

The Fourth Canadian ISO 17799/ISO 27001 Conference

COBIT for ISO27001 Users Concepts, Myths and Misconceptions

Anton J Aylward, CISSP, CISA



COBIT is not ISO27000

- ◆ What they have in common
 - Based on Experience
 - Continuous Refinement
 - Committee to make 'general'
- ◆ How they differ
 - Audit is not implementation
 - There's more to IT than ISMS
 - There's more to audit than IT!
 - COBIT is more than an ISMS

Quick side-by-side



How they differ

Audit is not implementation

There's more to IT than ISMS

There's more to audit than IT!

COBIT is different from an
ISMS

Quick side-by-side

Goals

Paradigm

Maturity levels

InfoSec Paradigm

Organization Model

Inputs

Outputs

Certifiable



Goals

CobIT	ISO27001
Many. Strategic Alignment, IT Resource Management & Optimizations, Governance, Performance Measurement "Dashboard", Compliance, budgeting, reporting ...Identification of Processes, Value Delivery. Oh, and Risk Management - at many levels.	"Absolute" Security?

"Security" can easily end up as managing by FUD, especially when dealing with absolutes - yes/no.

Granularity makes for better management,



Paradigm

CobIT	ISO27001
IT Process Based	Focus on Security Controls

"Process Based" is aligned with ISO9000 and ITIL
Controls and Process can be audited by testing
Controls don't have a defined output. Processes do.
Processes can be controlled and measured in terms of their I/O
A (malfunctioning) control produces no output to tell what is wrong with it



Maturity Levels

CobIT	ISO27001
Five	None (or just one)

"Process Based" is aligned with ISO9000 and ITIL

ISO27001 is a selective "Do everything or Do Nothing". This has economic implications as well as management implications.

Granularity and maturity levels can show progress, ROI, justify further investment; audit process supplies this management focus

Does ISO27001 need maturity Levels if the audit supplies it?



Infosec Paradigm

CobIT	ISO27001
1. Corporate Values 2. CIA + Effectiveness + Efficiency + Compliance + Reliability/Robustness 3. Errors & Omissions, Accidents, Attacks (not just infosec)	4. ISMS 5. CIA 6. Attacks



Organisational Model

CobIT	ISO27001
All stakeholders. All RACI Entities (Responsible, Accountable, Consulted, Informed) Board, executive, operations, procurement, support, development, audit, security (including GGGD)	Management / non-management

Granularity and specific responsibilities and inputs



Inputs

CobIT	ISO27001
Most CobIT process have inputs from other processes	No



Outputs

CobIT	ISO27001
CobIT metrics (KPIs etc) are based on defined outputs that are measureable and which makes managing the relevant processes possible	No



Certifiable?

CobIT	ISO27001
No	Yes

ISO-17799 -- “Code of Practice”

