

Frameworks for IT Governance

Lynda Cooper – Fox IT



Whose job is it anyway?

In Head Office, Business and IT were looking out of their windows deep in thought...

The Board's View...



“IT Governance? That can’t be my responsibility, can it? I must focus on profitability and leave IT Governance to the IT people.”

The IT View...



“IT Governance? Nothing to do with IT really. Sounds to me like a job for the Board.”

If only they talked to each other...

Questions

How do I “do IT Governance”?

Where do COBIT, ITIL, ISO9000, ISO20000, ISO27001, CMMi and all the other frameworks fit with IT Governance?

Do I need them? Which ones? When? How do I combine them? Where do I get help?

Objectives and Agenda

To demonstrate how best practice and standards can be used to create a framework to support
IT Governance

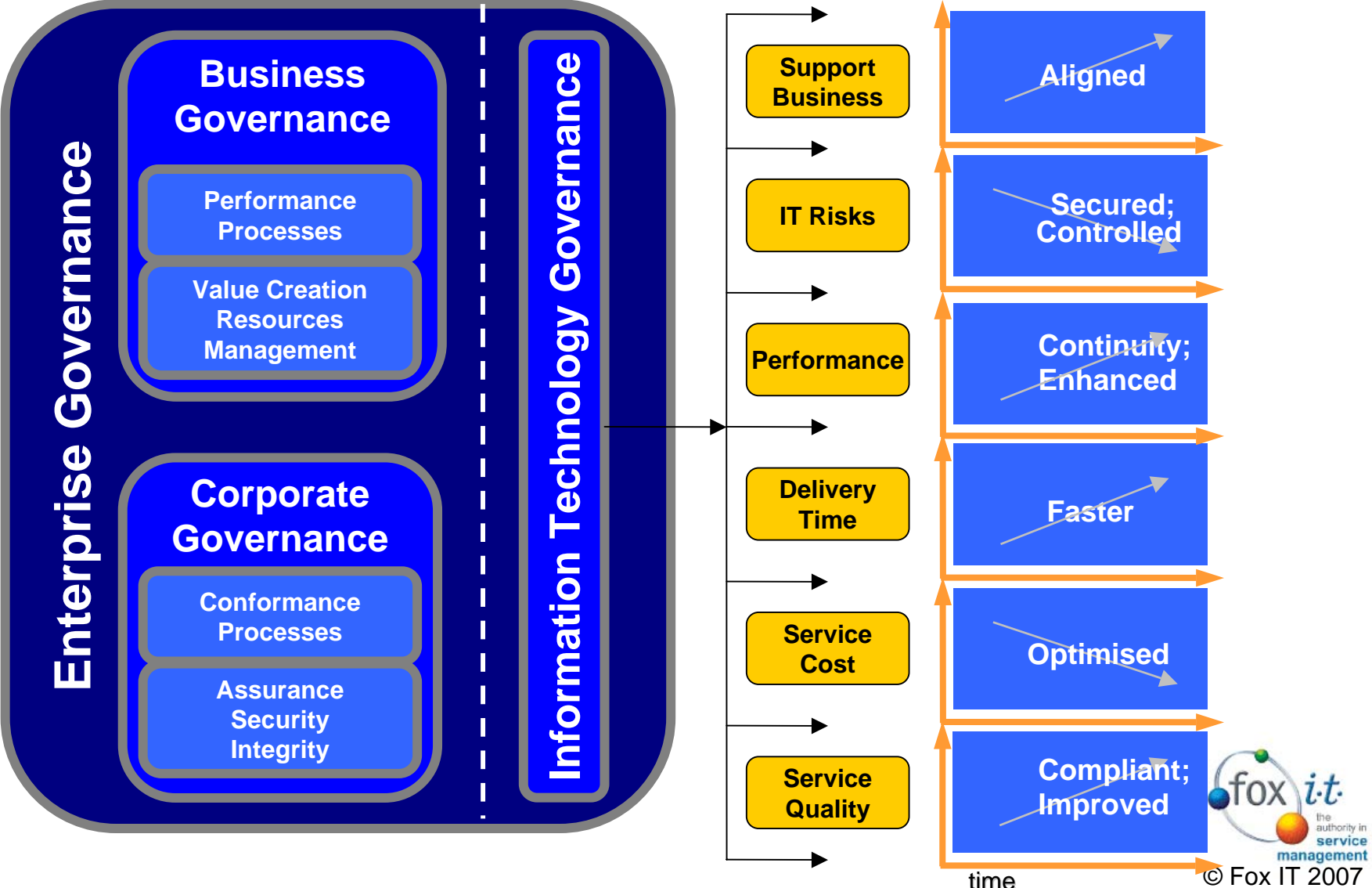
- IT Governance Challenge
- Creating a framework
- Framework constituents – a few
- Summary

- The Authority in Service Management
 - Authors of ITIL, MOF and BS15000/ISO20000, speakers, influencers
- The largest independent company focused on Service Management and IT Governance with a pedigree going back 25 years
- Services
 - Training
 - Consultancy
 - Product implementation
- UK based with offices in USA and partners in many countries across the globe
- www.foxit.net

IT Governance Challenge



Governance Overview



Who Wants to Govern IT?

