

Strategic IT Assurance

Develop an Strategic IT Assurance Plan

Berthing, Hans Henrik

Publication date:
2012

Document Version
Early version, also known as pre-print

[Link to publication from Aalborg University](#)

Citation for published version (APA):

Berthing, H. H. (2012). *Strategic IT Assurance: Develop an Strategic IT Assurance Plan*. Abstract from Euro CACS/ISRM 2012, München, Germany.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy

If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Strategic IT audit

Develop an IT Strategic
IT Assurance Plan



Speaker Biography

Hans Henrik Berthing is Partner at Verifica and Senior Advisor & Associated Professor at Aalborg University. He is specialized in IT Assurance and IT Governance, including risk and control reviews. He is a member of the IT Advisory board for the Danish CPA Association (FSR-Danske Revisorer).

Berthing have helped develop a national & international audit and controls guidelines including Good IT Governance (God IT Skik). He has for the last four years been a CISA instructor. He serves as a speaker and instructor at both the local and international levels, on topics relating to Audit, IT Assurance, IT Governance and risk management. During the past 16 years Berthing has been involved in numerous IT General controls reviews and Third Party Audit Reporting (ISAE 3402) for different clients in size and industry.

- Develop an IT strategic assurance plan
- Use Cobit 4.1 as framework for the IT Assurance plan
- Involve CxO and Board of Directors in IT Governance
- Integrate IT Audit with Financial Audit
- Risk based IT audit in practice
- How can technology facilitate IT audit goals for risk identification and measurement
- Audit Programs based on IT Assurance Framework

Objective

- This course will give the participant a detailed IT Assurance plan and Strategic.
- It will ensure that Business Goals, Objectives and Risks are considered as part of the IT Assurance work.
- Requirement from International Standards of Audit will be highlighted and participants will be able to communicate the IT Audit work to the External Auditor.
- The participant will be able to use tools as part of the planning process and communication with executive management and the Risk and Compliance function.

Hans Henrik Berthing

- 44 year, married with Louise and dad for Dagmar and Johannes
- CPA, CRISC, CGEIT, CISA and CIA
- ISO 9000 Lead Auditor
- IT Audit Director and professional responsible
- 7 Years Financial Audit and 16 Years IT Assurance
- Former President & Vice President ISACA, Denmark Chapter
- Instructor, facilitator and speaker
- Articles and editor of ISACA newsletter
- Senior Advisor & Associated professor Aalborg University

Argumentation

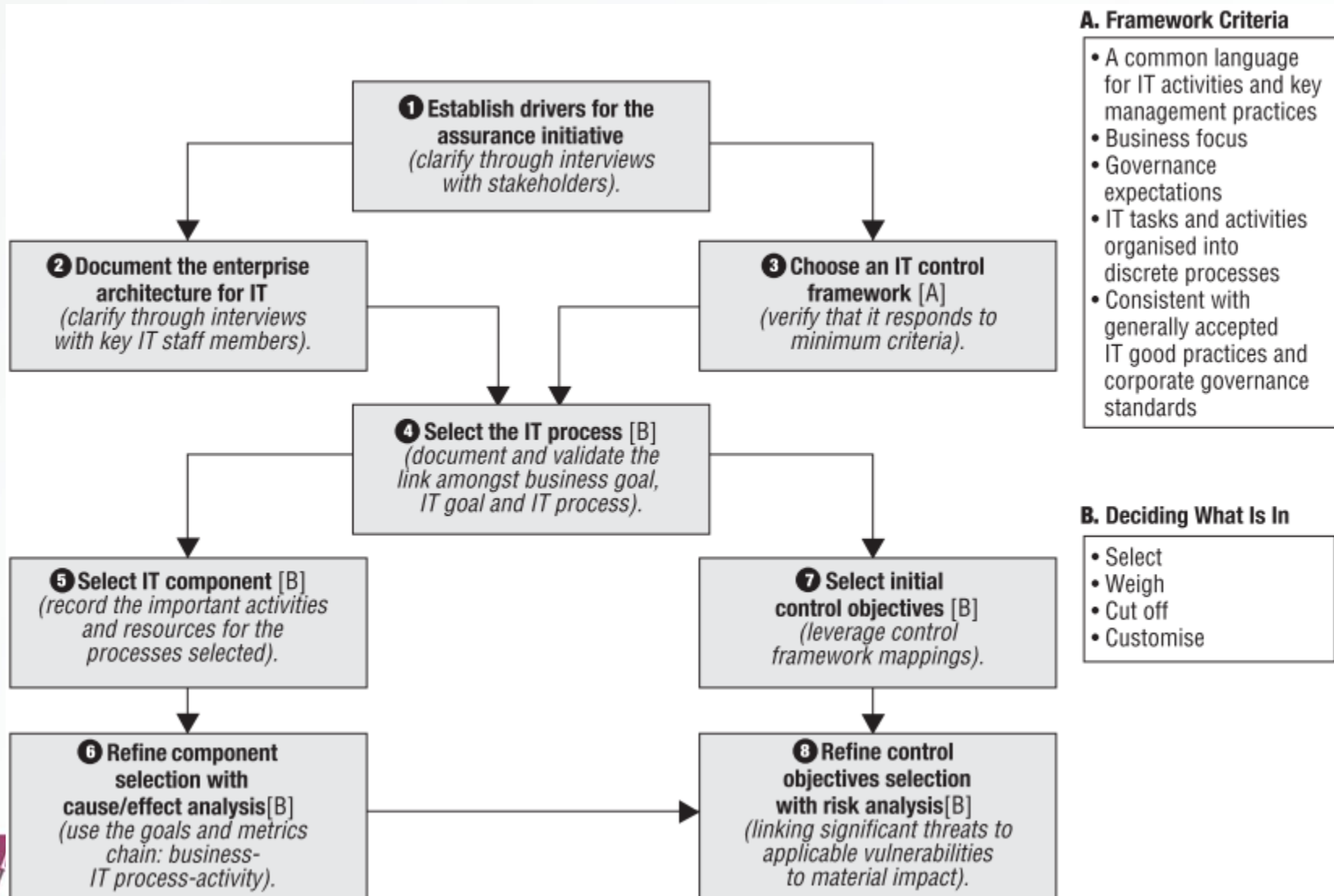
- A huge number of various systems interacting
- Operations, maintenance and change management are difficult
- Systems runs critical business processes
- Realisation of business benefits through SSC
- Data flows are not integrated properly
- Data are not adequately available
- Inadequate Business development and standardisation due to IT investment and infrastructure

Strategic IT audit

Develop an IT Strategic
IT Assurance Plan



IT Scoping Road Map



#ISACAEU

IT Audit Plan

Understand the Business

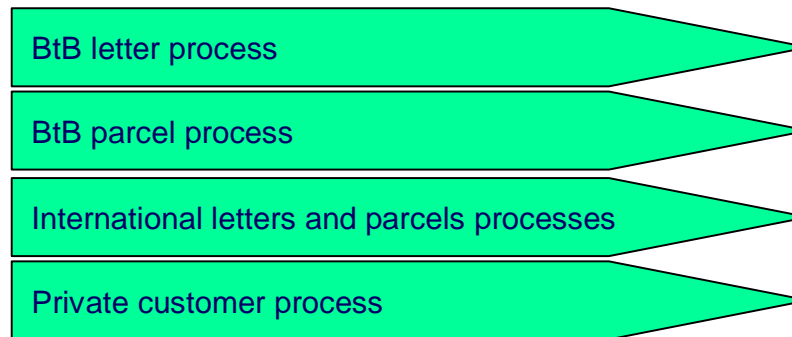
- Identify the Organizations strategies and Business Objectives
- Recognize the risk profile for the Organization
- Assess how the organization structures its business operations
- Comprehend the IT Service support model