ISO-27001 -- Standard

CobIT -- Methodology



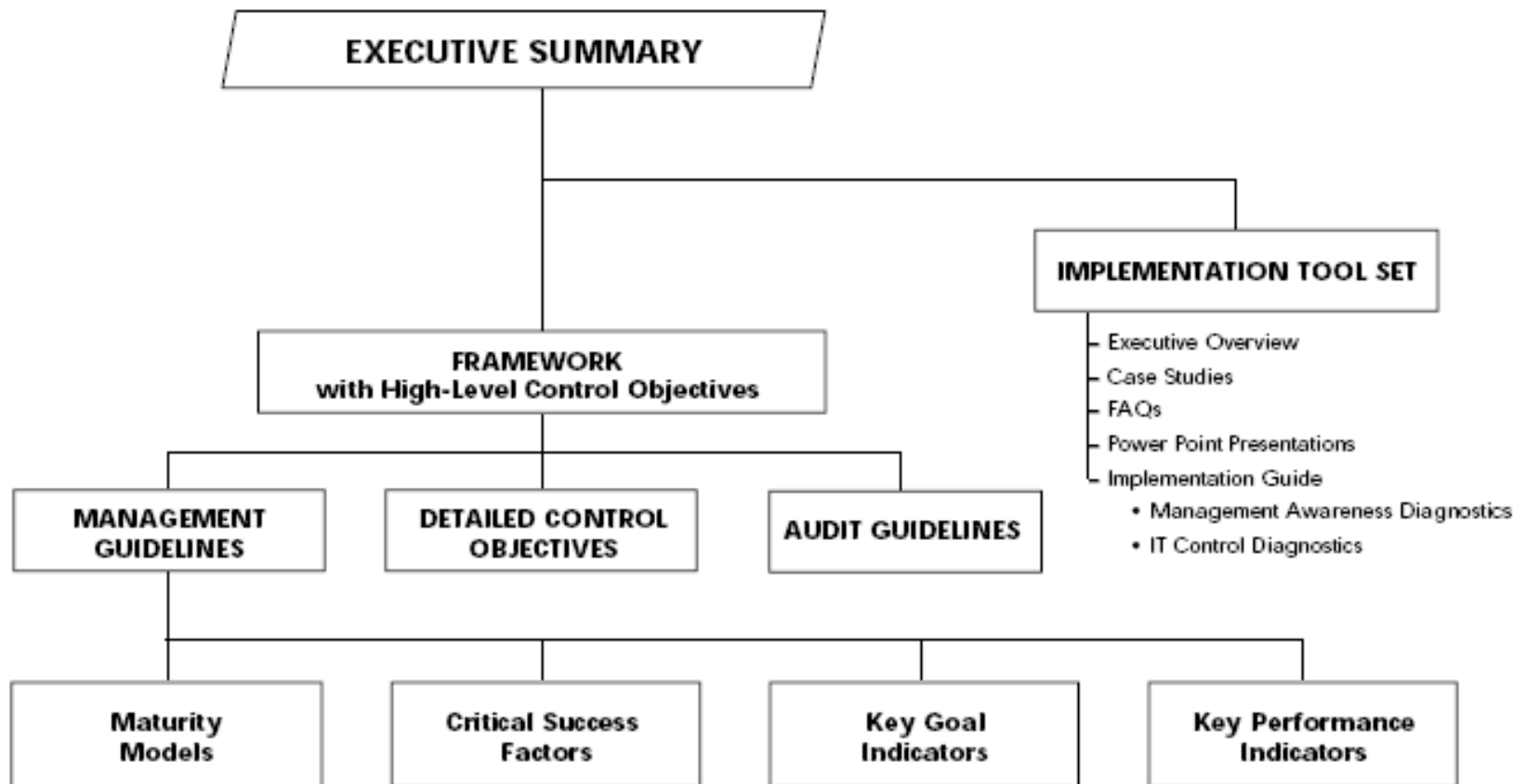
CobIT Documentation

Its Time

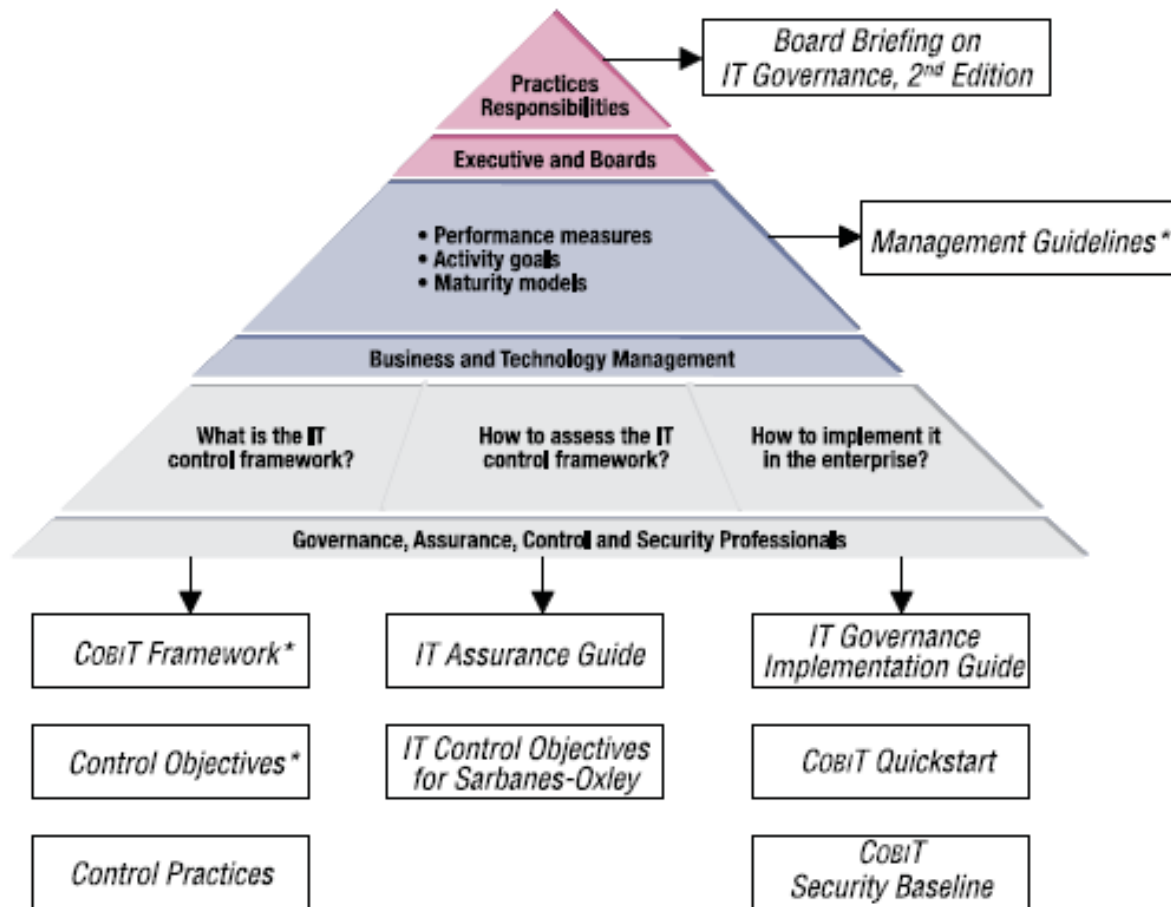


CobIT Documentation

COBIT Family of Products




CobIT Documentation



* Now integrated into COBIT 4.0



What is an Audit?



