A lecture of lectures about CoBIT and ISO 27000

Dr. Hale
University of Nebraska at Omaha

Information Security and Policy– Lecture 6

Today’s topics:

Last Time recap: FISMA related docs

IS27000 Series

- slides from 2013 Jones and Bartlett Learning, LLC
- slides from 2007 Luděk Novák, CISA, CISSP
- ISO Assessment tool

CoBIT: Control Objectives for Information and related Technology

- slides from 2007 IT Governance Institute
- slides from 2013 Jones and Bartlett Learning, LLC

ISO 27000 related slides

Policy Frameworks

ISO/IEC 27000

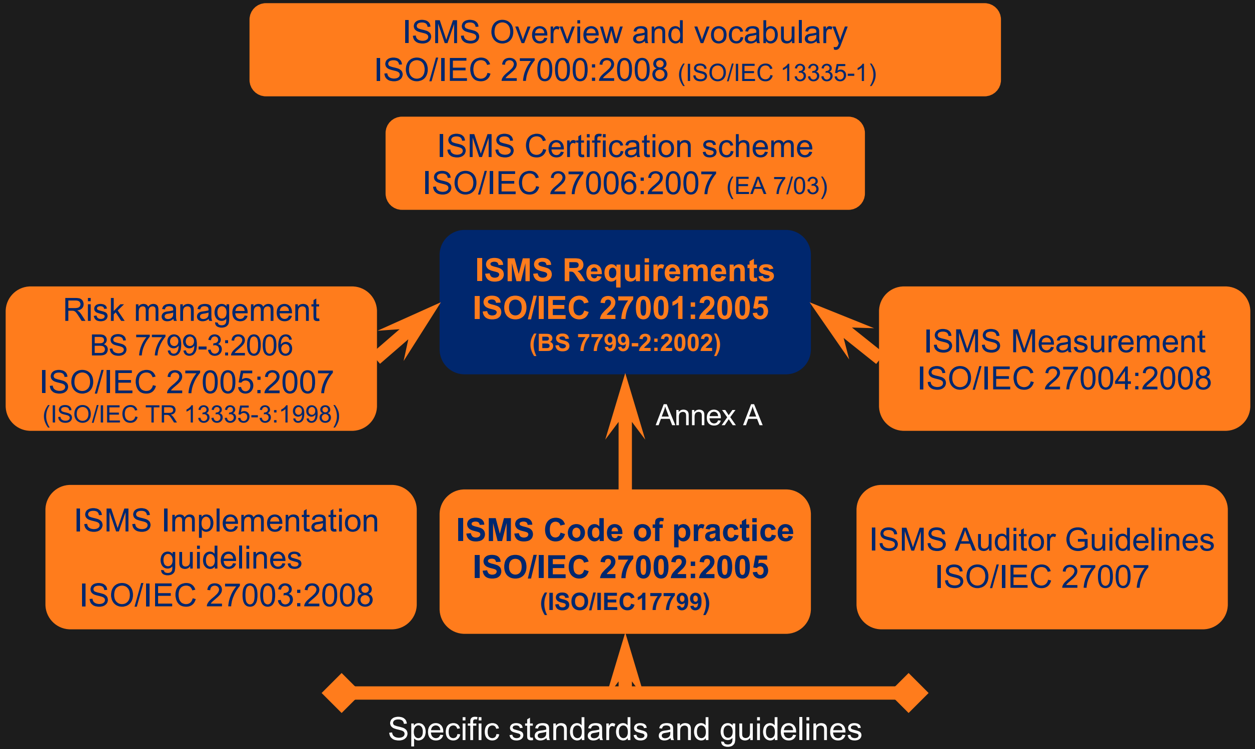
- The International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) develop and publish international standards.
- It is common to see these standards abbreviated to ISO/IEC.
- ISO/IEC 27001 and 27002 are the most interesting of the family

Overview of Documents

ISO 27000: Overview and Vocabulary
ISO 27001: ISMS Requirements
ISO 27002: Code of Practice
ISO 27003: ISMS Implementation Guidance
ISO 27004: ISM Measurement
ISO 27005: InfoSec Risk Management
ISO 27006: Requirements for Bodies Providing Audit and Certification of ISMS
ISO 27007 – 27008: Guidelines for Auditing InfoSec Controls
ISO 27014: Governance of InfoSec
ISO 27015: ISM Guidelines for Financial Services

Next Few slides from 2007 Luděk Novák, CISA, CISSP, modified by MLH 2015

ISO/IEC 27000 family review



ISMS Overview and vocabulary
ISO/IEC 27000:2008 (ISO/IEC 13335-1)

ISMS Certification scheme
ISO/IEC 27006:2007 (EA 7/03)

ISMS Requirements
ISO/IEC 27001:2005
(BS 7799-2:2002)

Risk management
BS 7799-3:2006
ISO/IEC 27005:2007
(ISO/IEC TR 13335-3:1998)

ISMS Measurement
ISO/IEC 27004:2008

Annex A

ISMS Implementation guidelines
ISO/IEC 27003:2008

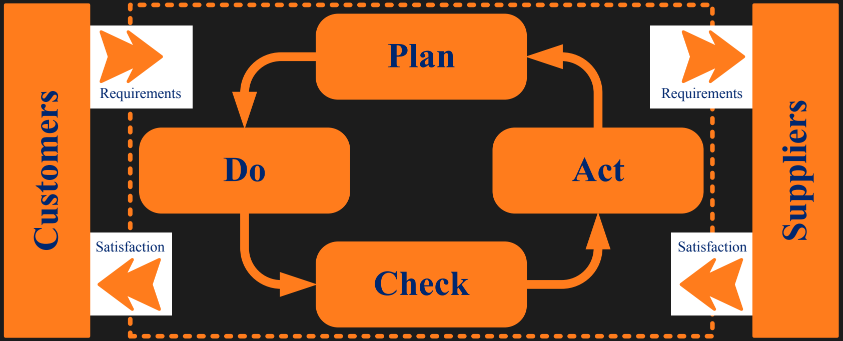
ISMS Code of practice
ISO/IEC 27002:2005
(ISO/IEC17799)

ISMS Auditor Guidelines
ISO/IEC 27007

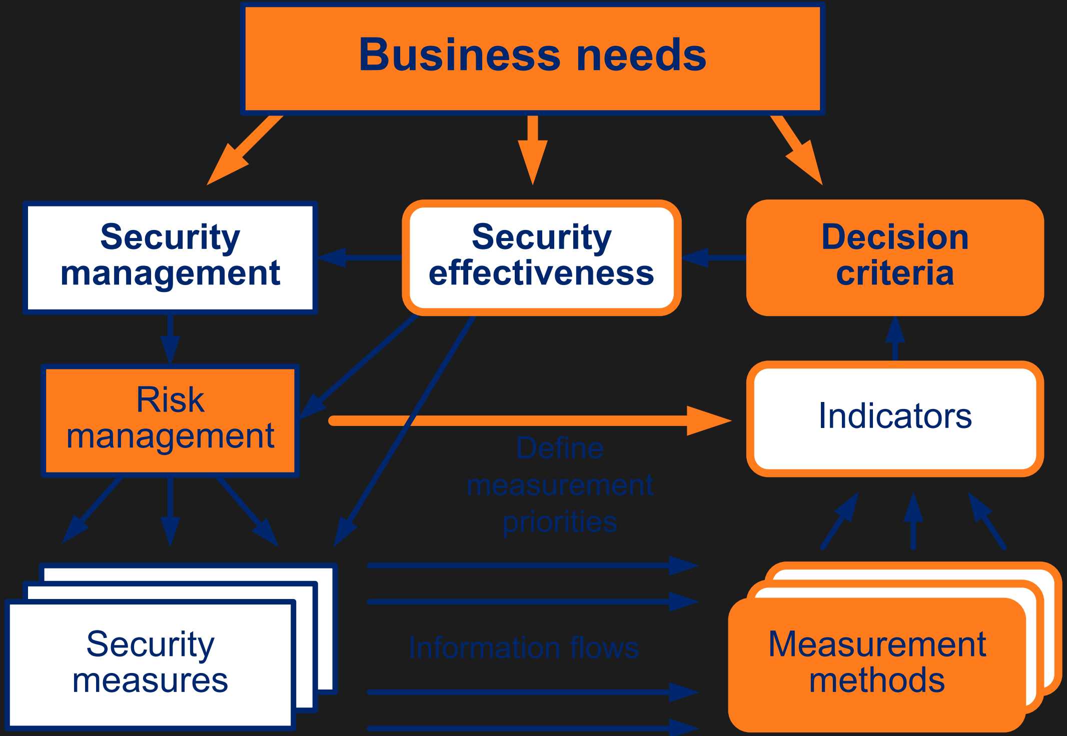
Specific standards and guidelines

ISO/IEC 27001:2013 principles

- Definition of requirements on Information Security Management System (ISMS)
- Information security management process based on PDCA Model
  - Plan – Do – Check – Act
- Ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties
- All defined requirements are mandatory and it is not possible to exclude anyone
  - **But it is not necessary to implement all security controls !!!**