Business processes

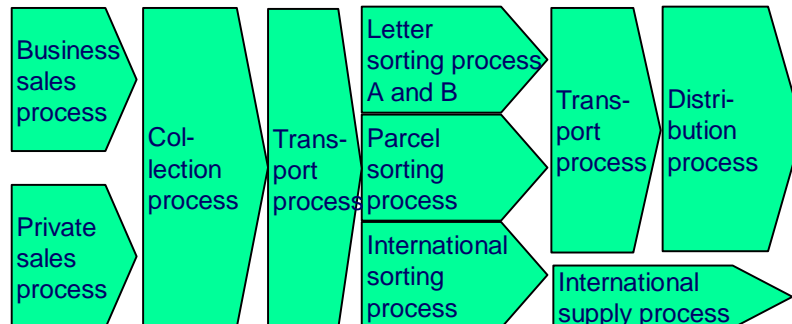
Strategic processes



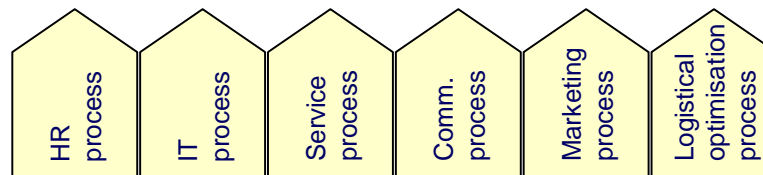
Core processes



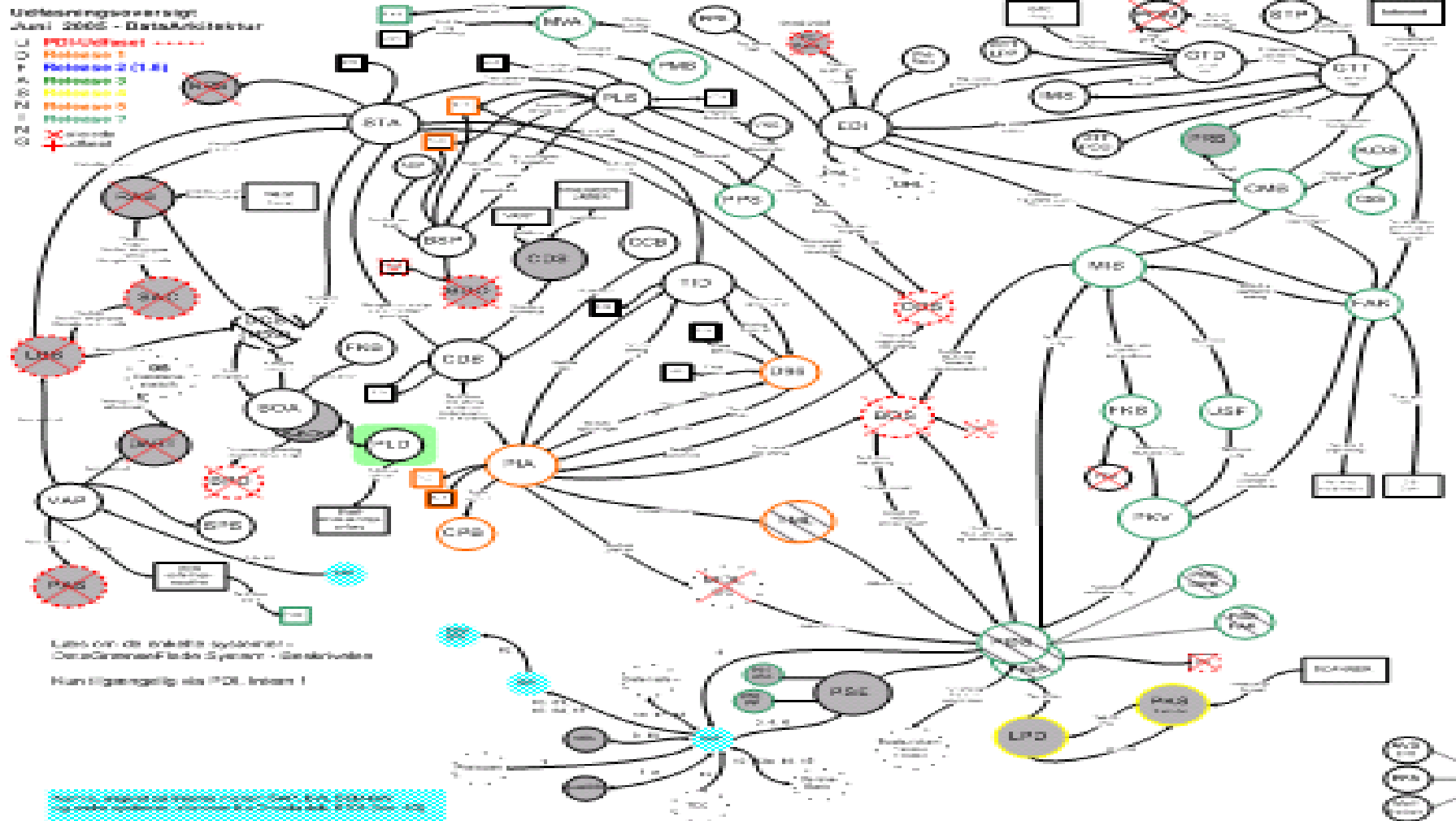
Operational processes



Support processes



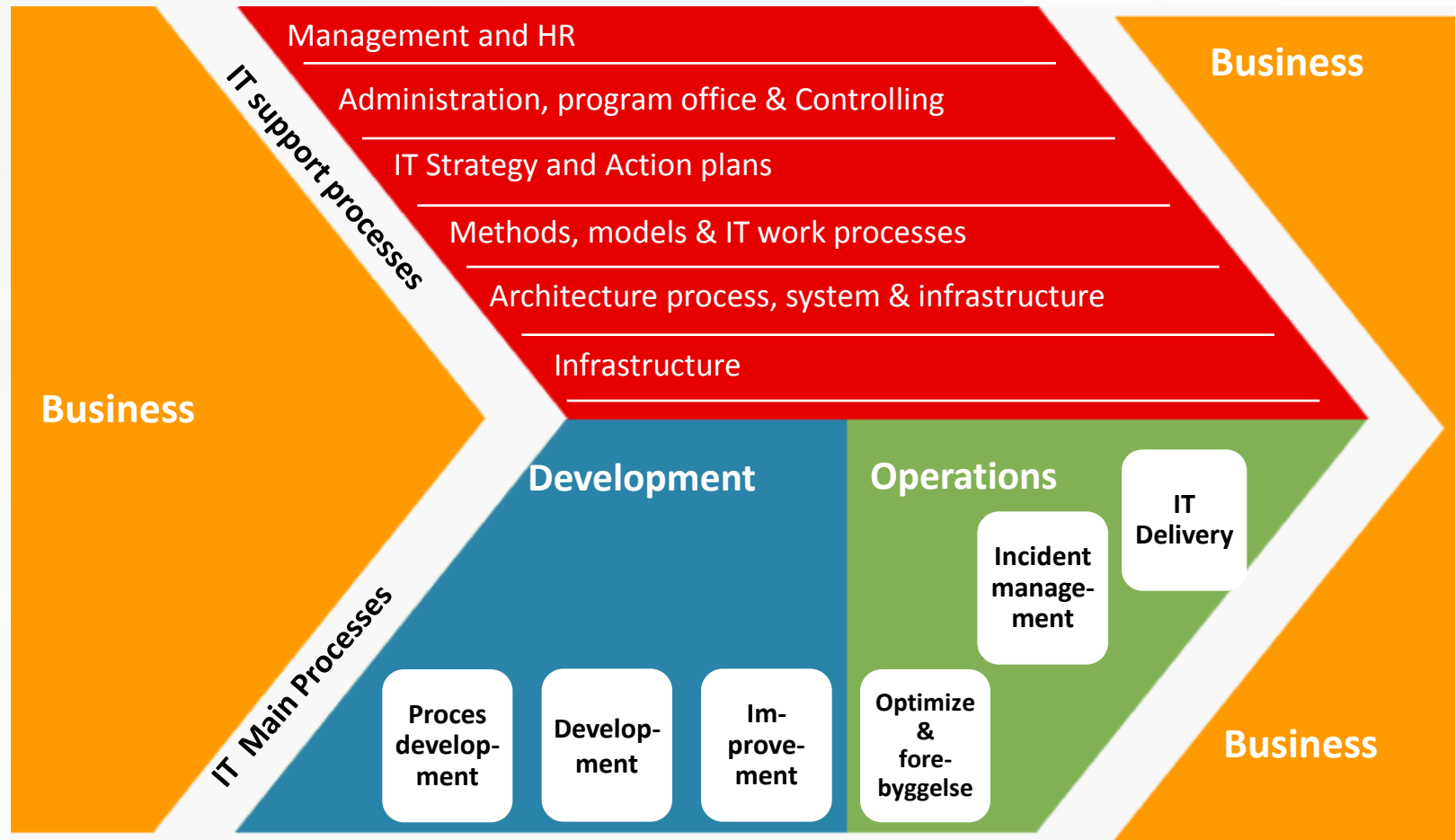
Systemlandscape



IT risk for Business

- System failure or breakdowns
- Error in Dataflow or Data
- Access to systems and data
- Complex applications
- Legacy IT infrastructure and applications

IT processes



IT Assurance Road Map

PLANNING

- Establish the IT assurance universe.
- Select an IT control framework.
- Perform risk-based IT assurance planning.
- Perform high-level assessments.
- Scope and define the high-level objectives for the initiative.

IT ASSURANCE PLANS

SCOPING

Business goals

↳ IT goals

↳ Key IT processes and key IT resources

↳ Key control objectives

↳ Customised key control objectives

DETAILED SCOPE AND OBJECTIVES

EXECUTING

Refine the understanding of the IT assurance subject.

Refine scope of key control objectives for the IT assurance subject.

Test the effectiveness of the control design of the key control objectives.

Alternatively/ additionally test the outcome of the key control objectives.

Document the impact of control weaknesses.

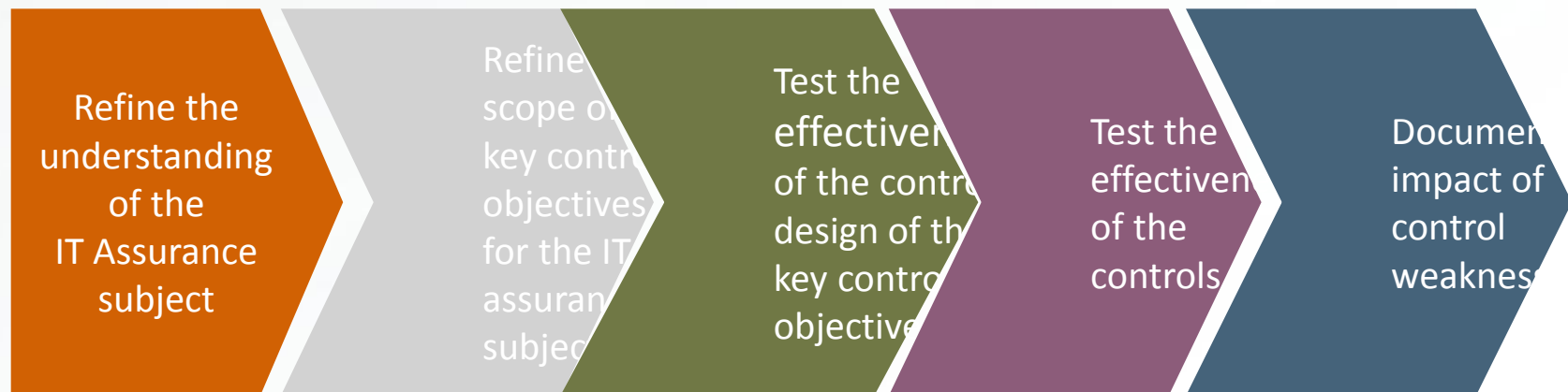
Develop and communicate overall conclusion and recommendations.