*Uh Oh!
Audit Time!
Everyone be on their best behaviour*



Types of Audit

- ◆ Financial
- ◆ Compliance
 - ◆ against 'self defined' requirements
 - ◆ against outside requirements
 - ◆ by internal audit
 - ◆ by external auditors
- ◆ Risk
 - ◆ Scope?
 - ◆ Types of Risk
 - ◆ Business
 - ◆ Technological



Financial ?

Remember: These are all different!

Financial Risk

Security Risk

Business Risk

InfoSec Risk



Value of COBIT

On the face of it, only TWO of the 34 top level COBIT control objectives map to security.

PO9 - Asses and manage IT Risks

DS5 - Ensure Systems Security

In reality:

- a) these take input from and supply output to many other processes
- b) there are many of the 318 second-level control objectives that supply input to the security processes



Value of COBIT. Continue.

See also

"Aligning COBIT, ITIL and ISO 17799 for Business Benefit"

<http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22490>

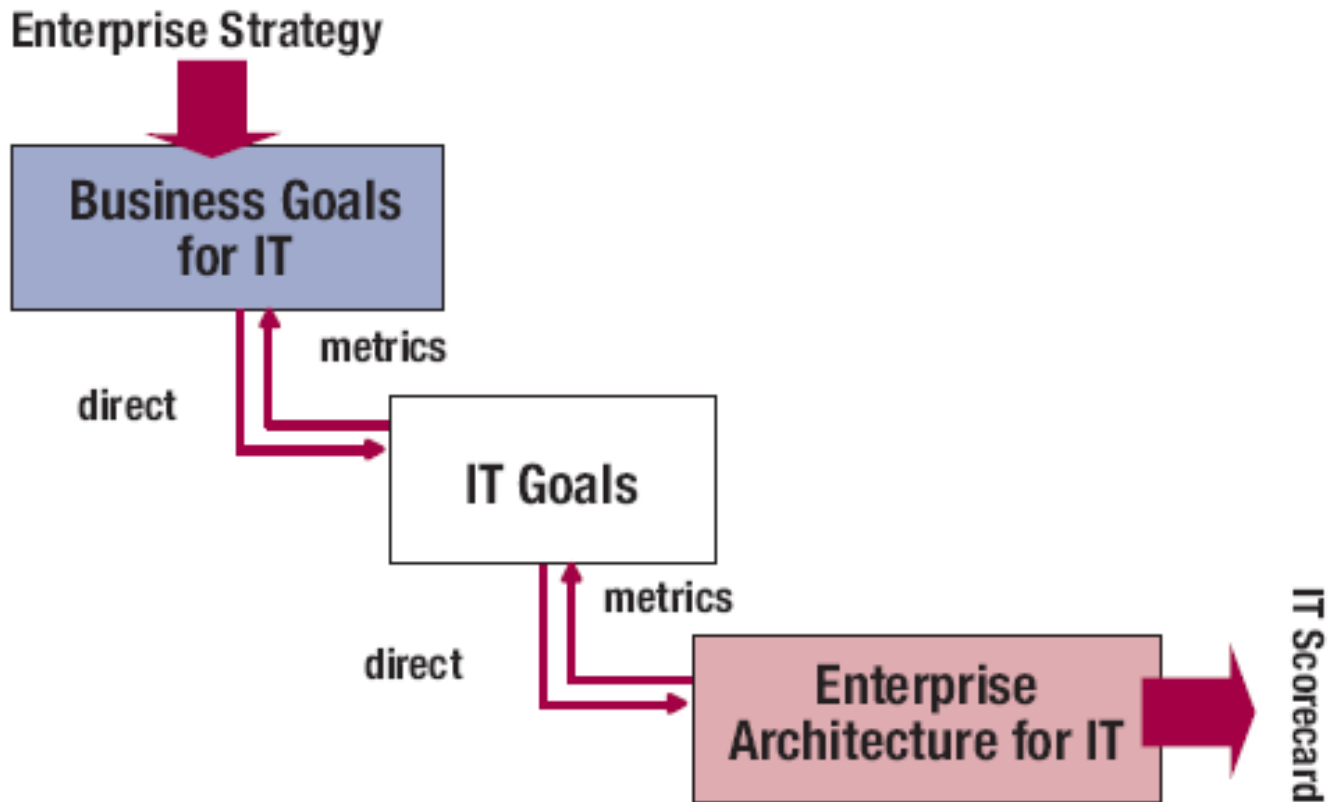


Process Oriented

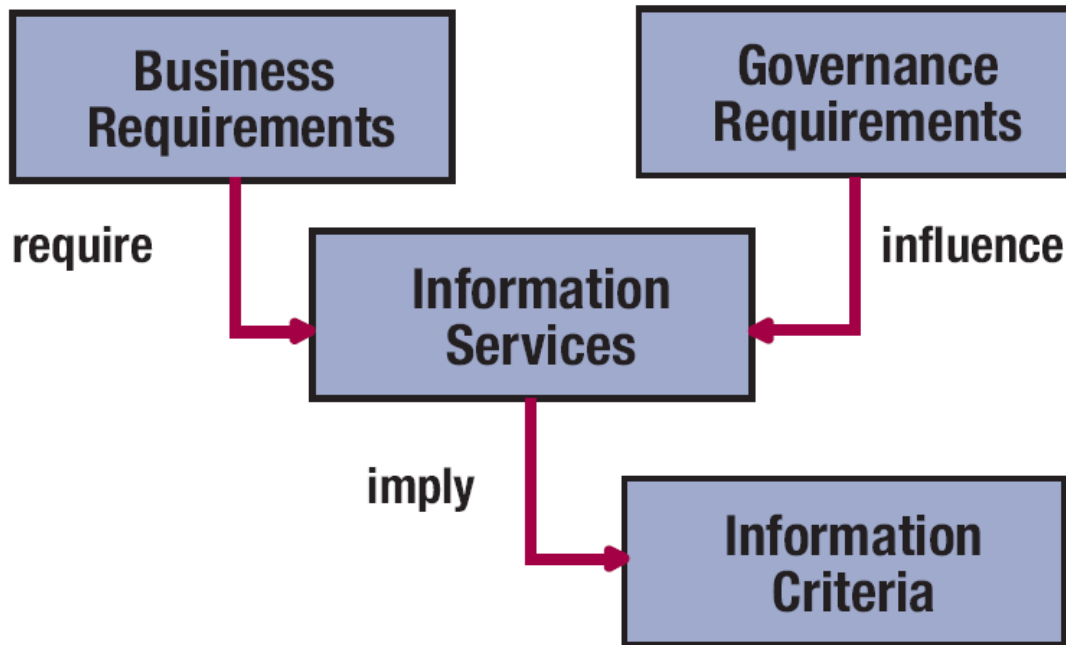
- ◆ Business Processes
 - ◆ Driven in terms of Business Outcomes
- ◆ Four Domains
 - ◆ Like the Deming/Shewhart Cycle
 - ◆ Plan & Organize
 - ◆ Acquire and Implement
 - ◆ Deliver and Support
 - ◆ Monitor and Evaluate