Process	Governance Integrity Risk Security Compliance Performance Value Cost
Data	
System software and operations	Operational Management
Hardware and networks	

Why?

- Firms with superior IT governance had more than 20% higher profits than firms with poor governance given the same strategic objectives
- These top performers have custom designed IT Governance for their strategies

Peter Weill, MIT

So, what is the Management Challenge?

- The ability of an organisation to achieve its objectives depends upon the provision of effective IT services. Therefore, some significant challenges must be overcome. For example:
 - How does the organisation get IT under control, such that it delivers the information the enterprise needs?
 - How does the organisation manage the risks and secure the IT resources on which it is so dependent?
 - How does the organisation ensure that IT achieves its objectives and supports the business?

Responding to the Challenge

- Management must implement suitable policies, processes and plans, supported by appropriate control measures to ensure that they are followed.
- These, along with effective organisational structures must be designed to provide reasonable assurance that:
 - Business objectives are achieved
 - The right level of service is provided, at a reasonable price
 - Undesired events are prevented, or detected and corrected
 - Resources are managed efficiently
 - Performance is measured and reported to Senior Management

Developing the Solution

- The IT Governance requirements of each organisation are likely to be unique
- Senior Management must assess these requirements and develop an appropriate solution
- The solution is likely to be a composite framework, drawing upon elements of many different methodologies, techniques and standards

Creating a framework



What is a Framework?

- A mechanism used for steering, controlling or measuring the way in which organisations work (in this case with reference to IT)

- Broadly 3 types:-
 - Best Practice Guidelines
 - Standards
 - Measurement techniques

Industry best practice guidelines

- Recognised and used widely within the industry
- Created by a cross section of experts with practical experience
- Supported by reference material usually openly available
- Often also supported by a user group with tools, courses and qualifications
- A set of guidelines which organisations can implement selectively
- Cannot be certified as compliant

Best Practice	Area of usage
ITIL	IT Service Management
PRINCE2	Project Management
DSDM	Agile development
COBIT	IT Governance
COSO	Corporate Governance
PAS- 77	Service Continuity
AS8015	Corporate Governance of ICT
UK Combined Code	Corporate Governance
MoR, CRAMM	Risk Management
BS25999	Business Continuity

Standards

- Recognised and used widely
- Created on behalf of standards organisations (BSI in UK) by a cross section of experts representing relevant companies and organisations
- Standard is published and is usually supported by reference material
- Supported by a certification scheme
- Courses and qualifications usually available
- A set of mandatory clauses which can be certified as compliant by an independent auditor
- Must achieve full compliance to be certified
- Strict terms of certification and regular audits

Standard	Area of Usage
ISO20000	IT Service Management
ISO27001	Information Security
ISO19770	Software Asset management
ISO9000	Quality Management
TickIT	Application Development
ISO14001	Environmental management

Recognised Measurement Techniques

- Recognised and used widely within the industry
- Often created by experts within one organisation (or academia) and then adopted more widely
- Supported by reference material usually openly available
- Often also supported by a user group with tools, courses and qualifications
- A set of requirements which can be certified as compliant by an independent assessor
- Can often be certified for partial compliance
- Certification is usually not so strictly regulated as standards

Technique	Area of Usage
CMMi (Maturity scale of 1-5)	IT Application Development and PM Plus many other adaptations
EfQM Malcolm Baldrige	Organisation wide excellence model
JD Power/SSPA	Certified Technology Service and Support program
Six-Sigma Lean mgt	Process Improvement methods

Why use Frameworks?

Already exist

Why spend all of the time and effort to develop a framework based on limited experience when internationally developed standards already exist?

Structured

A Framework provides a structure that organisations can follow. Furthermore, the structure helps everyone be “on the same page” because they can see what is expected.

Best Practice

Developed over time and assessed by many people and organisations all over the world. The cumulative years of experience reflected in the models can not be matched by a single organisation's efforts.

Knowledge Sharing

Can share ideas between organisations, profit from user groups, Web sites, magazines, books and so on. Proponents of company-specific approaches do not have this luxury.

Auditable

Without standards, it becomes far more difficult for auditors, especially third-party auditors, to effectively assess control. Not all organisations will need (or want) to be audited against a standard.