ISMS Measurement as a feedback



Source: draft of ISO/IEC 27004

Examples of ISMS metrics

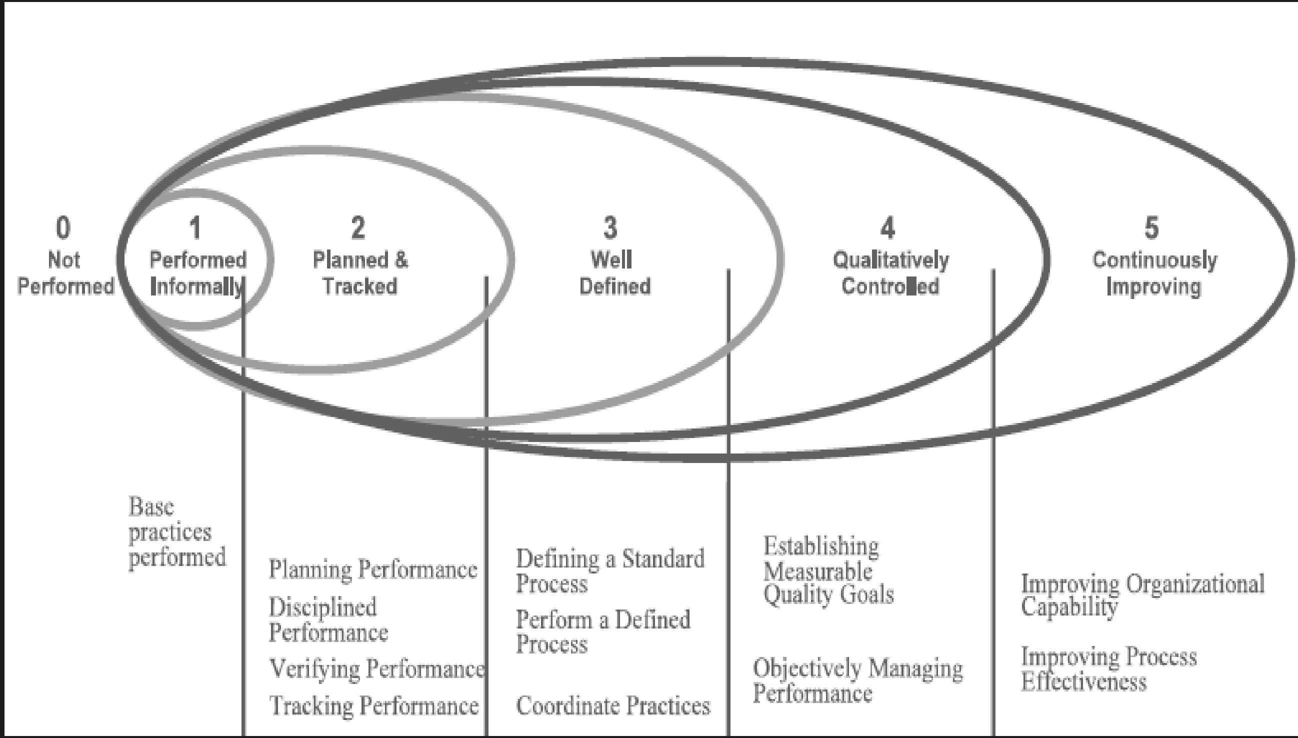
- Percentage (%) of system users/security personnel that have received basic awareness training
- Average frequency of audit records review and analyses for inappropriate activity
- Percentage of systems using automated mechanisms to conduct analysis and reporting of inappropriate activities
- Percentage (%) of systems that are compliant with the baseline configuration
- Percentage (%) of systems successfully addressed in the testing of the contingency plan
- Percentage of accounts not associated with specific users
- Percentage (%) of system components that undergo maintenance on schedule
- Cost of information security incidents of unauthorized access to information systems, due to physical security failures
- Percentage (%) of employees who signed acknowledgement that they have read and understood rules of behavior, before being authorized access to the information system

Source: NIST SP 800-80 Guide for Developing Performance Metrics for Information Security (draft)
http://csrc.nist.gov/publications/drafts/draft-sp800-80-ipd.pdf

CMM® Security

ISO/IEC 21827 – Systems Security Engineering – Capability Maturity Model (SSE-CMM®)

- Capability model for security
- Advantage: more levels to compare security enforcement



[GOTO ISO 27001 control documents]

Policy Frameworks

Some slides from 2013 Jones and Bartlett, modified by MLH 2015-2017

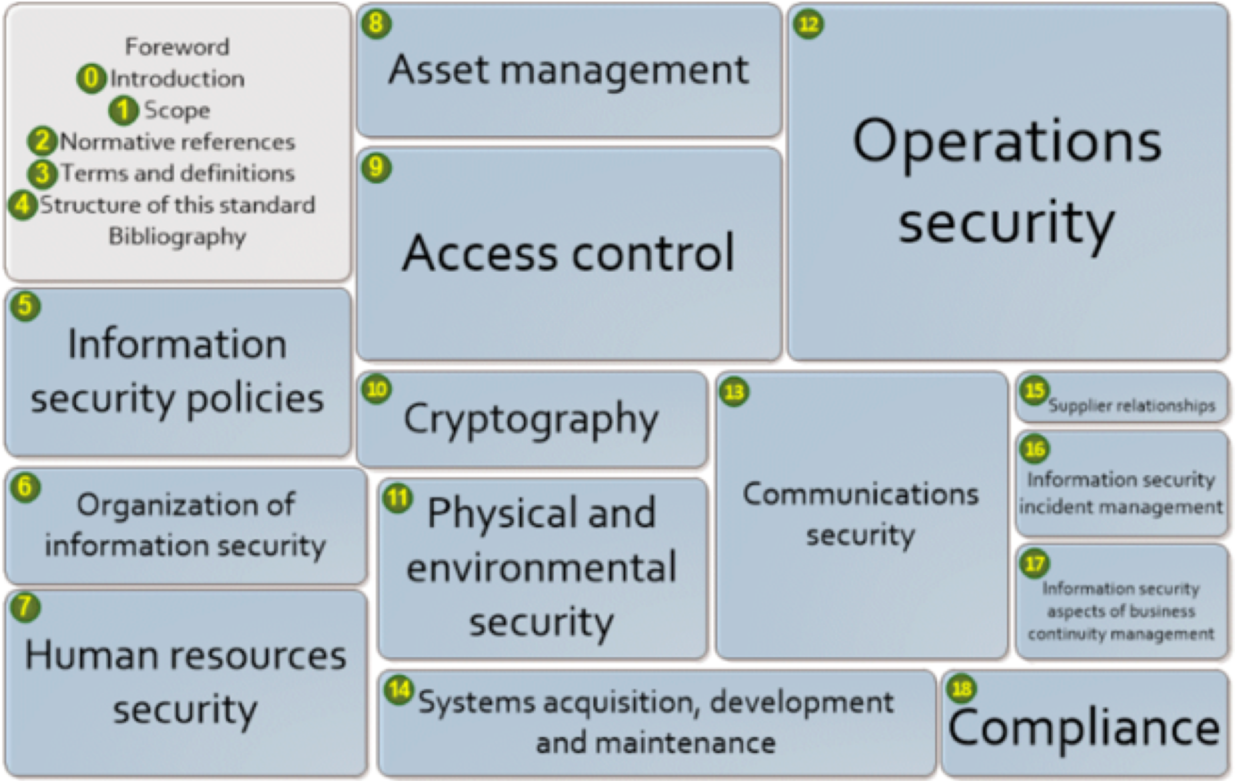
Policy Frameworks

ISO/IEC 27002 (2015)

ISO/IEC 27002 has 19 sections of best practices, of those, there are 12 main areas that compose the framework

Contents of ISO/IEC 27002:2015 New

In more detail, here is a breakdown summarizing the standard's 19 sections or chapters (21 if you include the unnumbered foreword and bibliography). ~~Click the diagram to jump to the~~ relevant description.



Foreword
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Structure of this standard
Bibliography

5 Information security policies

6 Organization of information security

7 Human resources security

8 Asset management

9 Access control

10 Cryptography

11 Physical and environmental security

12 Operations security

13 Communications security

14 Systems acquisition, development and maintenance

15 Supplier relationships

16 Information security incident management

17 Information security aspects of business continuity management

18 Compliance

© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

ISO/IEC 27002 (2015)

- ISO/IEC 27002 outlines 12 main areas that compose the framework:
  - Risk assessment and treatment
    - Describes how to perform periodic risk assessments.
  - Security policy
    - Describes how management should define an information security policy.
    - Organizations usually maintain detailed security policies in a library. Information security standards, procedures, and guidelines support the library.