ASSURANCE CONCLUSION

Overview of three year plan

Plan & Organise:	Maturity	Materiality	20x1	20x2	20x3
PO1 Define a Strategic IT plan	2-3	M	R	R	F
PO2 Define the information architecture	2-3	M	R	R	F
PO3 Determine technological direction	2	M	F	R	F
PO4 Define the IT processes, organisation and relationships	3	M	R	F	F
PO5 Manage the IT investment	3	L	F	F	F
PO6 Communicate management aims and direction	2	M	F	F	F
PO7 Manage human resources	3-4	M	F	F	F
PO8 Manage quality	2-3	M	F	R	F
PO9 Assess and manage IT risks	2-3	H	R	F	F
PO10 Manage projects	3	H	R	F	F

IT Assurance process

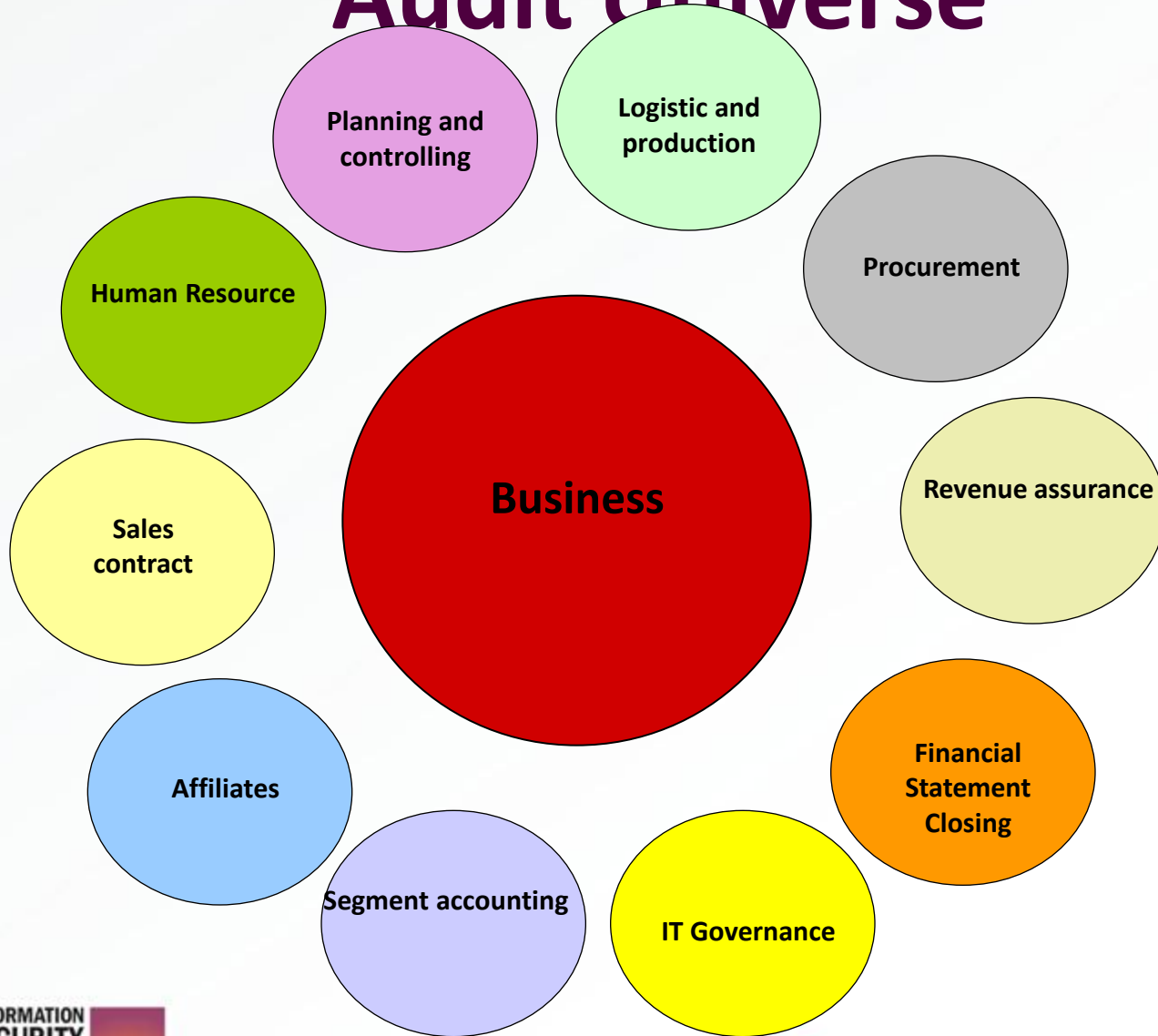


IT Audit Plan

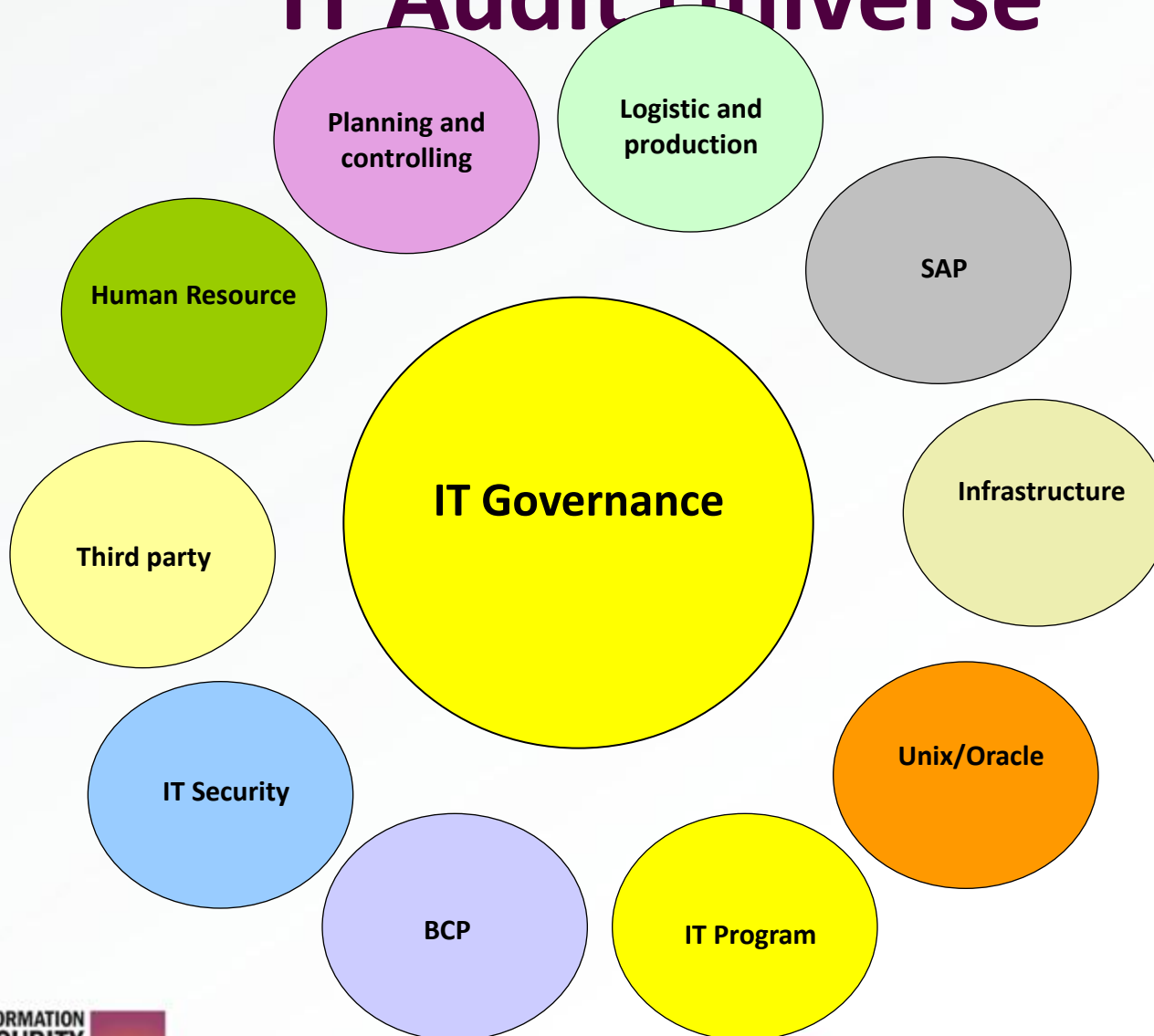
Define the IT Assurance Universe

- Analyze the business fundamentals
- Isolate significant applications that sustain the business operations
- Distinguish critical infrastructure for the significant applications
- Appreciate the role of the supporting technologies
- Categorize major projects and initiatives

Audit Universe



IT Audit Universe



IT Audit Plan

Perform Risk Assessment

- Evaluate business and IT processes to identify Risk
- Assess risks and rank audit subjects using IT risk factors
- Assess risks and rank audit subjects using Business risk factors

Risk assessment of IT Processes

No	What can go wrong/inherent risk	IR	Key control that remedy risk (example)	Control-type	Control-type	Frequency	CR	Comb IR x CR	IT control objectives							Audit assignment
									Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	
		H M L	Who does what and on the basis of what input?	DE PR	IM MP	D, W, M, Q, Y, AH	H M L	H M L								
1	Systems Development & Maintenance Mega Process															
1.1	Implementation & Change Process - Applies to implementation of new systems, major changes to existing systems, and patches and upgrades to systems software.															
1.	Systems Development Life Cycle procedures have not been formally documented and communicated.	M	Systems Development Life Cycle procedures are published and communicated to provide policies and procedures governing the installation of new and modified software and hardware into production. (AI 7)	PR	M	AH	M	M	X							05:359 07:1780
2	Project Management procedures have not been formally documented and communicated.	M	Project Management procedures are published and communicated to provide policies, procedures, and standards governing the management of new or modified systems installations. These procedures address, but are not limited to the following. (PO 10) <ul style="list-style-type: none"> Project initiation (PO 10.1) Management review and approval requirements (PO 10.2-3) Scope development and control (PO 10.2) Team building and management (PO 10.8) Budget management (PO 10.6-7) Timeline development and control (PO 10.7)x 	PR	M	AH	M	M	X							05:359 06:444 07:1768, 1780

IT Audit Plan

Form IT Audit Plan

- Choose Audit subjects and group to audit actions
- Establish audit cycle and frequency
- Attach appropriate actions based on management requests or opportunities for advisory
- Confirm the plan with management