Business Processes



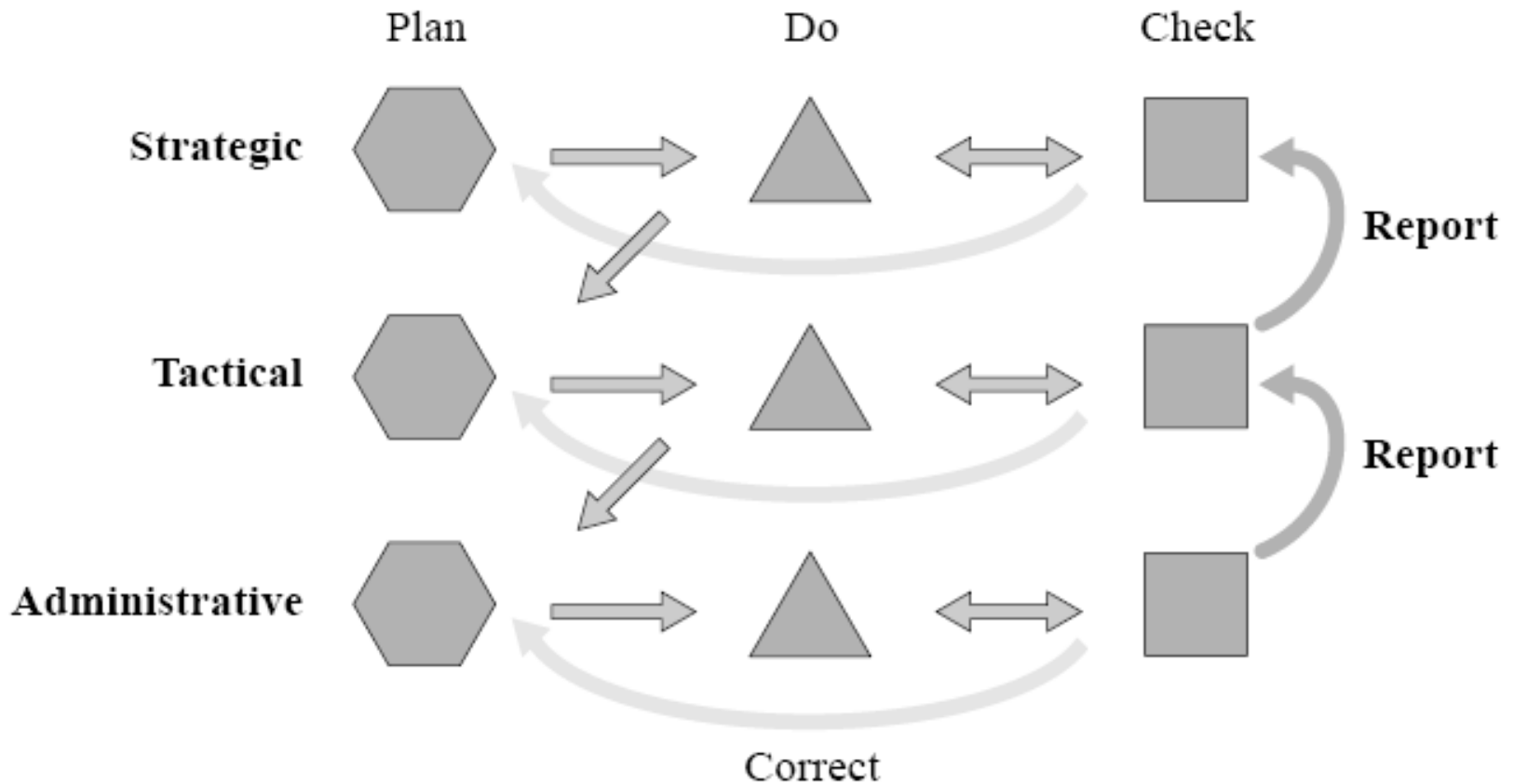
Driven in terms of Business Outcomes



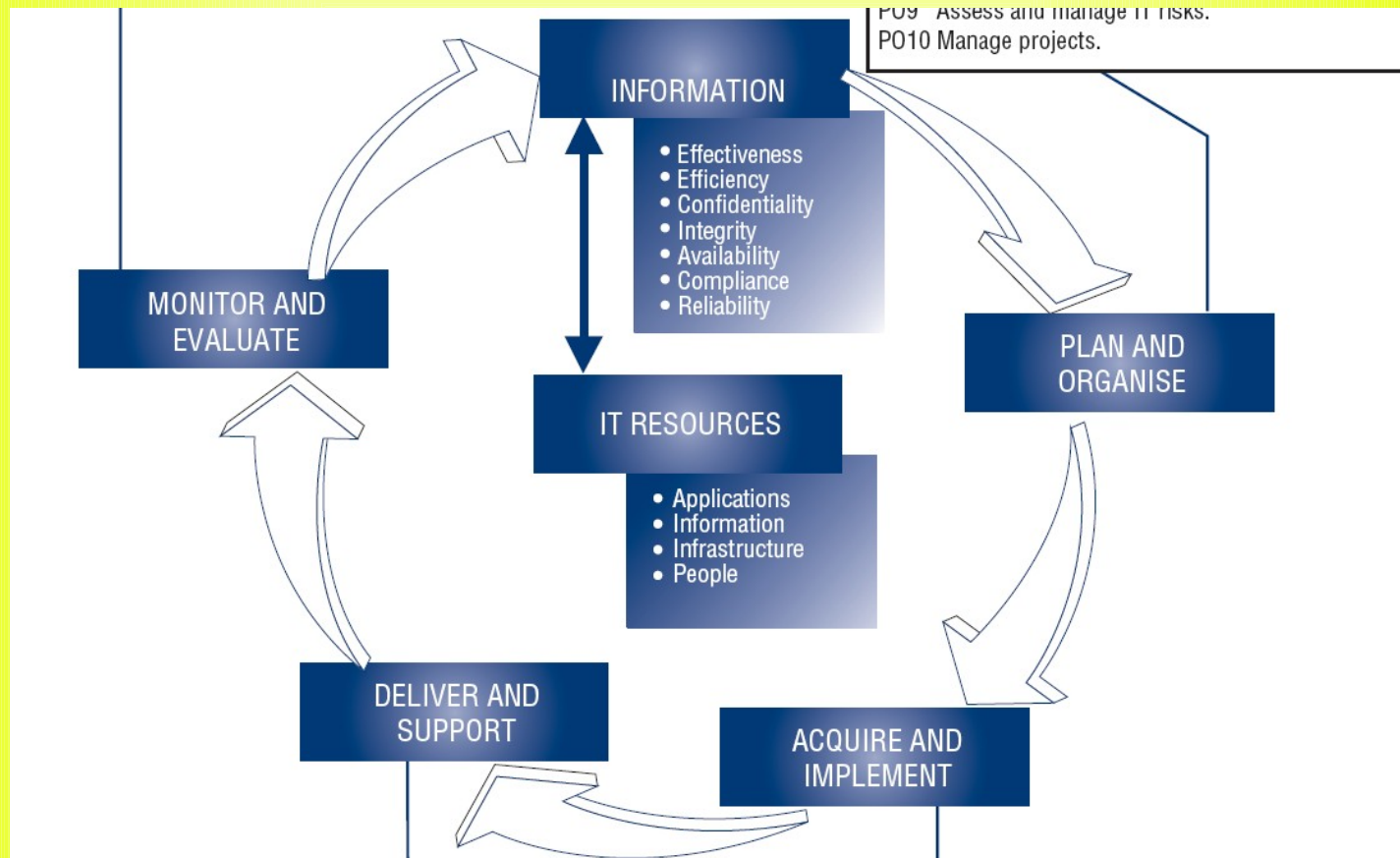
Business Goals for IT



Deming Cycle - at all levels



Four Domains



Plan & Organize

This domain covers **strategy and tactics**, and concerns the identification of the way IT can best contribute to the achievement of the **business objectives**. Furthermore, the realization of the strategic vision needs to be **planned, communicated and managed** for **different perspectives**. Finally, a proper organisation as well as technological domain infrastructure should be put in place.