ISO/IEC 27002 (2015)

- ISO/IEC 27002 outlines 12 main areas that compose the framework:
  - Organization of information security
    - Describes how to design and implement an information security governance structure.
    - Covers the need for an internal group that manages the program.
  - Asset management
    - Describes inventory and classification of information assets. The organization should understand what information assets it holds, and manage its security

ISO/IEC 27002 (2015)

- ISO/IEC 27002 outlines 12 main areas that compose the framework:
  - Human resources security
    - Describes security aspects for employees joining, moving, and leaving an organization. The organization should manage systems access rights.
  - Physical and environmental security
    - Describes the protection of computer facilities. Valuable IT equipment should be physically protected against malicious or accidental damage or loss.

ISO/IEC 27002 (2015)

- ISO/IEC 27002 outlines 12 main areas that compose the framework:
  - Communications and operations management
    - Describes management of technical security controls in systems and networks
  - Access control
    - Describes restriction of access rights of networks, systems, applications, functions, and data.
    - Addresses controlled logical access to IT systems, network, and data to prevent unauthorized.

Policy Frameworks

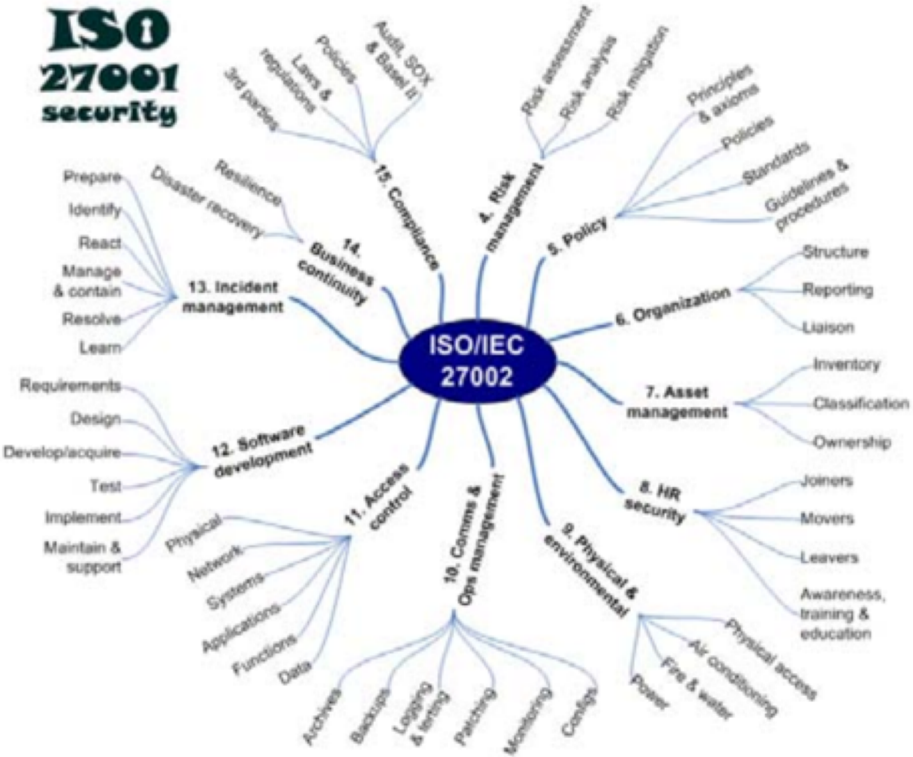
ISO/IEC 27002 (2015)

- ISO/IEC 27002 outlines 12 main areas that compose the framework:
  - Information systems acquisition, development, and maintenance
    - Describes building security into applications in the Systems Development Life Cycle (SDLC)
  - Information security incident management
    - Describes anticipating and responding appropriately to information security breaches.
    - Information security events, incidents, and weaknesses should be promptly reported and properly managed.

ISO/IEC 27002 (2015)

- ISO/IEC 27002 outlines 12 main areas that compose the framework:
  - Business continuity management
    - Describes protecting, maintaining, and recovering business-critical processes and systems.
    - Covers contingency planning from analysis and documentation to regular testing of the plans.
  - Compliance
    - legal requirements
    - security policies and standards, and technical compliance
    - audit considerations.

ISO 27001 Security

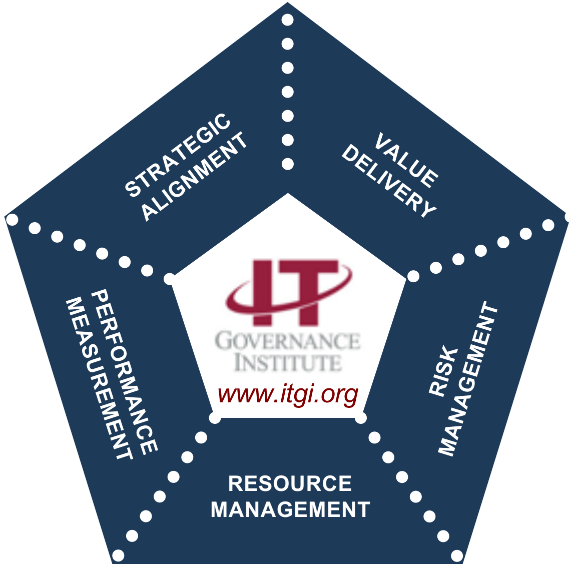


© 2013 Jones and Bartlett Learning, LLC, an Ascend Learning Company
www.jblearning.com
All rights reserved.

Next: CoBIT is at the highest level of “standards”

(next slides from 2007 IT governance institute, modified by mlh 2015)

The Need for IT Governance

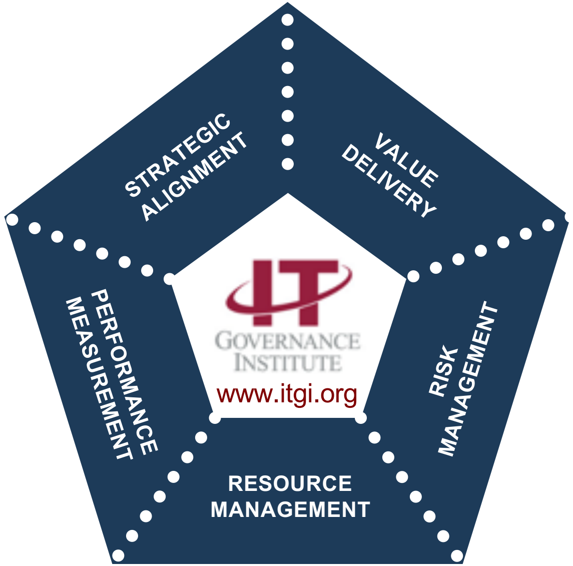


Enterprise governance is a set of responsibilities and practices exercised by the board and executive management with the goal of:

- Providing **strategic direction**
- Ensuring that **objectives** are achieved
- Ascertaining that **risks** are managed appropriately
- Verifying that the **enterprise's resources** are used responsibly

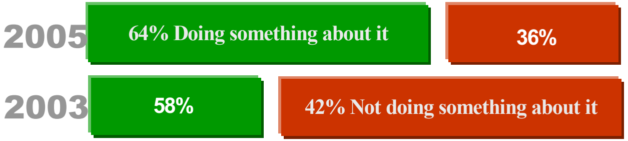
©2007 IT Governance Institute. All rights reserved.

IT Governance, as Defined by ITGI



IT governance is:

- The responsibility of the board of directors and executive management
- An **integral part** of enterprise governance, consisting of the leadership, organisational structures and processes that ensure that the **enterprise's IT sustains and extends the organisation's strategies and objectives**



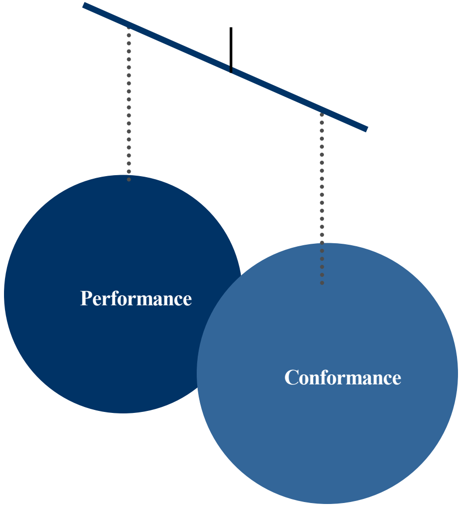
Source: Surveys by PwC for the IT Governance Institute Sep-Oct 2003 and Sep-Oct 2005

©2007 IT Governance Institute. All rights reserved.

Enterprise Governance Drives IT Governance

Enterprise governance is about:

- **Conformance**
  - Adhering to legislation, internal policies, audit requirements, etc.
- **Performance**
  - Improving profitability, efficiency, effectiveness, growth, etc.



Enterprise governance and IT governance require a balance between conformance and performance goals directed by the board.

©2007 IT Governance Institute. All rights reserved.