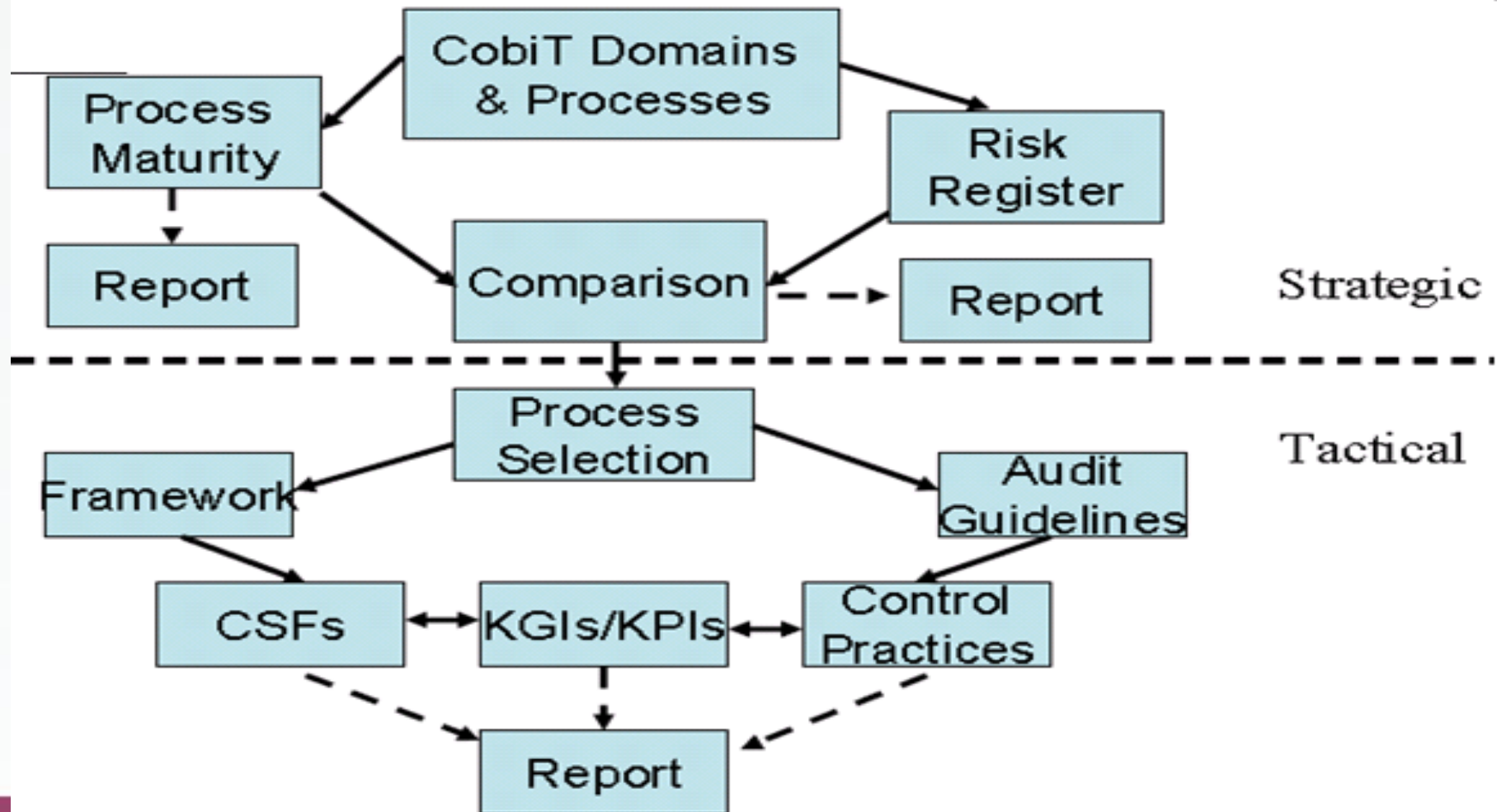
IT audit plan 201x

Assignment	Priority	May	June	July	August	September	Q4	Value
ACR		X	X				X	
Pre implementation review								
Evaluation of network strategy						X		
Compliance with ITIL			X					
Portfolio management								
Review of interfaces					X		X	
Baseline for Unix/Oracle							X	
System Development							X	
Active Directory						X		
QA Reference Group and Business Blueprint Review							X	
Advisory for projects							X	
Outplacement of legacy systems					X	X		
Follow up SAP							X	
Review SAP basis							X	
IT procurement		X	X				X	
Data center security			X					
Review of user administration		X						
Method for Risk Assessment			X					
DRP		X						
Backup and recovery		X	X					
Procedures and guidelines IT security								
Operation for SAP		X	X					
Review of IT strategy								
SAP Portal							X	

Management Awareness

Risk		<div>Importance = How important for the organisation on a scale from 1 (not at all) to 5 (very) Performance = How well it is done from 1 (very well) to 5 (do not know or badly) Formality = Is there a contract, an SLA or a clearly documented procedure (Y, N or ?) Audited? = Y, N or ? Accountable = Name or 'do not know'</div>	Who Does It?						Who Is Accountable?
Importance	Performance		IT	Other	Outside	Do Not Know	Audited?	Formality	
COBIT Processes									
		PO1 Define a strategic IT plan.							
		PO10 Manage projects.							
		A16 Manage changes.							
		DS2 Manage third-party services.							
		DS5 Ensure systems security.							
		ME1 Monitor and evaluate IT performance.							