Industry Analyst view

- IS process improvement through the use of standards (/best practices) helps answer increasing business demands for low cost, reliable information services and frees up IS management to think about contributing to transformational business initiatives. But which standard(/best practice) to use is anything but standard. The CIO must adopt an integrated approach to create business value. Gartner 2006
- Deploying new policies and procedures for each new regulation is simply too inefficient and costly. For example, many of the common IT Security requirements found in US IT compliance laws are addressed through ISO17799. Using industry standard frameworks will reduce the set of policies and controls that would result from individual compliance projects. ITCi 2006

Industry Analyst view

- ISO9000 adopted in 21% IS organisations, COBIT in 9% and CMMi in 4%. ITGI 2005
- Average development organisations increase productivity by 30% through the consistent use of IT standards(/best practices). Gartner 2006
- Most of the best practices and standards are not mutually exclusive and are most effective when used in combination such as ITIL, COBIT, CMM and ISO17799. Forrester 2006

Customised Framework Example

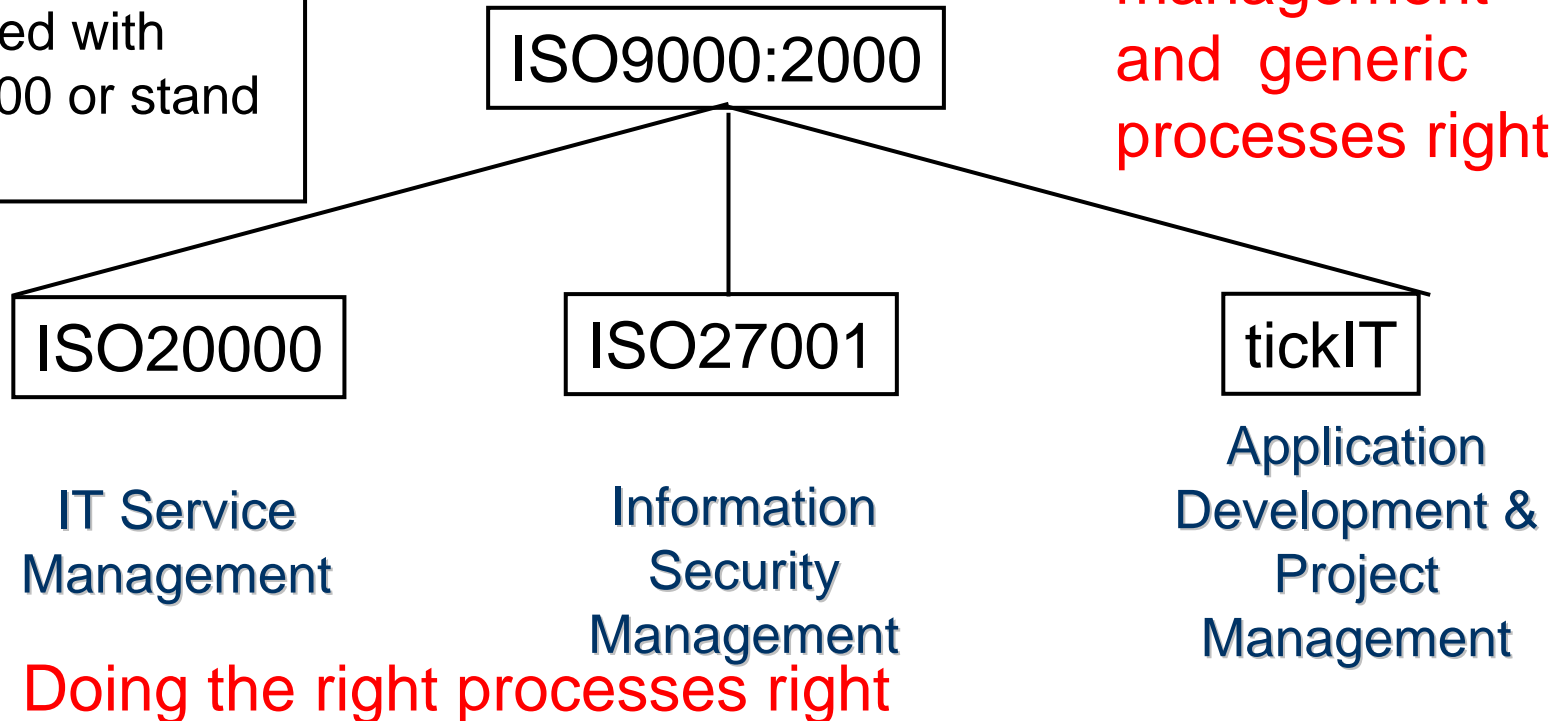
Corporate Governance			
ISO9000	EfQM	BS25999	
IT Governance			
ISO27001	COBIT	MoR	
IT Development		IT Services	
PRINCE2		ITIL	
DSDM		ISO20000	
CMMi			

Framework constituents - just a few!



ISO9000 and other standards

Lower level standards can be achieved with ISO9000 or stand alone.