IT Governance Focus Areas

Strategic alignment

Focuses on ensuring the **linkage of business and IT plans**; on defining, maintaining and validating the **IT value proposition**; and on **aligning IT operations** with enterprise operations

Value delivery

Is about executing the **value proposition** throughout the delivery cycle, ensuring that IT delivers the **promised benefits against the strategy**, concentrating on optimising costs and proving the intrinsic value of IT

Resource management

Is about the optimal investment in, and the proper management of, **critical IT resources**: applications, information, infrastructure and people. Key issues relate to the **optimisation of knowledge and infrastructure.**

Risk management

Requires risk awareness by senior corporate officers, a clear understanding of the **enterprise's appetite for risk**, understanding of **compliance requirements**, transparency about the significant risks to the enterprise, and **embedding of risk management responsibilities** in the organisation

Performance measurement

Tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that **translate strategy into action** to achieve **goals measurable beyond conventional accounting**

©2007 IT Governance Institute. All rights reserved.

IT Governance Stakeholders

Board and executive	Set direction for IT, monitor results and insist on corrective measures
Business management	Defines business requirements for IT and ensures that value is delivered and risks are managed
IT management	Delivers and improves IT services as required by the business
IT audit	Provides independent assurance to demonstrate that IT delivers what is needed
Risk and compliance	Measures compliance with policies and focuses on alerts to new risks

©2007 IT Governance Institute. All rights reserved.

COBIT Provides a Framework for IT Governance

COBIT helps bridge the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure.

COBIT:

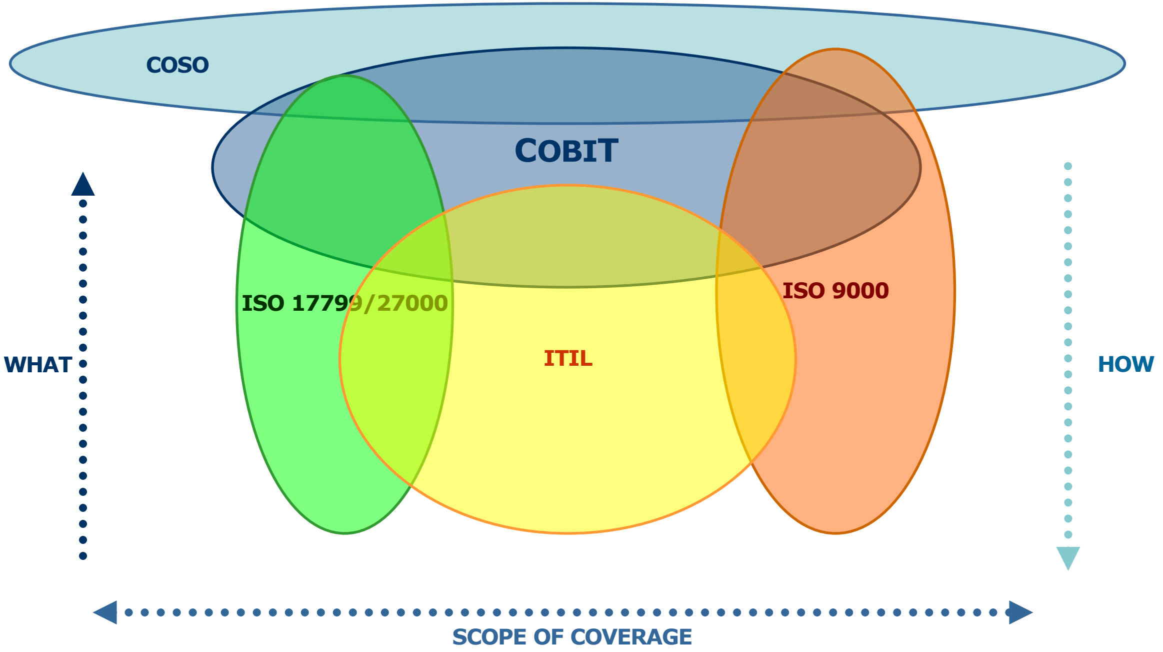
- Starts from business requirements
- Is process-oriented, organising IT activities into a generally accepted process model
- Identifies the major IT resources to be leveraged
- Defines the management control objectives to be considered
- Incorporates major international standards
- Has become the *de facto* standard for overall control of IT

IT resources need to be managed by a set of naturally grouped processes. COBIT provides a framework that achieves this objective.

©2007 IT Governance Institute. All rights reserved.

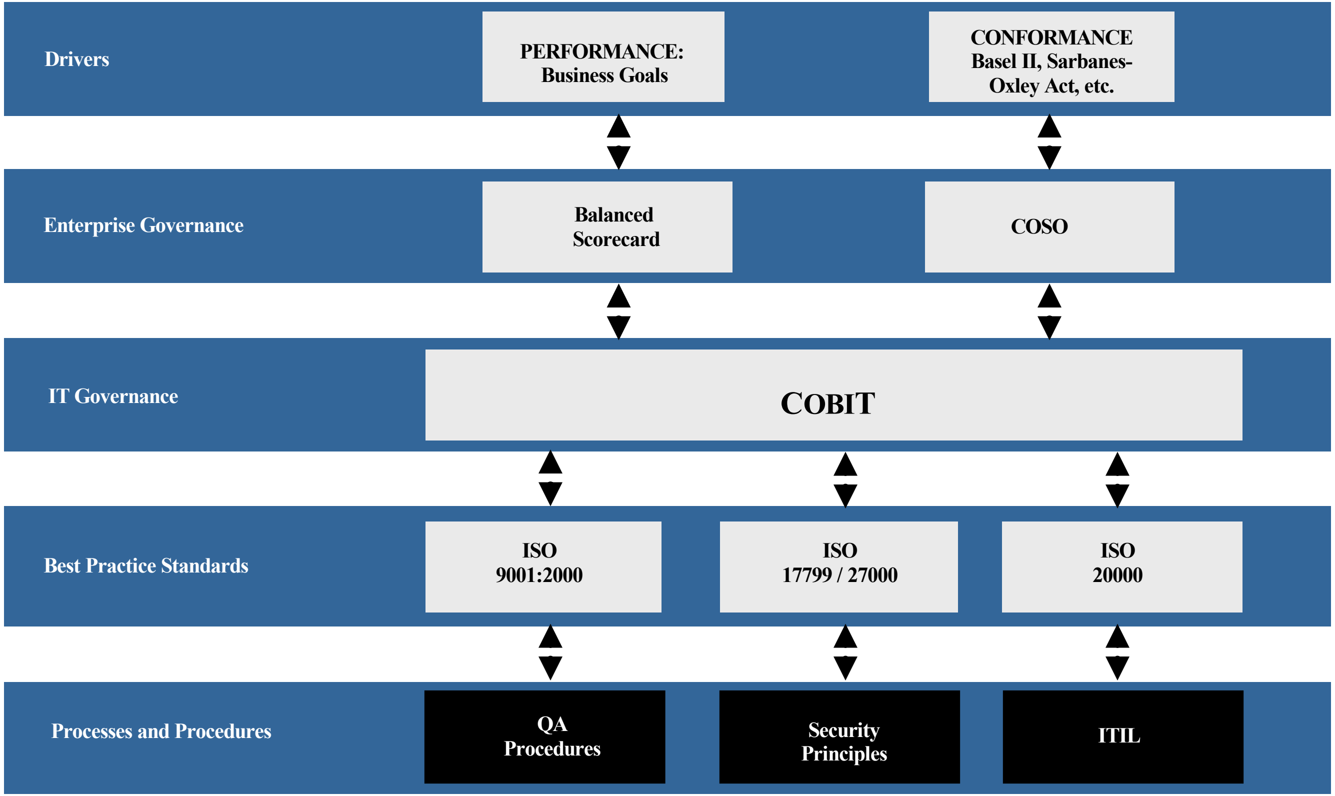
COBIT and Other IT Management Frameworks

Organisations will consider and use a variety of IT models, standards and best practices. These must be understood in order to consider how they can be used together, with COBIT acting as the consolidator (‘umbrella’).



©2007 IT Governance Institute. All rights reserved.

Where Does COBIT Fit?



Drivers — PERFORMANCE: Business Goals — CONFORMANCE Basel II, Sarbanes-Oxley Act, etc.

Enterprise Governance — Balanced Scorecard — COSO

IT Governance — COBIT

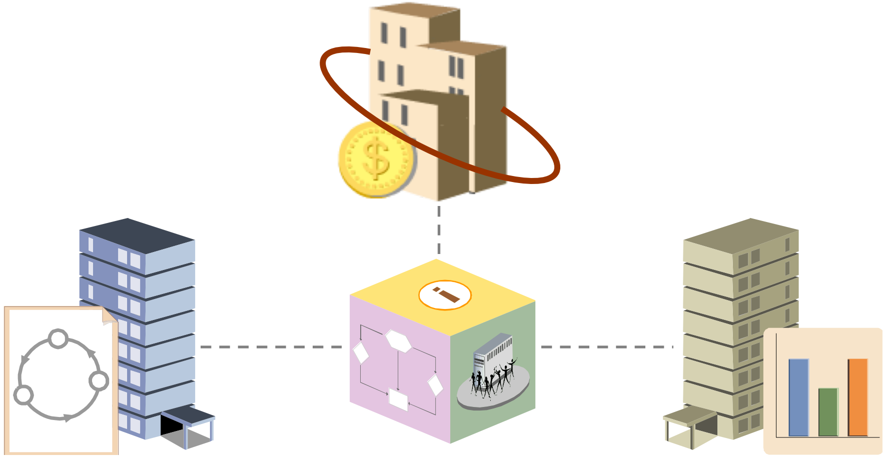
Best Practice Standards — ISO 9001:2000 — ISO 17799 / 27000 — ISO 20000

Processes and Procedures — QA Procedures — Security Principles — ITIL

©2007 IT Governance Institute. All rights reserved.