Tactical IT Assurance Strategy

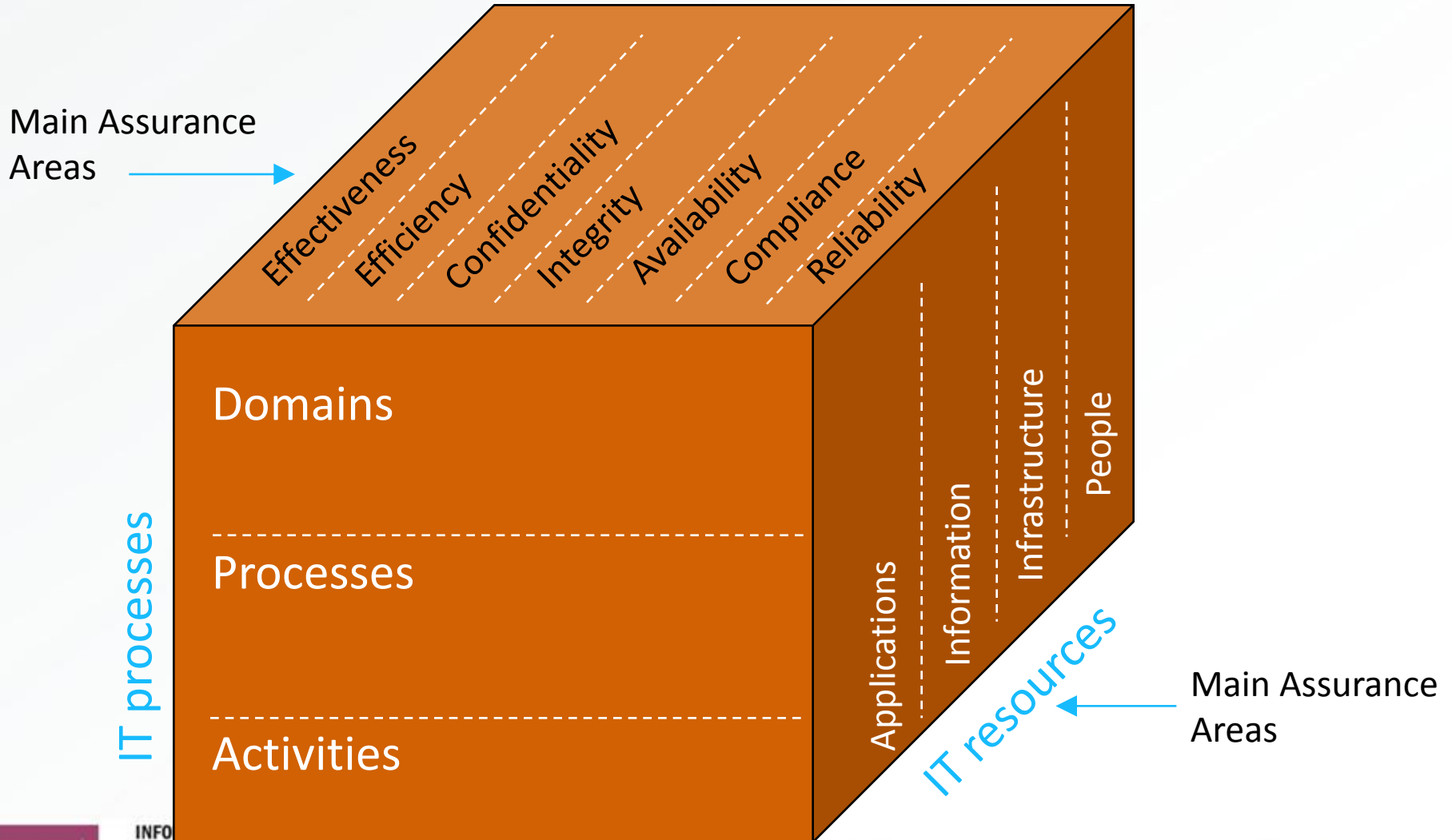


Cobit 4.1

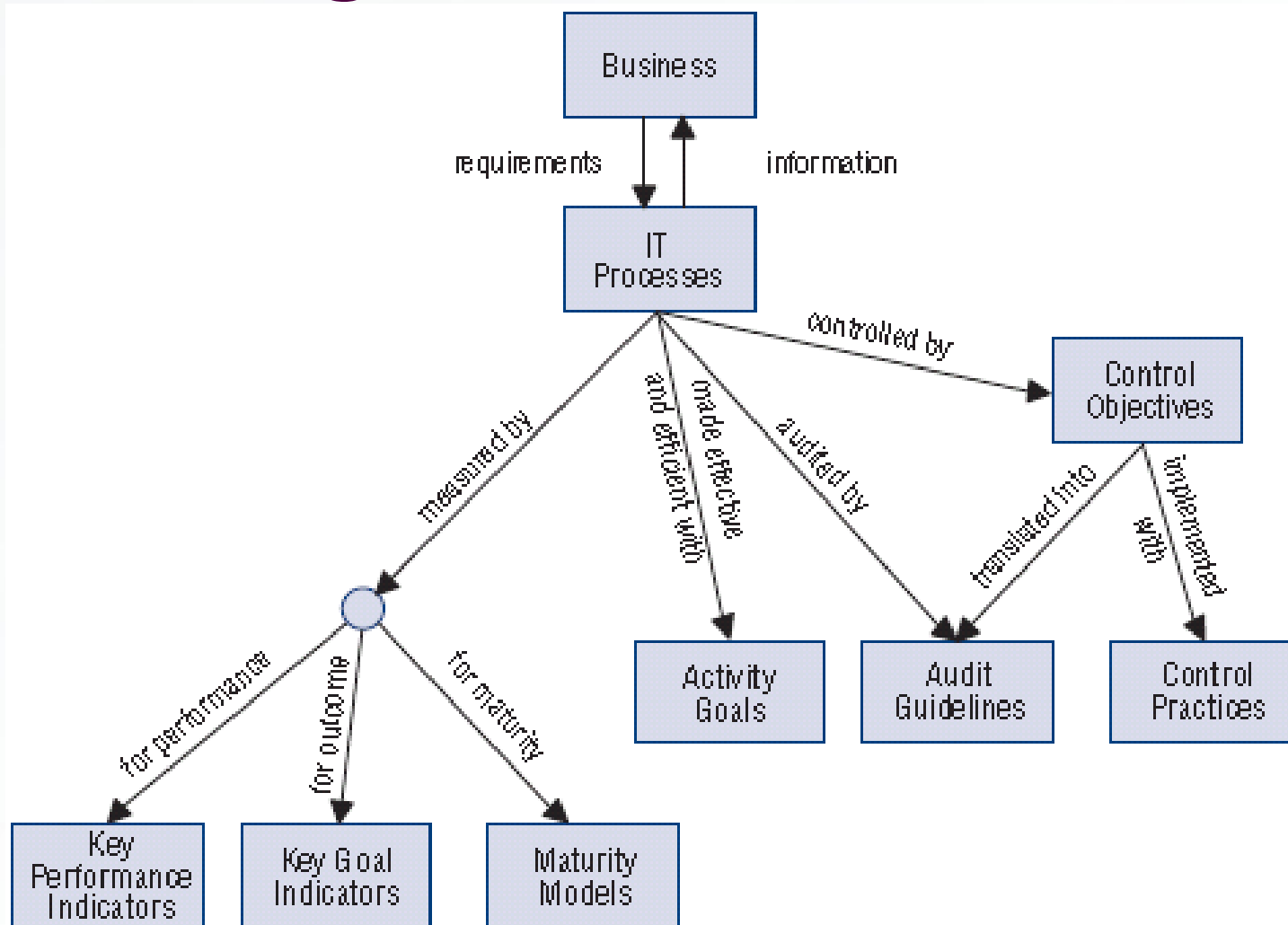
Framework for the IT Assurance Plan



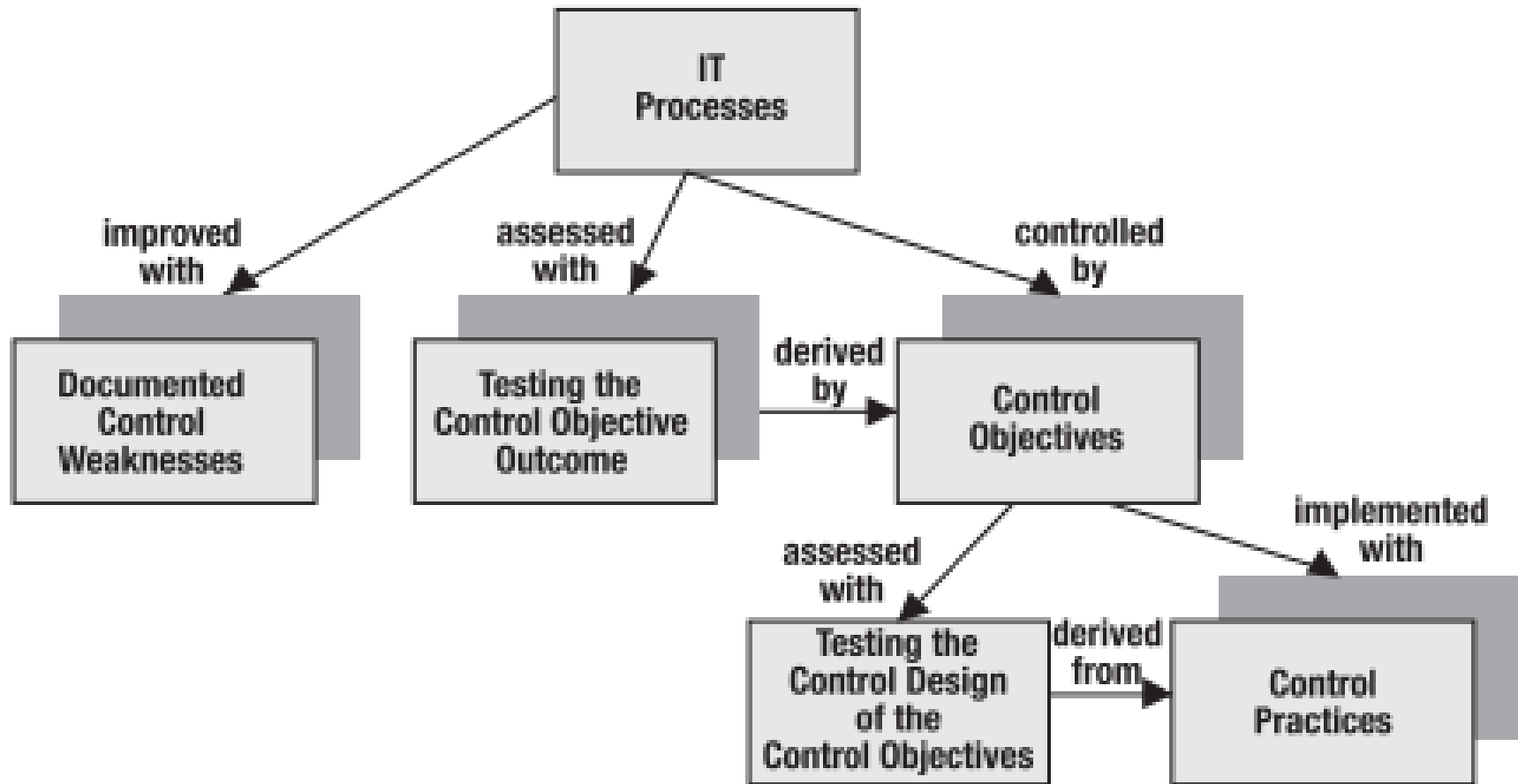
IT Assurance



Linking the IT Assurance



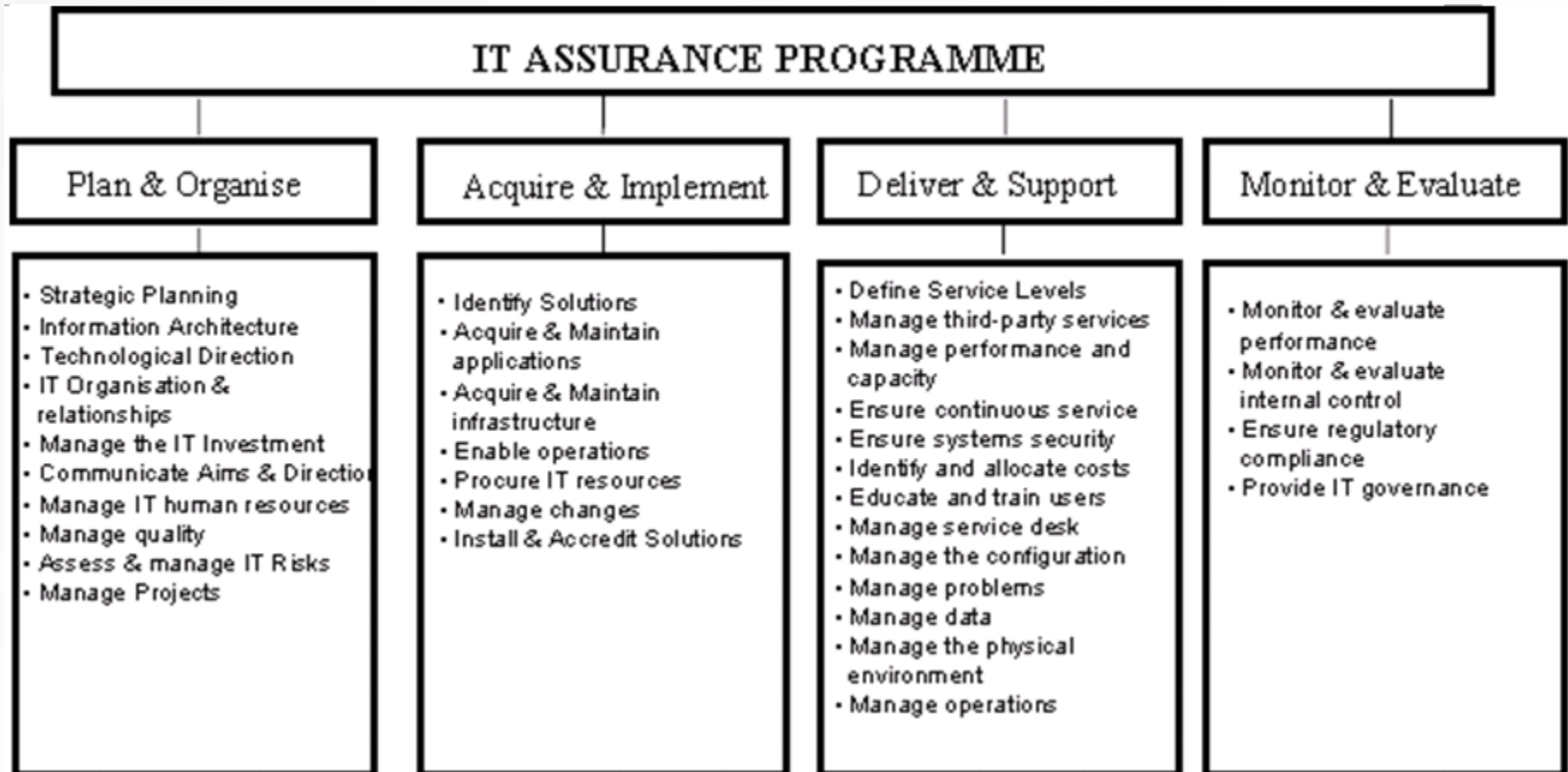
IT Assurance Advice



Generic (■) and Specific (□) Advice in the Assurance Guide

IT Governance

4 domains -> 34 processes -> 210 control objectives



Maturity Model - Concept

Method of evaluating the organisation,

Rated from a maturity level of non-existent (0) to optimised (5).