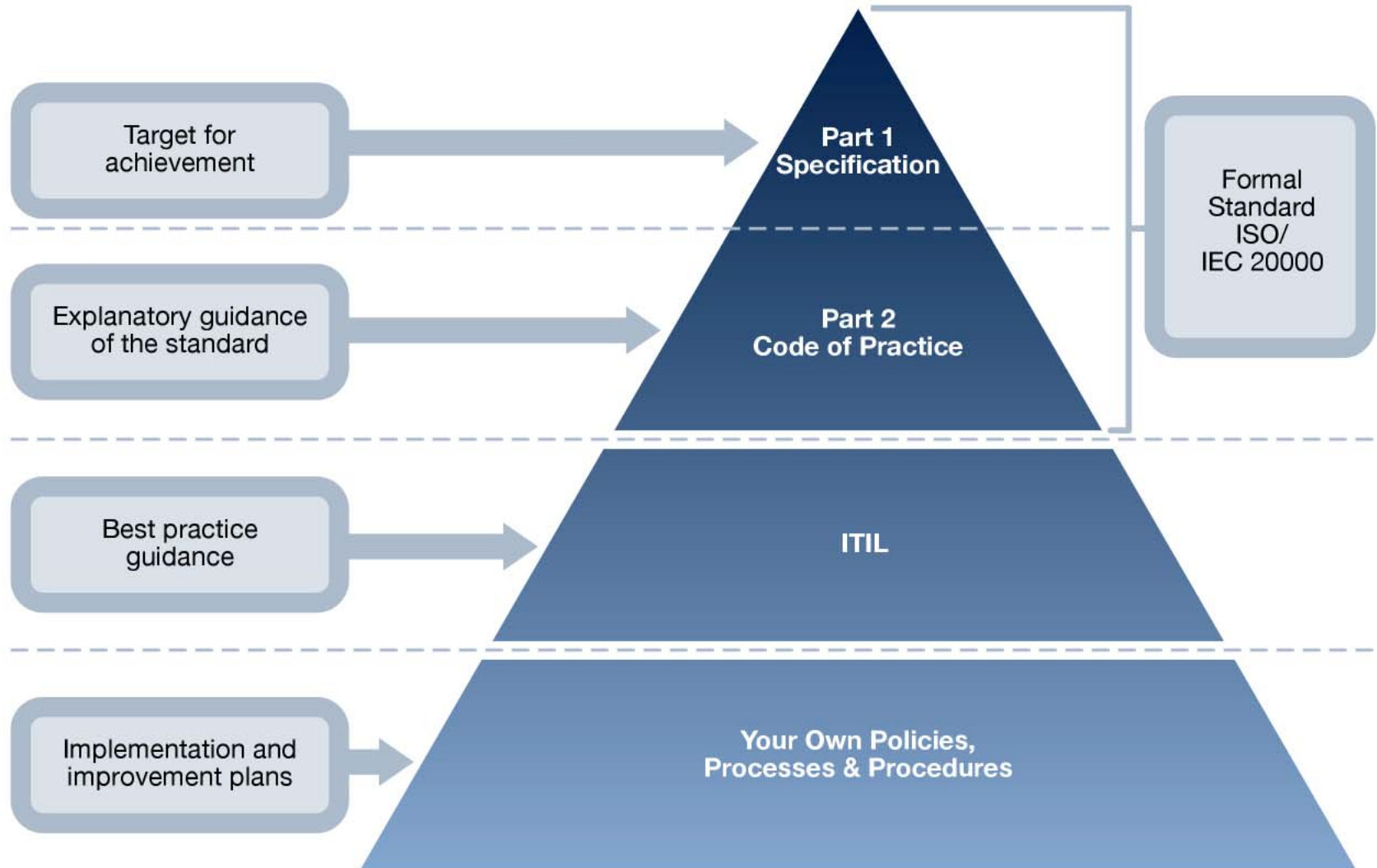


Provided scope is the same:

