA
APO01.07	Process improvement opportunities	All APO; All BAI; All DSS; All MEA
APO02.06	Communications package	All APO; All BAI; All DSS; All MEA

© 2013 ISACA. All Rights Reserved.