Designed as profiles of IT processes

Possible current and target levels.

Facilitated assessments

Motivate improvement.

The advantage of a maturity model approach is that it is relatively easy for management to place itself on the scale and appreciate what is involved if improved performance is needed.

Maturity Model - general

General

0 Non-existent

1 Initial.

2 Repeatable.

3 Defined.

4 Managed.

5 Optimised

Process

0 Non-existent

1 Initial/Ad Hoc

**2 Repeatable but
Intuitive**

3. Defined Process

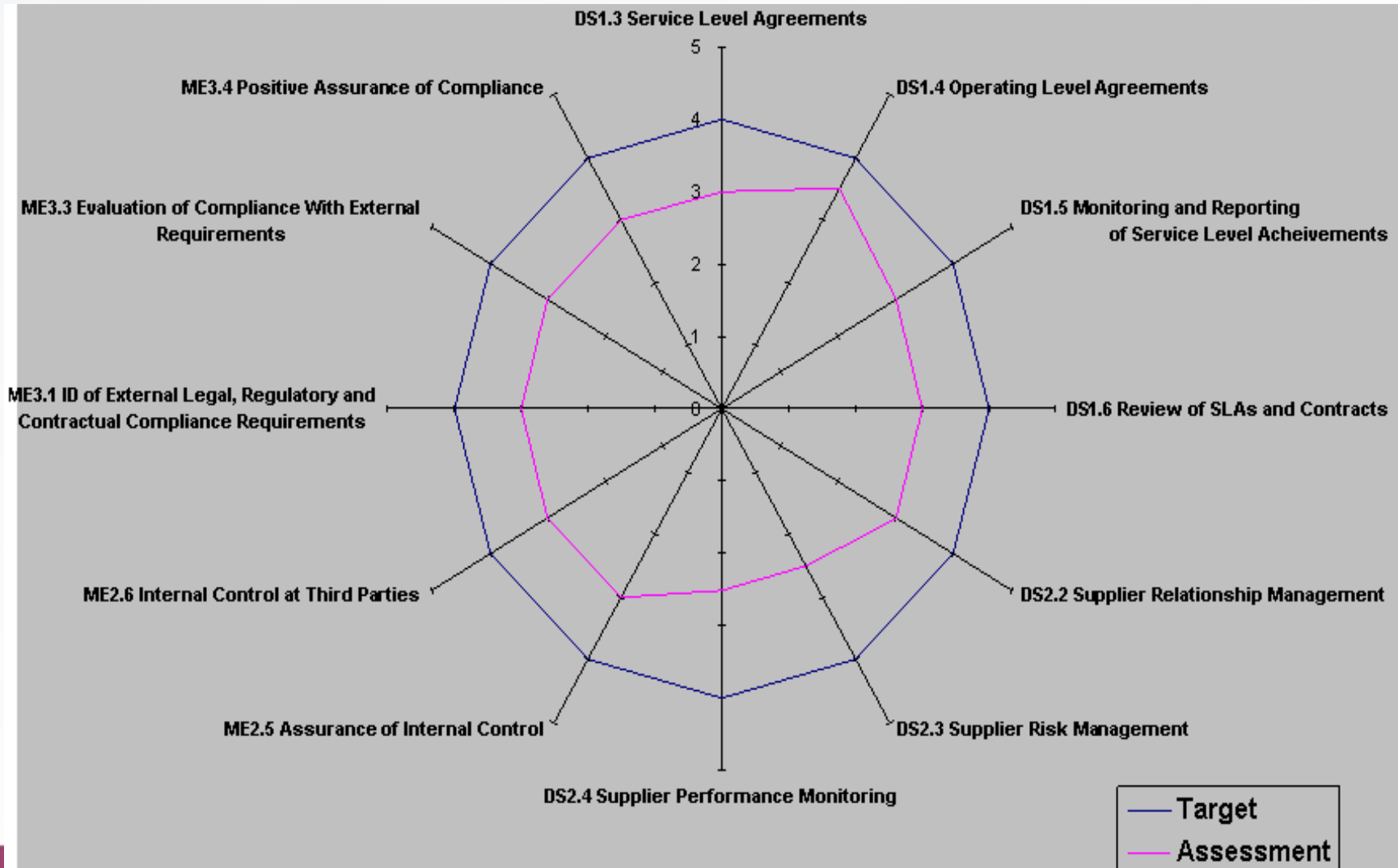
**4 Managed and
Measurable**

5 Optimised

Self assessment of COBIT Processes

- Maturity of the process
- Risk
- Materiality
- Controls
- Goals
- Awareness and Communication
- Policies, Standards and Procedures
- Tools and Automation
- Skills and Expertise
- Responsibility and Accountability
- Goal Setting and Measurement

Maturity Assessment



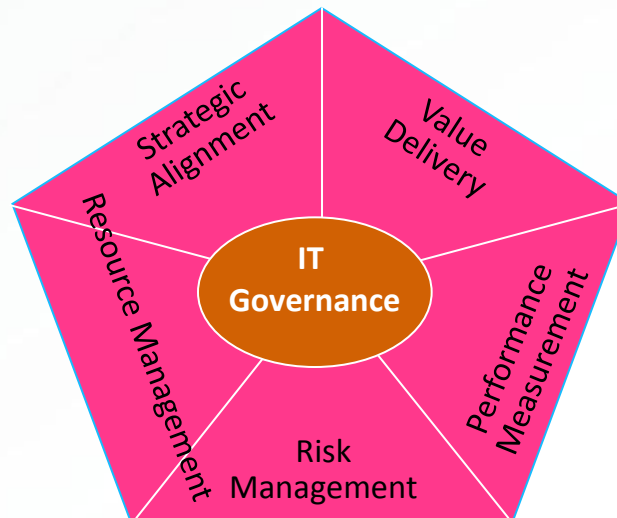
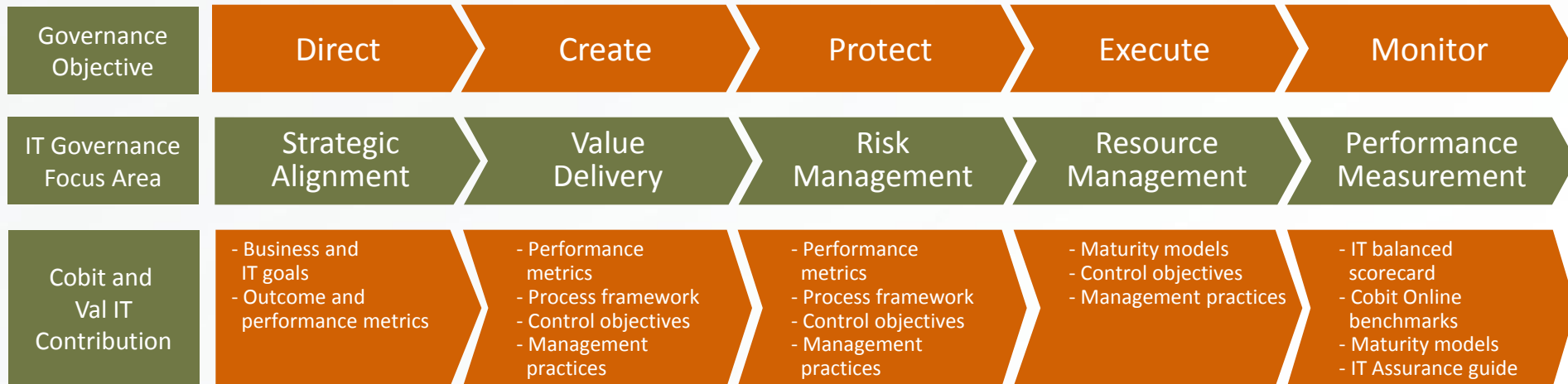
Involve Mangement