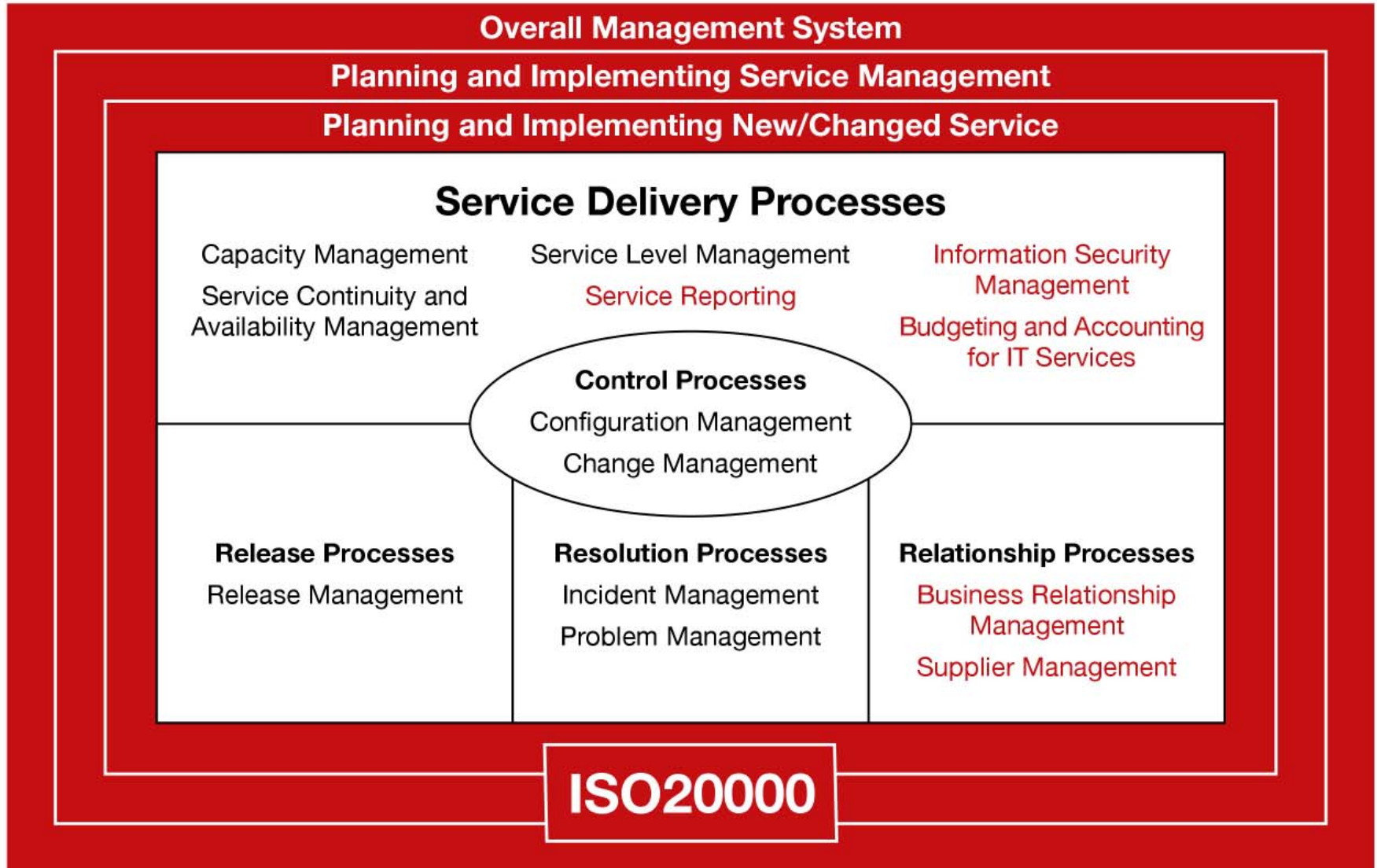
If you have ISO9001, then you will already be compliant with most of the management system requirements of ISO20000.

If you have BS7799/ISO27001, then you will already be compliant with the Information Security aspects of ISO20000 as they are a sub-set.