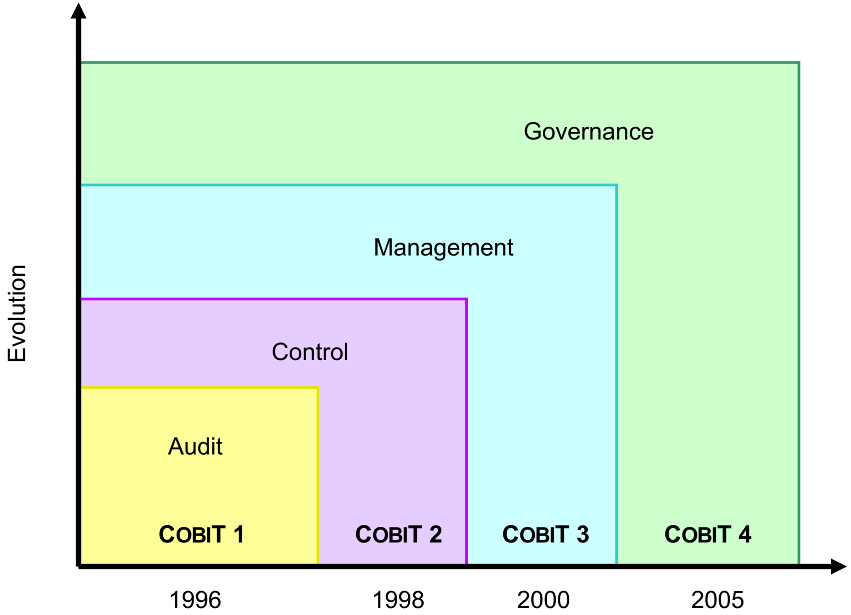
COBIT Framework

- The COBIT framework was created with the main characteristics:
  - Business-focused
  - Process-oriented
  - Controls-based
  - Measurement-driven
- The acronym COBIT stands for *Control Objectives for Information and related Technology*.



COBIT Framework Characteristics

COBIT: An IT Control Framework



For latest updates on COBIT, log on to *[www.isaca.org/cobit.](http://www.isaca.org/cobit)*

©2007 IT Governance Institute. All rights reserved.

COBIT: Value and Limitations

COBIT:

- Has internationally accepted good practices
- Is management-oriented
- Is supported by tools and training
- Is ~~freely downloadable~~ LIES!!!
- Allows the knowledge of expert volunteers to be shared and leveraged
- Continually evolves
- Is maintained by a reputable not-for-profit organisation
- Maps 100 percent to COSO
- Maps strongly to all major, related standards
- Is a reference, not an ‘off-the-shelf’ cure

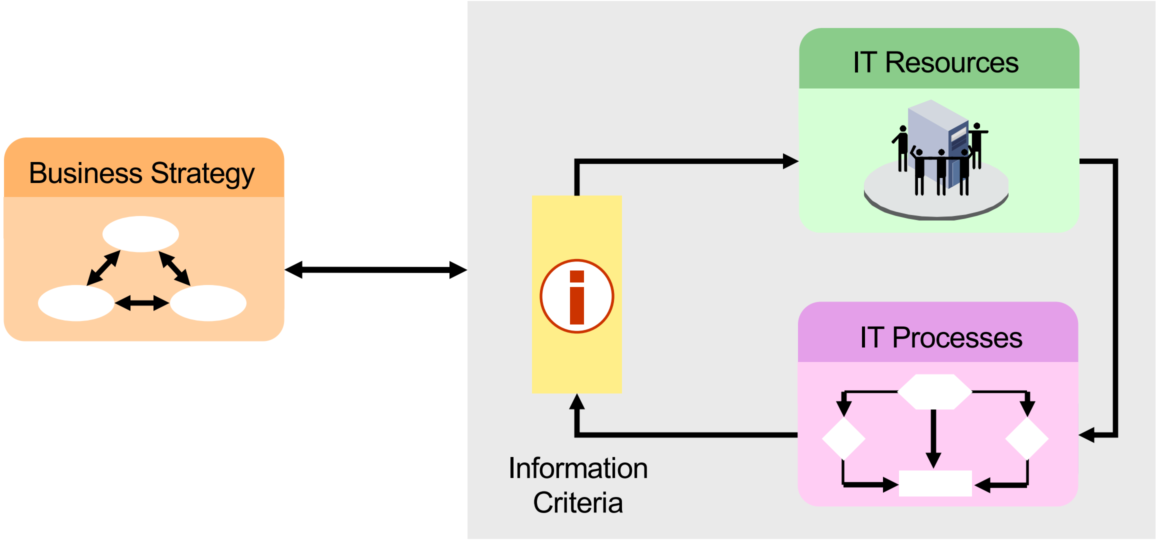
Enterprises still need to analyse control requirements and customise COBIT based on their:

- Value drivers
- Risk profile
- IT infrastructure, organisation and project portfolio

©2007 IT Governance Institute. All rights reserved.

CobiT Components

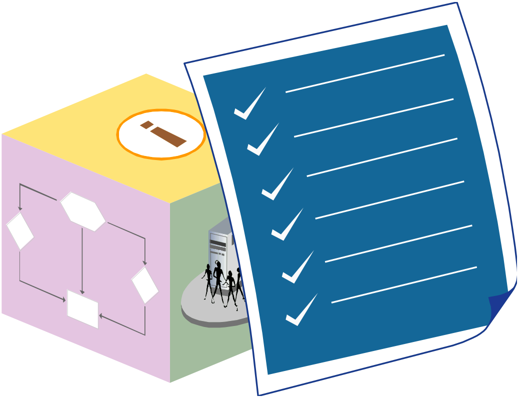
An organisation depends on reliable and timely data and information. COBIT components provide a comprehensive framework for delivering value while managing risk and control over data and information.



COBIT: Advantages

Some of the advantages of adopting COBIT are:

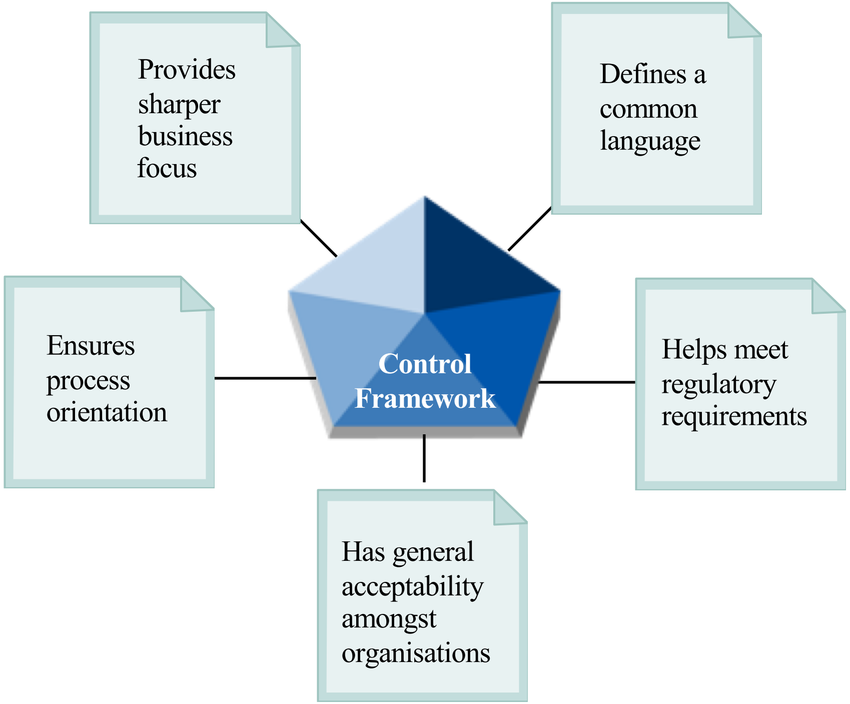
- COBIT is aligned with other standards and good practices and should be used together with them.
- COBIT's framework and supporting best practices provide a well-managed and flexible IT environment in an organisation.
- COBIT provides a control environment that is responsive to business needs and serves management and audit functions in terms of their control responsibilities.
- COBIT provides tools to help manage IT activities.



©2007 IT Governance Institute. All rights reserved.

COBIT and IT Governance

- COBIT focuses on improving IT governance in organisations.
- COBIT provides a framework to manage and control IT activities and supports five requirements for a control framework.