CxO and Board of Directors
IT Governance

IT challenges

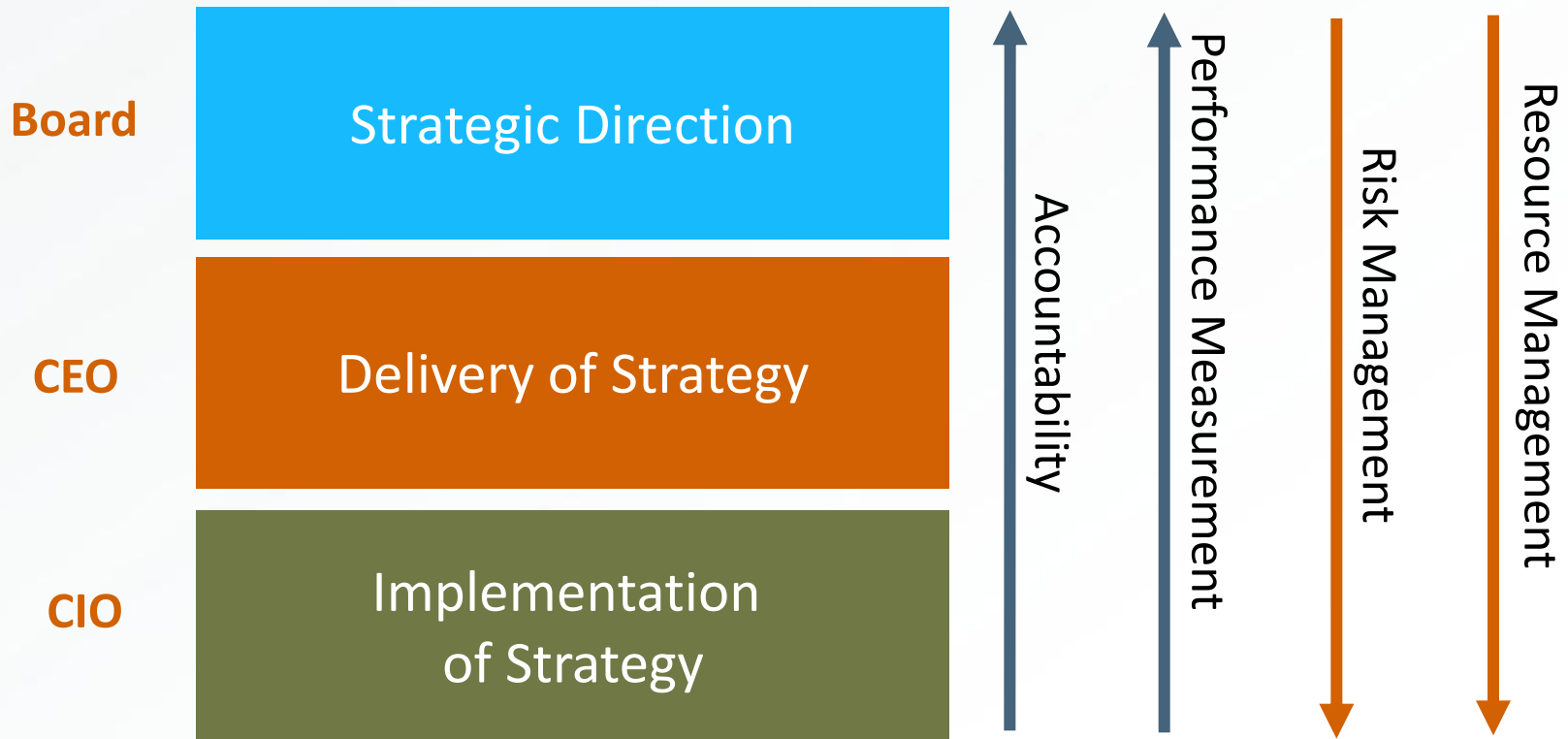
- Low involvement of management
- 8 EU Directive & SOX
- Formal IT strategy
- Preparation of Business Impact Analysis
- Guidelines for IT Security
- Description of system development life cycle
- Preparation of IT operation manuals
- Lack of or inadequate DRP or recovery
- Inadequate security
- Lack of system documentation
- Lack of procedures for access to systems and data
- Overruns of project budgets
- Increasing of IT TCO

IT Governance life cycle



Roles and responsibility

Major/Main Responsibilities



IT Management

- Follow up
- Plan & Organise:
 - PO1 Define a Strategic IT plan
 - PO2 Define the information architecture
 - PO3 Determine technological direction
 - PO8 Manage quality
- Acquire & Implement
 - AI1 Identify automated solutions
 - AI2 Acquire and maintain application software
 - AI3 Acquire and maintain technology infrastructure
 - AI4 Enable operation and use
 - AI5 Procure IT resources
- Deliver & Support
 - DS1 Define and manage service levels
 - DS2 Manage third-party services
 - DS8 Manage the service desk and incidents
 - DS12 Manage the physical environment
- Monitor and evaluate
 - ME1 Monitor & evaluate performance
 - ME2 Monitor & evaluate internal control
 - ME3 Ensure regulatory compliance
 - ME4 Provide IT governance

IT Governance

- Strategy
- VAL IT
- COSO / ERM
- IT Risk
- COBIT
- Business oriented



Failure in implementing new complex IT-systems

Implementation of SAP increases the risk for material errors in financial report:

- Data conversion errors
- Systems errors
- Inadequate controls
- Inadequate training of users

Early warning challenges in SAP:

- Fixed assets
- Procurement
- SOD
- IT GC

Increase business risks and financial risks

- SAP CRM
- Sales contracts
- Orders and invoicing
- SAP Portal solution
- SAP HR
- Time planning and salary

Audit work related to SAP and the program


- User rights and SOD
- Compliance
- Data conversion and related controls
- Training plans
- System documentation and users manual
- SAP-Basis and ACR
- QA meeting and QA reference group
- Review of Business Blueprint

First year:

- Review of implemented modules
- ITGC
- Compliance

Second & Third year

- Follow up on first years findings
- Review of new modules
- SAP Transport (Change management)
- QA on HR

–  Follow us @ISACANews
Benefits #ISACAEU

Complex IT-infrastructure

System failure impact service goal. IT infrastructure are business critical for BUS. Unavailability might impact on financial loss.

- Unable to deliver products
 - Delay in Financial Statements
 - Non timely management decision reports
- Increase business risks and financial risks
- Network interruption
 - Virus attack
 - Emails
 - Hardware/OS failure
 - Poor baseline in infrastructure
 - SOD
 - Lack of application controls

Audit work related to IT infrastructure

- General IT controls based on COBIT
- IT Governance
- Procedures and processes
- Follow up on identified failure

IT assurance strategy:

- Risk Assessment
- Cover Domains in COBIT
- Advisory assignments

Integrate IT Audit with Financial Audit



Assignments

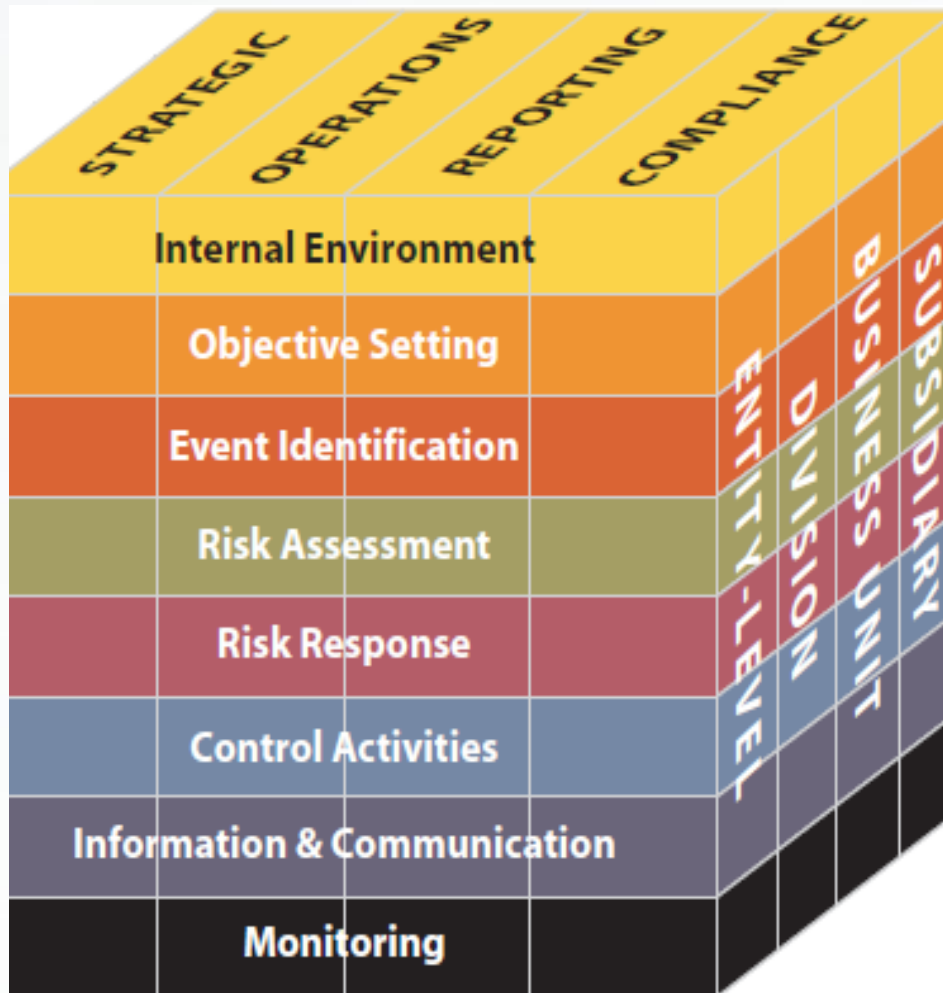
- External Audit Support (ISA 315 og 330)
- Quality Assurance
- Clients seminars, Speaks and education
- Advisory
- External Clients