Plan & Organize...

This typically addresses the following management questions:

Are IT and the business strategy aligned?

Is the enterprise achieving optimum use of its resources?

Does everyone in the organization understand the IT objectives?

Are IT risks understood and being managed?

Is the quality of IT systems appropriate for business needs?



Acquire and Implement

To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives.



Acquire and Implement...

This domain typically addresses the following management questions:

Are new projects likely to deliver solutions that meet business needs?

Are new projects likely to be delivered on time and within budget?

Will the new systems work properly when implemented?

Will changes be made without upsetting current business operations?



Deliver and Support

This domain is concerned with the actual **delivery** of **required** services, which includes service delivery, management of security and continuity, service support for users, and management of data and the operational facilities.



Deliver and Support...

It typically addresses the following management questions:

Are IT services being delivered in line with business priorities?

Are IT costs optimised?

Is the workforce able to use the IT systems productively and safely?

Are adequate confidentiality, integrity and availability in place?



Monitor and Evaluate

All IT processes need to be **regularly** assessed over time for their **quality** and **compliance** with control requirements. This domain addresses **performance management**, monitoring of internal control, regulatory compliance and providing **governance**.



Monitor and Evaluate...

It typically addresses the following management questions:

Is IT's performance measured to detect problems before it is too late?

Does management ensure that internal controls are effective and efficient?

Can IT performance be linked back to business goals?

Are risk, control, compliance and performance measured and reported?



Control Based

- ◆ Ownership & Responsibility
 - ◆ Data
 - ◆ Processes
 - ◆ Including inputs
- ◆ Business Controls vs IT Controls
 - ◆ Consistent
 - ◆ Consistent Results
 - ◆ Efficient and Effective