Control Framework

Provides sharper business focus

Defines a common language

Ensures process orientation

Helps meet regulatory requirements

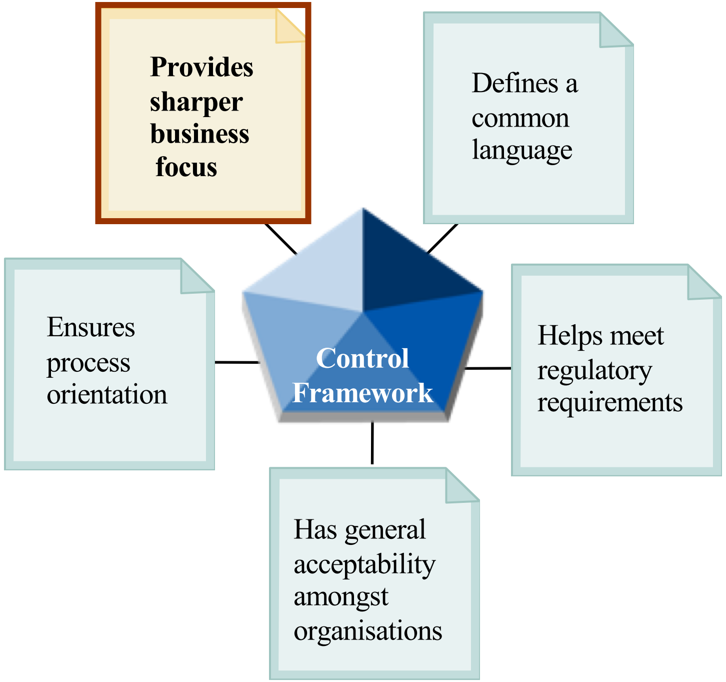
Has general acceptability amongst organisations

©2007 IT Governance Institute. All rights reserved.

COBIT and IT Governance *(Cont.)*

Business Focus

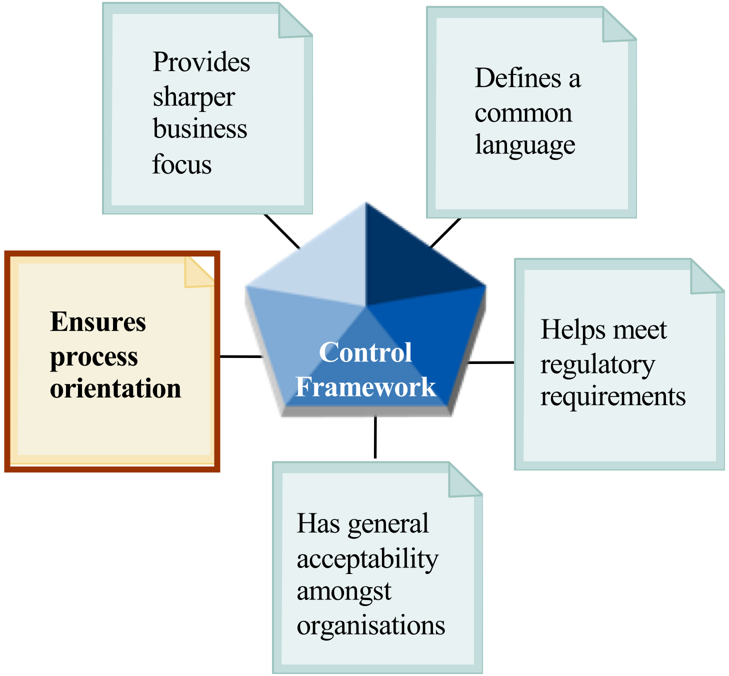
- COBIT achieves sharper business focus by aligning IT with business objectives.
- The measurement of IT performance should focus on IT's contribution to enabling and extending the business strategy.
- COBIT, supported by appropriate business-focused metrics, can ensure that the primary focus is value delivery and not technical excellence as an end in itself.


Provides sharper business focus
Defines a common language
Ensures process orientation
Control Framework
Helps meet regulatory requirements
Has general acceptability amongst organisations

COBIT and IT Governance *(Cont.)*

Process Orientation

- When organisations implement COBIT, their focus is more process-oriented.
- Incidents and problems no longer divert attention from processes.
- Exceptions can be clearly defined as part of standard processes.
- With process ownership defined, assigned and accepted, the organisation is better able to maintain control through periods of rapid change or organisational crisis.

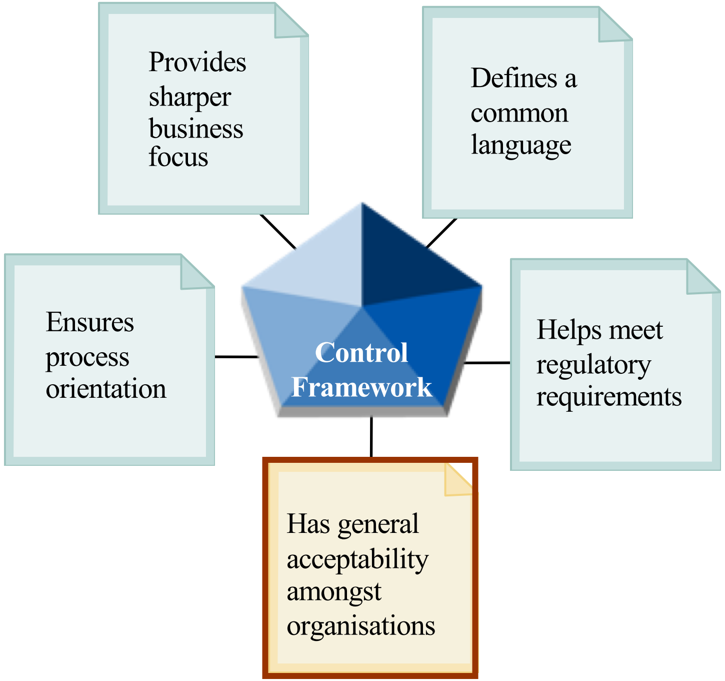

Provides sharper business focus
Defines a common language
Ensures process orientation
Control Framework
Helps meet regulatory requirements
Has general acceptability amongst organisations

©2007 IT Governance Institute. All rights reserved.

COBIT and IT Governance *(Cont.)*

General Acceptability

- COBIT is a proven and globally accepted standard for increasing the contribution of IT to organisational success.
- The framework continues to improve and develop to keep pace with good practices.
- IT professionals from all over the world contribute their ideas and time to regular review meetings.

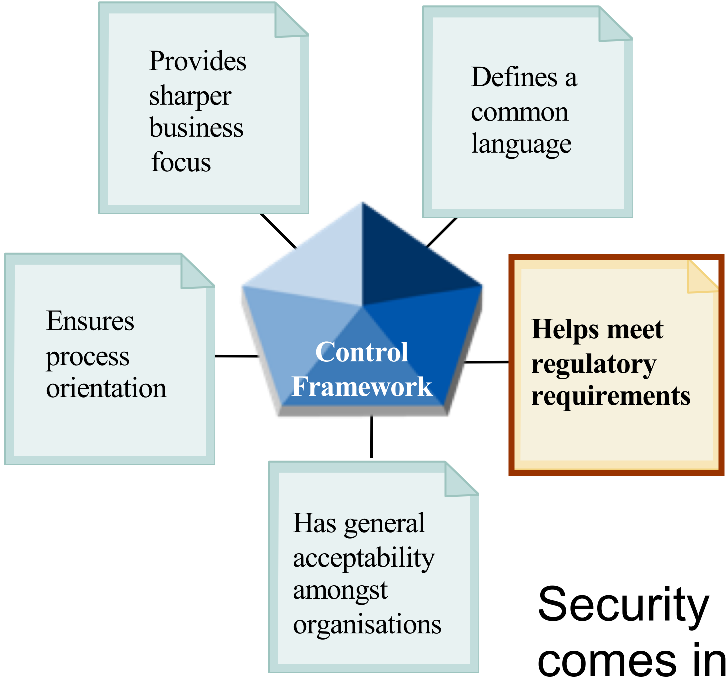

Provides sharper business focus
Defines a common language
Ensures process orientation
Control Framework
Helps meet regulatory requirements
Has general acceptability amongst organisations

©2007 IT Governance Institute. All rights reserved.

COBIT and IT Governance *(Cont.)*

Regulatory Requirements

- Recent corporate scandals have increased regulatory pressures on boards of directors to report their status and ensure that internal controls are appropriate. This pressure covers IT controls as well.
- Organisations constantly need to improve IT performance and demonstrate adequate controls over their IT activities.
- Many IT managers, advisors and auditors are turning to COBIT as the *de facto* response to regulatory IT requirements.