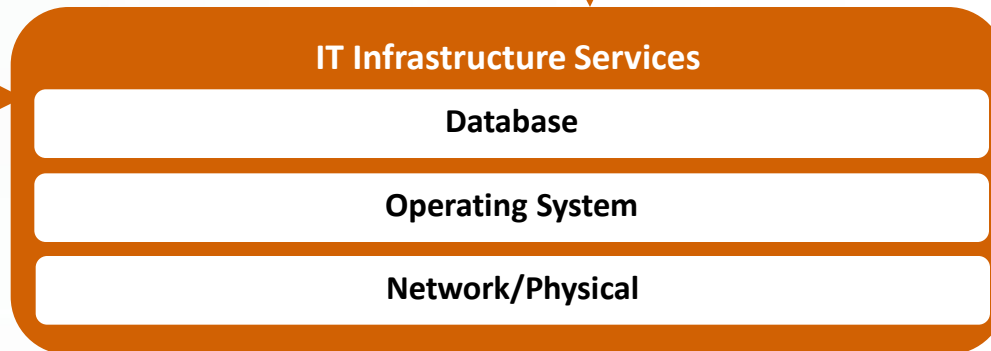
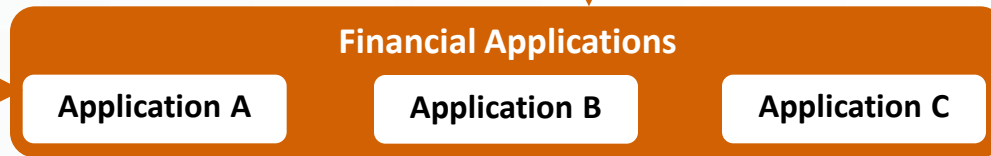
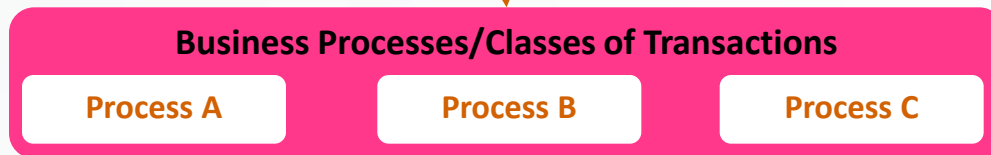
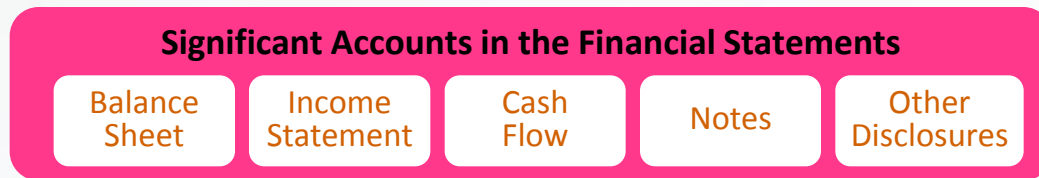
IT Assurance and Assurance

		Assurance Stages (IAASB)						
		Determine the responsible party and intended user of assurance output.	Determine the nature of the subject matter.	Define and agree on evaluation criteria.	Collect evidence.	Assess evidence.	Make judgement.	Report and conclude.
Stages in the Road Map	Planning	✓	✓	✓				
	Scoping			✓				
	Execution	Refine the understanding of the IT assurance subject.	✓	✓				
		Refine the scope of key control objectives.		✓				
		Test the effectiveness of the control design.			✓	✓		
		Test outcomes of key control objectives.			✓	✓		
		Document the impact of control weaknesses.			✓	✓		
		Develop and communicate the overall conclusion and recommendations.					✓	✓

Internal Controls - COSO



Cobit and Financial Audit



IT General Controls

- § Program development
- § Program changes
- § Program operations
- § Access control
- § Control environment

Application Control Objectives/Assertions

- § Accuracy
- § Completeness
- § Authorization
- § Segregation of duties

Strategic IT audit

How can technology facilitate



IT Assurance

- COBIT
 - Planning and organize
 - Aquisition and implementing
 - Delivery and support
 - Monitoring and evaluate
- IT Assurance guide
- Process audit standards

Tools

MDS (Methods for Documentation and standards)

- Risk and control matrix
- Audit programs
- Audit report
- Audit papers

Audit work

- SAP GRC for SOD conflicts
- Script for IT infrastructures
- ACL and SAP Direct link for Data analysis
- Microsoft Office

External and professional Standards and guidelines

- ISACA standards and guidelines
- ISACA Audit programs (Oracle, Unix, SAP, CRM)
- ISACA IT assurance guide
- Cobit and VAL IT
- IIA standards and ISA
- COSO

Internal guidelines and standard

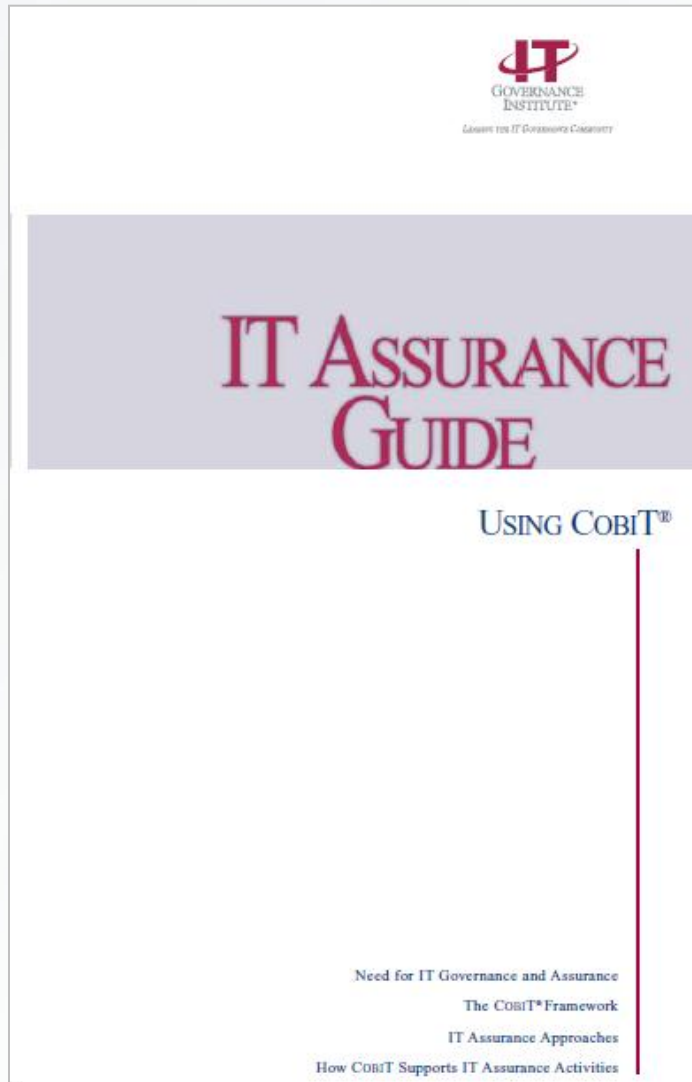
- IT security policy including procedures and guidelines based on ISF
- Procedures in systems development (CMMI level 2)
- Procedures in delivery and support based on ITIL
- ISO20000 and ISO9001
- Compliance Manual

Strategic IT audit

Audit Programs based on IT Assurance Framework



IT Assurance Guide



The objective of **IT Assurance Guide** is to provide guidance on *how to use COBIT to support a variety of IT assurance activities.*

IT Assurance Guide

Detailed guidance for ***assurance and IT professionals*** to use COBIT

Assurance steps and advice are provided for:

- **Generic controls** that apply to all processes (identified within the COBIT framework)
- **Application controls** (identified within the COBIT framework)
- Specific **process controls** (identified within the COBIT framework)

Assurance steps and guidelines are provided to:

- Test the control design of the control objective
- Test the outcome of the control objective (operational effectiveness)
- Document control weaknesses and their impact

IT Assurance Guide



ZIP-komprimeret
mappe



IT Assurance Guide – components

Control Objective

DS1.1 Service Level Management Framework

Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). The framework should include processes for creating service requirements, service definitions, SLAs, OLAs and funding sources. These attributes should be organised in a service catalogue. The framework should define the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers.

Value Drivers

- Clarified IT service responsibilities and IT objectives aligned with business objectives
- Improved communication and understanding between business customers and IT service providers
- Consistency promoted in service levels, service definitions, and service delivery and support

Risk Drivers

- Gaps between expectations and capabilities, leading to disputes
- Customers and providers not understanding their responsibilities
- Inappropriate priority given to different services provided
- Inefficient and costly operational service

Test the Control Design

- Inspect SLA policies and procedures for the alignment of SLA objectives and performance measures with business objectives and IT strategy.
- Enquire whether and confirm that policies exist for the alignment of SLA objectives and performance measures with business objectives and IT strategy.
- Inspect the service catalogue and verify that it incorporates service requirements, service definitions, SLAs, OLAs and funding sources.
- Enquire of staff members accountable for SLA escalation and resolution to determine whether the procedures or methods established reasonable service levels in responding to issues.
- Inspect a sample of relevant changes and verify that changes were implemented in accordance with the change management process.
- Inspect the design of the service improvement programme for standards to measure performance.

Audit instruction

Nr.	Audit step	Audit result	Auditor	Reviewer
2	<i>Service Level Management Framework</i>			
2.1	Enquire whether and confirm that a process exists for developing, reviewing and adjusting the service catalogue or portfolio of services.	Formal service level management process, and supporting processes (continuity management, change management, configuration management, incident and problem management etc.).	NN	NN
2.2	Confirm the existence of a management process to ensure that the service catalogue or portfolio is available, complete and up to date.	See 2.1. Renegotiation should be done yearly. We have noted that not all reviewed SLA have been renegotiated the last two years.	NN Obs	NN
2.3	Inspect the service catalogue or portfolio process to verify that it is reviewed on a regular basis.	Se 2.2	NN Obs	NN
	Conclusion	Based on work performed we evaluated the area as Defined (3). Some elements are Managed and Measurable (4).	NN	NN

Reporting and conclusion

3 Defined when

Responsibilities are well defined, but with discretionary authority. The SLA development process is in place with checkpoints for reassessing service levels and customer satisfaction. Services and service levels are defined, documented and agreed-upon using a standard process. Service level shortfalls are identified, but procedures on how to resolve shortfalls are informal. There is a clear linkage between expected service level achievement and the funding provided. Service levels are agreed to, but they may not address business needs.

4 Managed and Measurable when

Service levels are increasingly defined in the system requirements definition phase and incorporated into the design of the application and operational environments. Customer satisfaction is routinely measured and assessed. Performance measures reflect customer needs, rather than IT goals. The measures for assessing service levels are becoming standardised and reflect industry norms. The criteria for defining service levels are based on business criticality and include availability, reliability, performance, growth capacity, user support, continuity planning and security considerations. Root cause analysis is routinely performed when service levels are not met. The reporting process for monitoring service levels is becoming increasingly automated. Operational and financial risks associated with not meeting agreed-upon service levels are defined and clearly understood. A formal system of measurement is instituted and maintained.

Questions



Collaborate – Contribute – Connect



- <http://www.isaca.org/Knowledge-Center>
- The Knowledge Center is a collection of resources and online communities that connect ISACA members – globally, across industries and by professional focus - under one umbrella. Add or reply to a discussion, post a document or link, connect with other ISACA members, or create a wiki by participating in a community today!