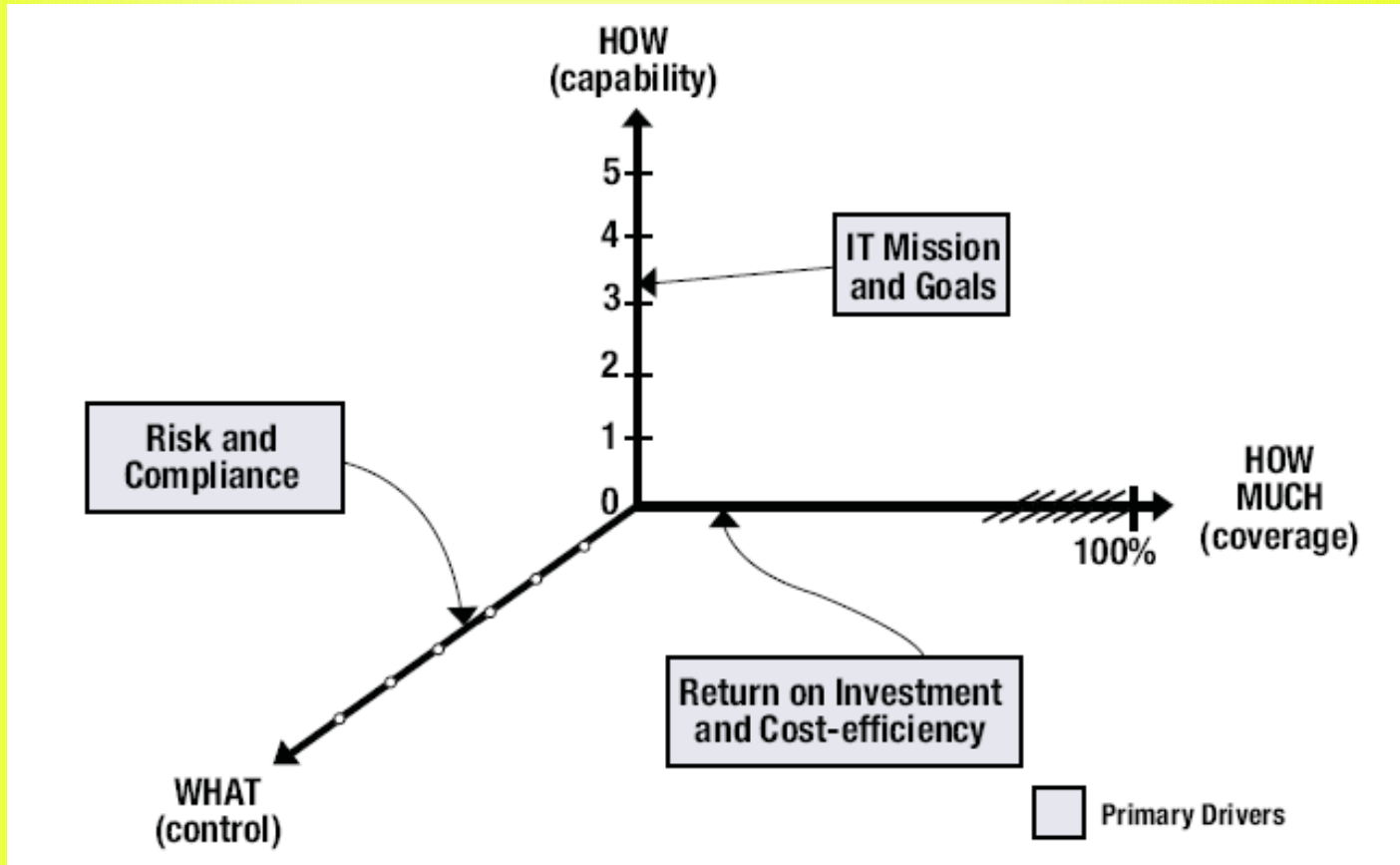


Measurement Driven

- ◆ Maturity Model
 - ◆ Consistent Benchmarking
 - ◆ Measure Improvement
 - ◆ Identify Areas of Concern
- ◆ Dimensions of Maturity
- ◆ Performance Goals
 - ◆ Capabilities not absolutes
 - ◆ Key Goal Indicators
 - ◆ Key Performance Indicators
- ◆ Activity Goals
- ◆ Key Indicators



Dimensions of Maturity



Misconceptions

- ◆ About the Role of Audit
- ◆ Only Two?
 - ◆ PO9
 - ◆ PO9 Inputs
 - ◆ PO9 Outputs
 - ◆ PO9 RACI
 - ◆ DS5
 - ◆ DS5 Inputs
 - ◆ DS5 Outputs
 - ◆ DS5 RACI
 - ◆ DS5 Relationship Between Goals and Metrics
- ◆ Pez will go into details about ITIL



Only Two?



Only Two?
That doesn't seem right



PO9

- ◆ PO9 Inputs
- ◆ PO9 Outputs
- ◆ PO9 RACI



PO9 Inputs

From	Inputs
P01	Strategic and tactical IT plans, IT service portfolio
P010	Project risk management plan
DS2	Supplier risks
DS4	Contingency test results
DS5	Security threats and vulnerabilities
ME1	Historical risk trends and events
ME4	Enterprise appetite for IT risks



PO9 Outputs

Outputs	To						
Risk assessment	P01	DS4	DS5	DS12	ME4		
Risk reporting	ME4						
IT-related risk management guidelines	P06						
IT-related risk remedial action plans	P04	A16					



PO9 RACI

RACI Chart

Functions

Activities

	CEO	CFO	Business Executive	CIO	Business Senior Management	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance Audit, Risk and Security
Determine risk management alignment (e.g., assess risk).	A	R/A	C	C	R/A	I					I
Understand relevant strategic business objectives.		C	C	R/A	C	C					I
Understand relevant business process objectives.				C	C	R/A					I
Identify internal IT objectives and establish risk context.					R/A		C	C	C		I
Identify events associated with objectives [some events are business-oriented (business is A); some are IT-oriented (IT is A, business is C)].	I			A/C	A	R	R	R	R		C
Assess risk associated with events.				A/C	A	R	R	R	R		C
Evaluate risk responses.	I	I	A	A/C	A	R	R	R	R		C
Prioritise and plan control activities.	C	C	A	A	R	R	C	C	C		C
Approve and ensure funding for risk action plans.		A	A		R	I	I	I	I		I
Maintain and monitor a risk action plan.	A	C	I	R	R	C	C	C	C	C	R

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.



DS5

- ◆ DS5 Inputs
- ◆ DS5 Outputs
- ◆ DS5 RACI
- ◆ DS5 Relationship Between Goals and Metrics



DS5 Inputs

From	Inputs
P02	Information architecture; assigned data classifications
P03	Technology standards
P09	Risk assessment
AI2	Application security controls specification
DS1	OLAs



DS5 Outputs

Outputs	To
Security incident definition	DS8
Specific training requirements on security awareness	DS7
Process performance reports	ME1
Required security changes	AI6
Security threats and vulnerabilities	P09