Provides sharper business focus
Defines a common language
Ensures process orientation
Control Framework
Helps meet regulatory requirements
Has general acceptability amongst organisations

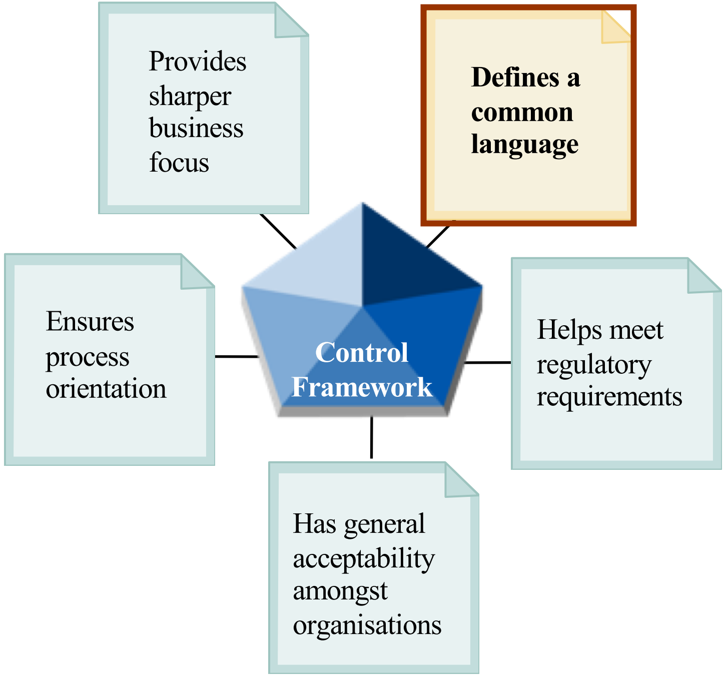
Security Baseline comes in here

©2007 IT Governance Institute. All rights reserved.

COBIT and IT Governance *(Cont.)*

Common Language

- A framework helps get everybody on the same page by defining critical terms and providing a glossary.
- Co-ordination within and across project teams and organisations can play a key role in the success of any project.
- Common language helps build confidence and trust.



Provides sharper business focus

Defines a common language

Ensures process orientation

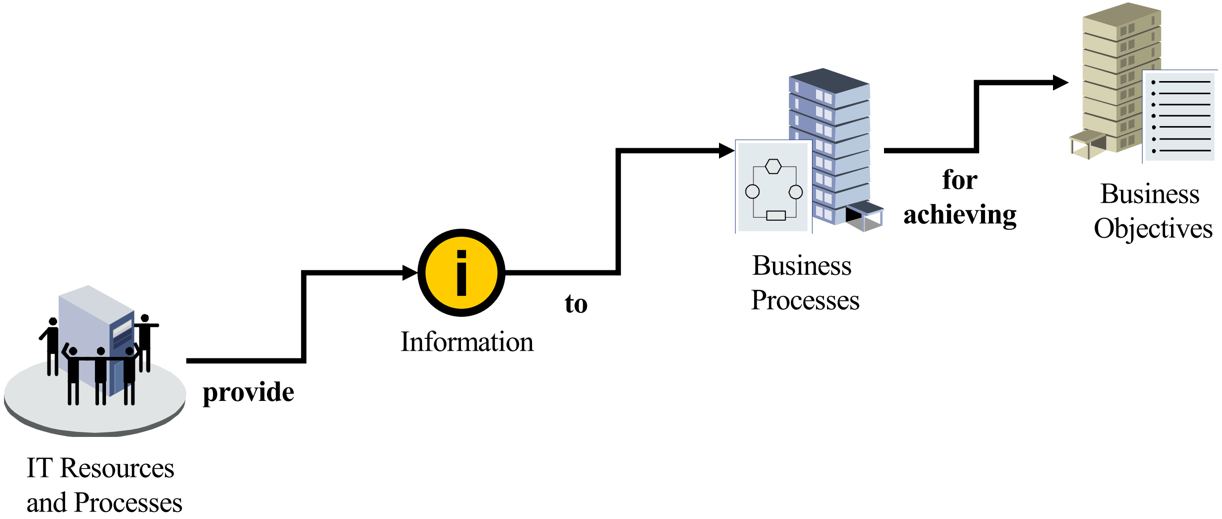
Control Framework

Helps meet regulatory requirements

Has general acceptability amongst organisations

COBIT: Premise

- The COBIT framework is based on the premise that IT needs to deliver the information that an enterprise requires to achieve its objectives.

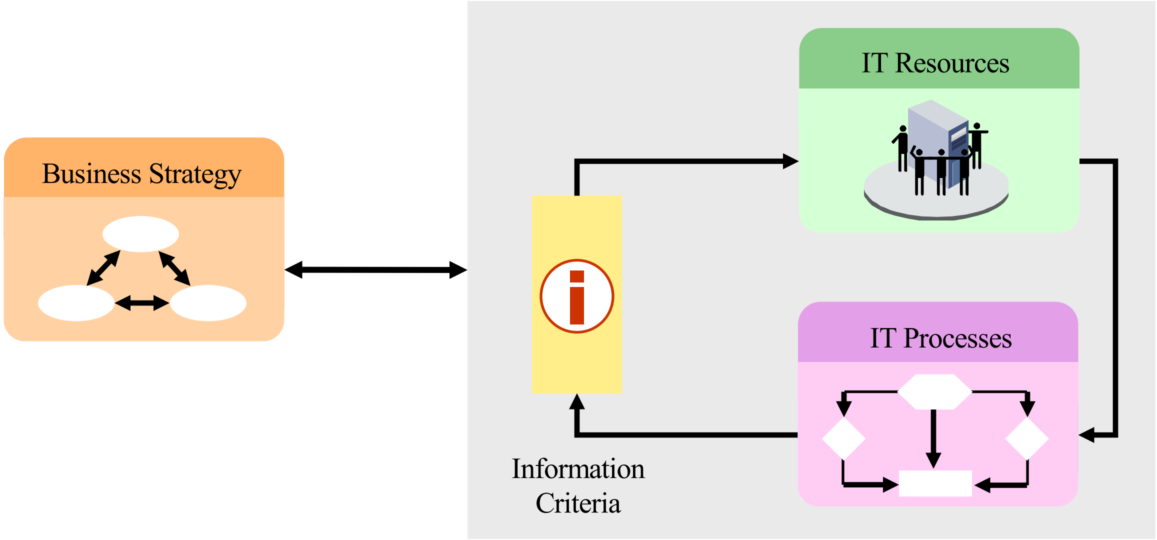


- The COBIT framework helps align IT with the business by focusing on business information requirements and organising IT resources. COBIT provides the framework and guidance to implement IT governance.

©2007 IT Governance Institute. All rights reserved.

COBIT: Principle

The principle of the COBIT framework is to link management's IT expectations with management's IT responsibilities. The objective is to facilitate IT governance to deliver IT value whilst managing IT risks.

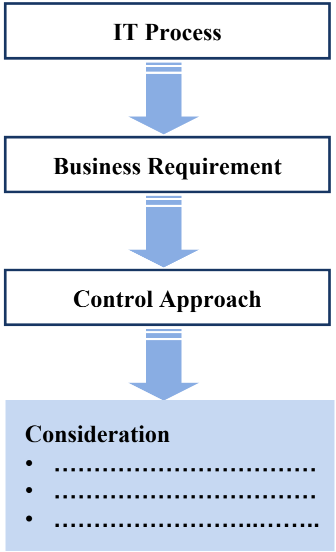


©2007 IT Governance Institute. All rights reserved.

COBIT Framework

As a control and governance framework for IT, COBIT focuses on two key areas:

- Providing the information required to support business objectives and requirements
- Treating information as the result of the combined application of IT-related resources that need to be managed by IT processes



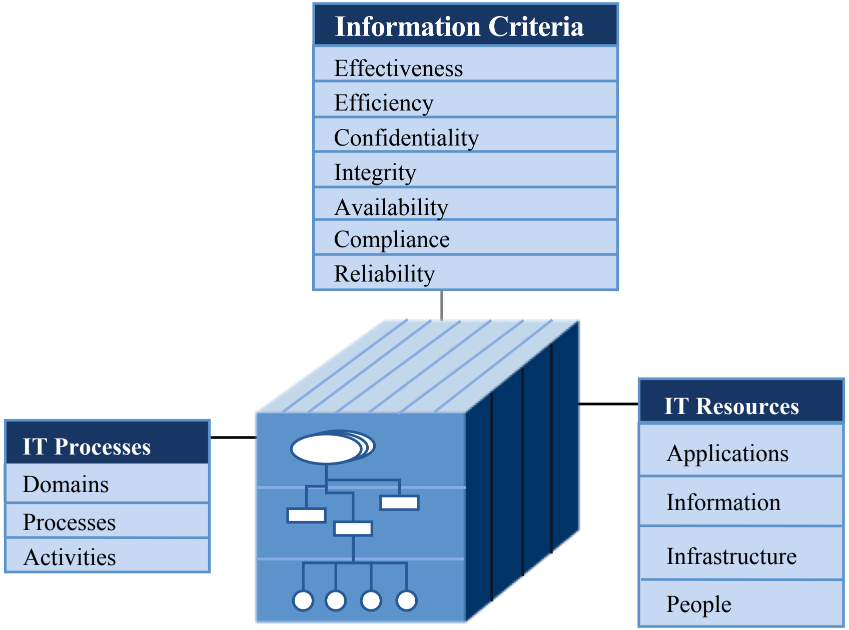
IT Process

Business Requirement

Control Approach

Consideration

- ………………………………
- ………………………………
- ………………………………



Information Criteria

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

IT Processes

- Domains
- Processes
- Activities

IT Resources

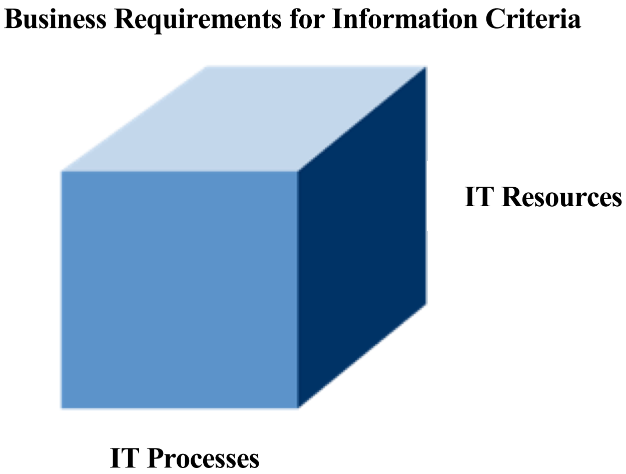
- Applications
- Information
- Infrastructure
- People

©2007 IT Governance Institute. All rights reserved.