IT Service Management standards and best practice framework

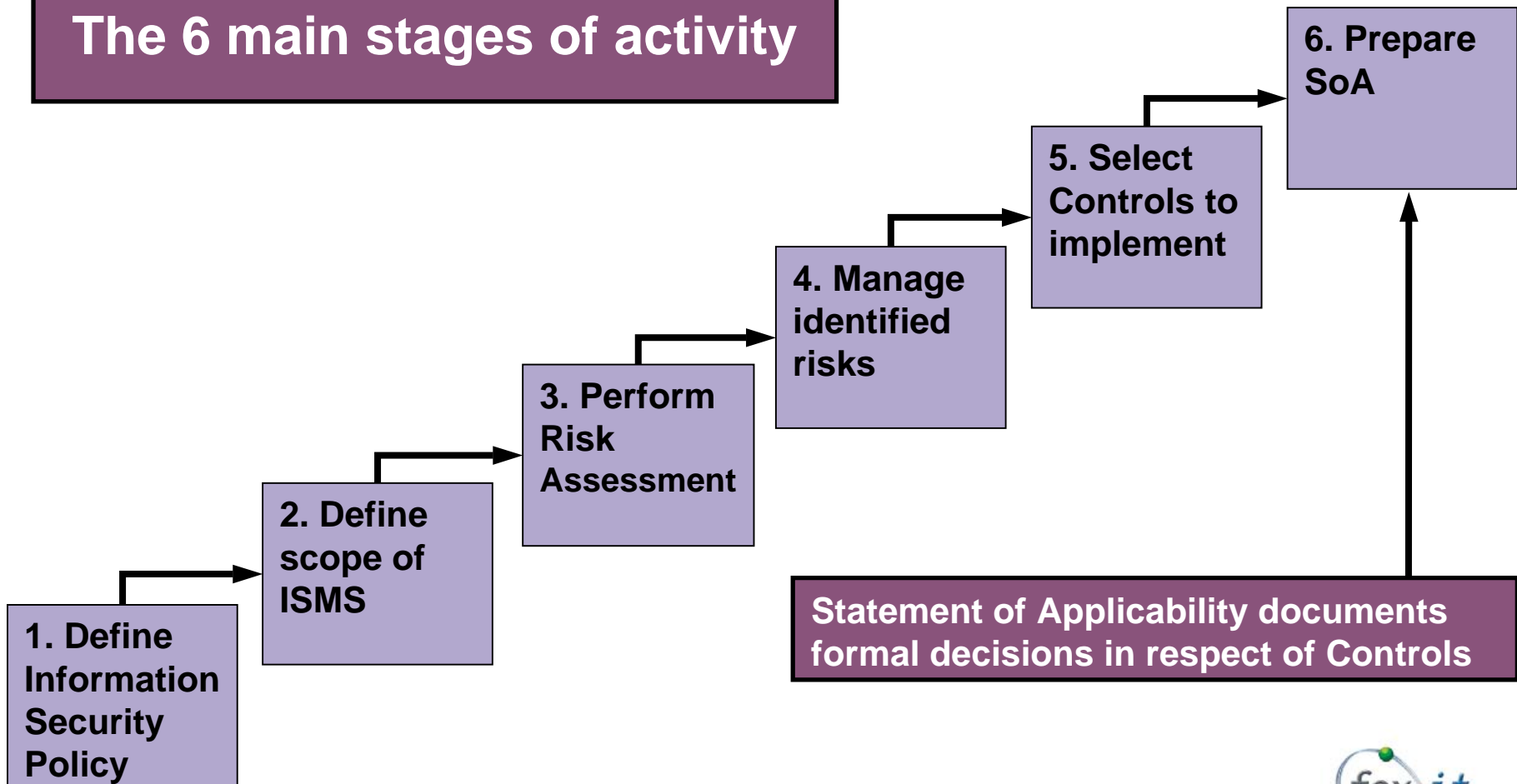


ISO20000 process model

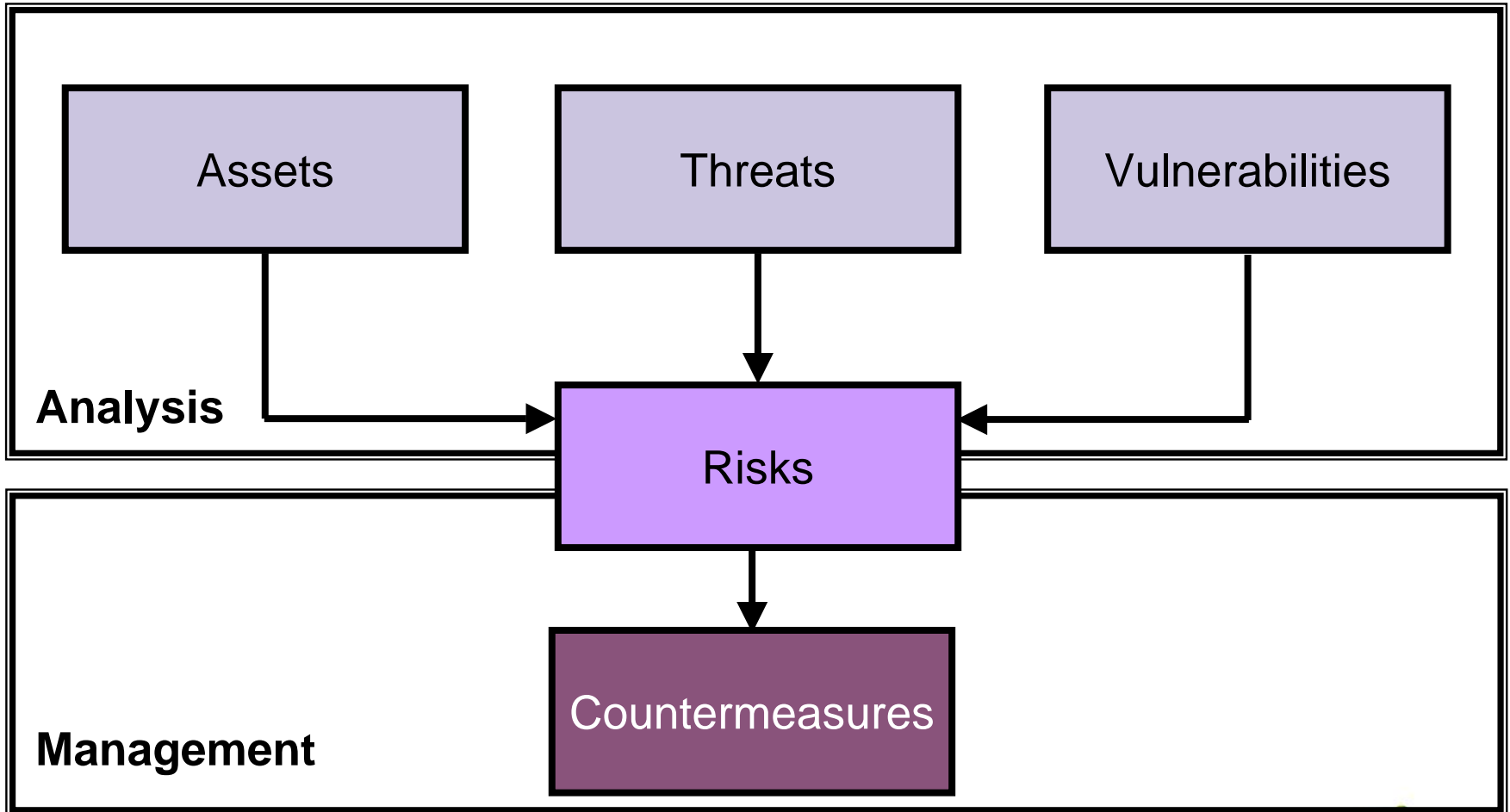


ISO17799 / ISO27001 – Information Security

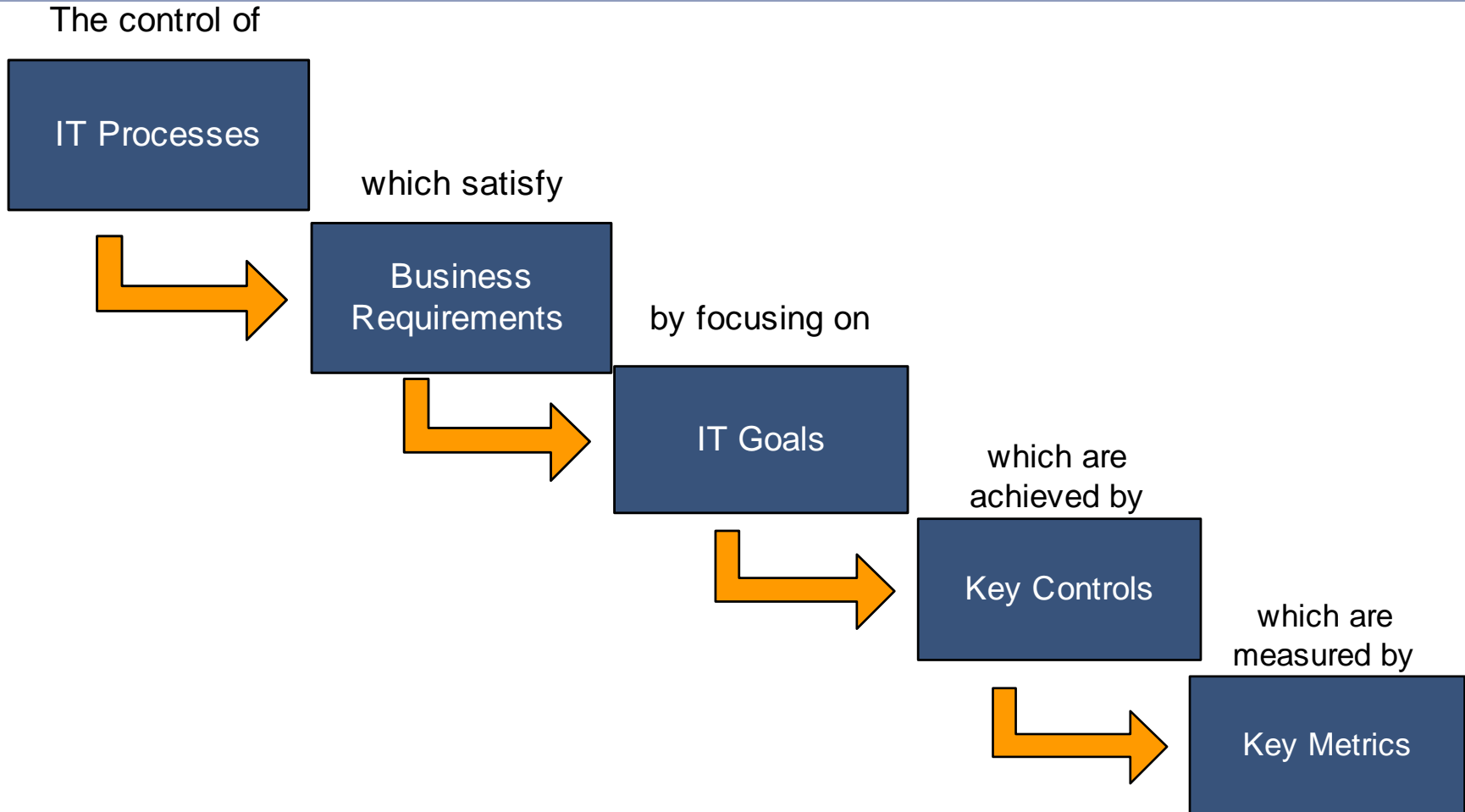
The 6 main stages of activity



CRAMM



The COBIT approach



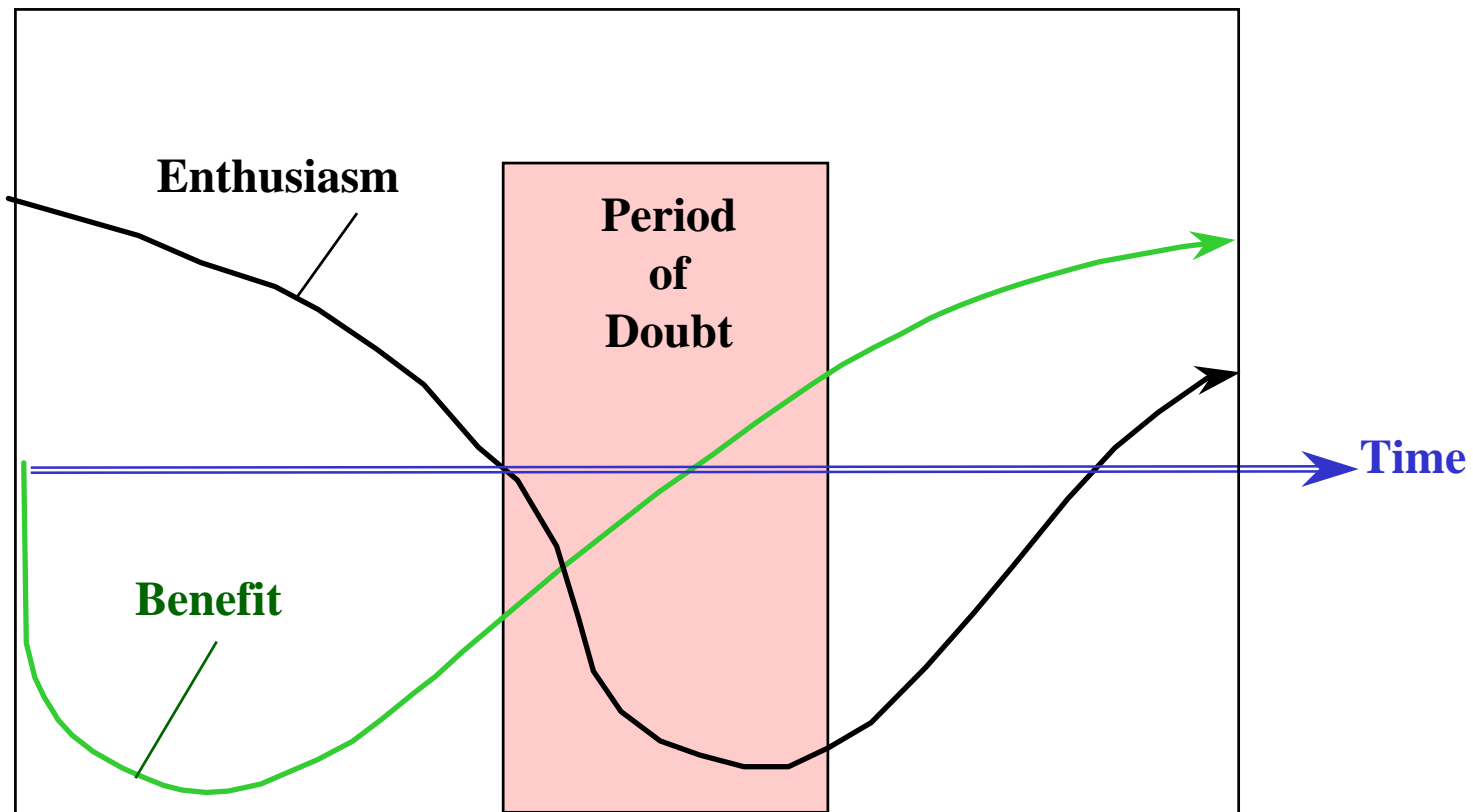
COBIT - Integrator of Best Practice

- COBIT is focused on what is required to achieve adequate management and control of IT, and is positioned at a high level
- COBIT focuses on getting the "what" right, without worrying about "how" things need to be done
- COBIT has been aligned and harmonised with other, more detailed, IT standards and best practices
- COBIT acts as an integrator of these different guidance materials, summarising key objectives under one umbrella framework that also links to governance and business requirements

Summary



Allow time!



Summary

- Best practice, standards and other measures all bring consistency, control, measurement and continuous improvement
- Selection, agreement, prioritisation and sponsorship of the appropriate framework for your business is critical to success
- Working together with defined interfaces, the framework will simplify and speed up the path to good corporate governance and support compliance and regulatory requirements

Questions?

● Lynda.cooper@foxit.net

● www.foxit.net