DS5 RACI

RACI Chart

Functions

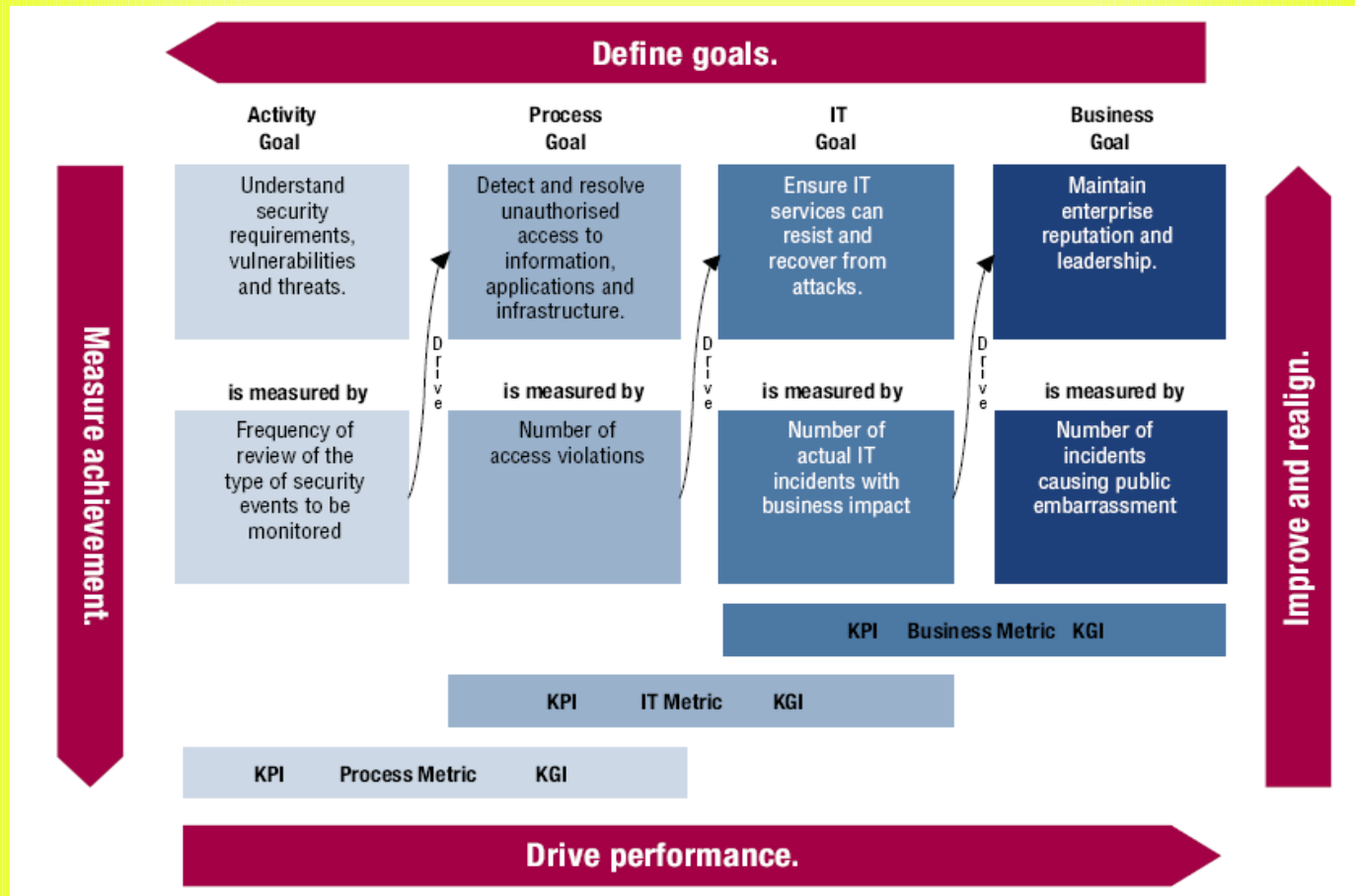
Activities

	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define and maintain an IT security plan.	I	C	C	A	C	C	C	C	I	I	R
Define, establish and operate an identity (account) management process.			I	A	C	R	R	I			C
Monitor potential and actual security incidents.				A	I	R	C	C			R
Periodically review and validate user access rights and privileges.				I	A	C					R
Establish and maintain procedures for maintaining and safeguarding cryptographic keys.				A		R			I		C
Implement and maintain technical and procedural controls to protect information flows across networks.				A	C	C	R	R			C
Conduct regular vulnerability assessments.		I		A	I	C	C	C			R

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.



DS5 Relationship between Goals and Metrics



More Information on COBIT

- ISACA

Information Systems Audit and Control Association
<http://www.isaca.org/cobit/>
COBIT-Online

- ITGI

IT Governance Institute
<http://www.itgi.org/>
Case Studies, Best Practices, ... more ...

An immense amount of freely downloadable supporting material



Pez will go into details about ITIL



The Fourth Canadian ISO 17799/ISO 27001 Conference

THANK YOU!



System Integrity
Toronto, Ontario

*The Fourth Annual Canadian
ISO 17799/ISO 17001 Conference*

30 Nov 2006/ Page 49
info@si.on.ca

Contact Information



System Integrity

“Security is not something that comes in a self-contained box. It requires a conscientious and continuous commitment that permeates every aspect of your enterprise and strategies. It is about understanding risks and managing them”

Anton J Aylward, CISSP CISA

aja@si.on.ca

<http://www.si.on.ca>

P: (416) 497-0201

C: (416) 509 9649

Blog: InfoSecBlog.antonaylward.com



System Integrity
Toronto, Ontario

*The Fourth Annual Canadian
ISO17799/ISO17001 Conference*

30 Nov 2006/ Page 50
info@si.on.ca