COBIT Cube

The COBIT framework describes how IT processes deliver the information that the business needs to achieve its objectives.

For controlling this delivery, COBIT provides three key components, each forming a dimension of the COBIT cube.



Business Requirements for Information Criteria

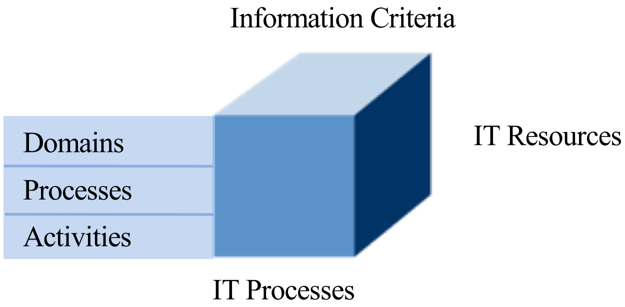
IT Resources

IT Processes

©2007 IT Governance Institute. All rights reserved.

COBIT Cube: IT Processes

- COBIT describes the IT life cycle with the help of four **domains**:
  - Plan and Organise
  - Acquire and Implement
  - Deliver and Support
  - Monitor and Evaluate
- **Processes** are series of activities with natural control breaks. There are 34 processes across the four domains. These processes specify what the business needs to achieve its objectives. The delivery of information is controlled through 34 IT processes.
- **Activities** are actions that are required to achieve measurable results. Moreover, activities have life cycles and include many discrete tasks.

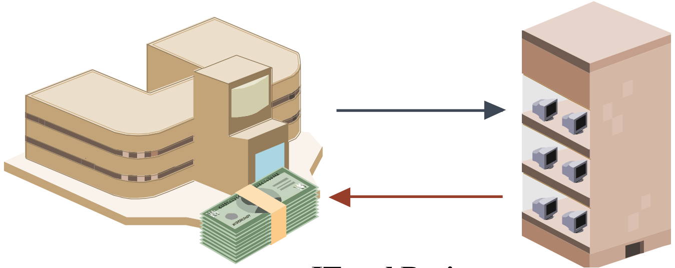


©2007 IT Governance Institute. All rights reserved.

COBIT Cube: IT Domains

Plan and Organise (PO)

- Objectives:
  - Formulating strategy and tactics
  - Identifying how IT can best contribute to achieving business objectives
  - Planning, communicating and managing the realisation of the strategic vision
  - Implementing organisational and technological infrastructure
- Scope:
  - Are IT and the business strategically aligned?
  - Is the enterprise achieving optimum use of its resources?
  - Does everyone in the organisation understand the IT objectives?
  - Are IT risks understood and being managed?
  - Is the quality of IT systems appropriate for business needs?

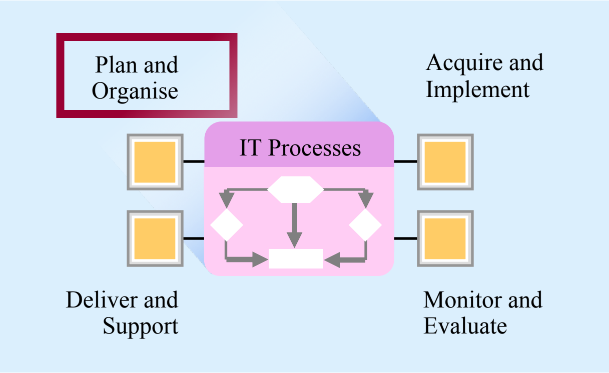


IT and Business

©2007 IT Governance Institute. All rights reserved.

COBIT Cube: IT Domains *(Cont.)*

Let's look at the COBIT process model, which consists of 34 IT processes defined within the four IT domains.



Plan and Organise

PO1 Define a strategic IT plan.

PO2 Define the information architecture.

PO3 Determine technological direction.

PO4 Define the IT processes, organisation and relationships.

PO5 Manage the IT investment.

PO6 Communicate management aims and direction.

PO7 Manage IT human resources.

PO8 Manage quality.

PO9 Assess and manage IT risks.

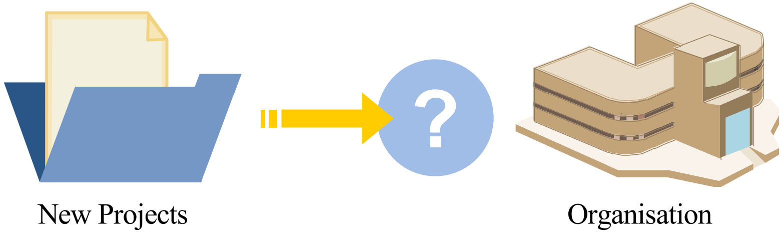
PO10 Manage projects.

©2007 IT Governance Institute. All rights reserved.

COBIT Cube: IT Domains *(Cont.)*

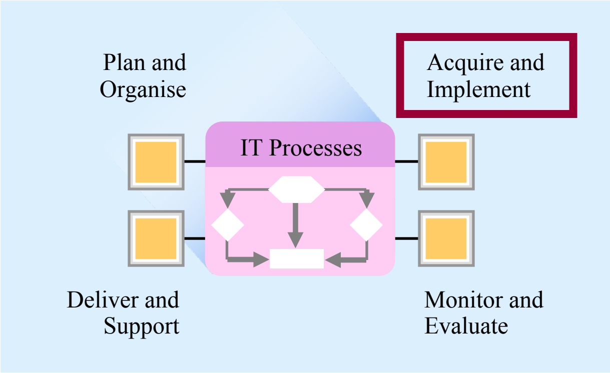
Acquire and Implement (AI)

- Objectives:
  - Identifying, developing or acquiring, implementing, and integrating IT solutions
  - Changes in and maintenance of existing systems
- Scope:
  - 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?



©2007 IT Governance Institute. All rights reserved.

COBIT Cube: IT Domains *(Cont.)*



Acquire and 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.

AI6 Manage changes.

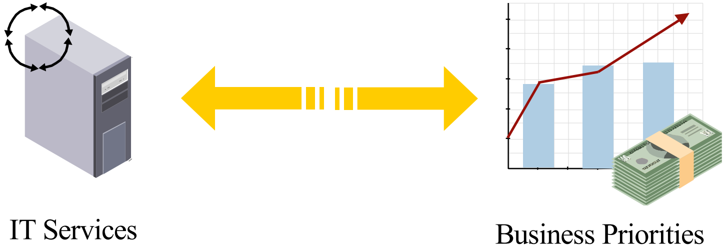
AI7 Install and accredit solutions and changes.

©2007 IT Governance Institute. All rights reserved.

CobiT Cube: IT Domains *(Cont.)*

Deliver and Support (DS)

- Objectives:
  - The actual delivery of required services, including service delivery
  - The management of security, continuity, data and operational facilities
  - Service support for users
- Scope:
  - Are IT services being delivered in line with business priorities?
  - Are IT costs optimised?
  - Is the workforce able to use IT systems productively and safely?
  - Are adequate confidentiality, integrity and availability in place?



IT Services

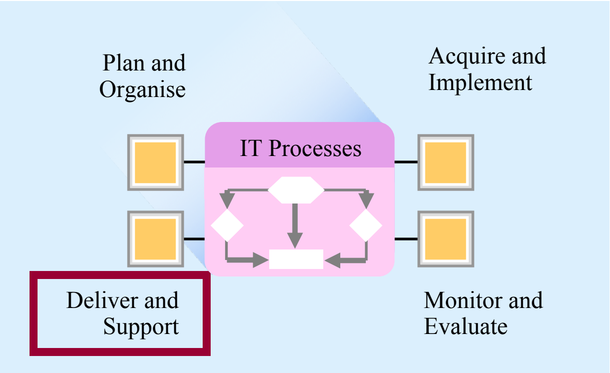
Business Priorities

©2007 IT Governance Institute. All rights reserved.

COBIT Cube: IT Domains *(Cont.)*

Deliver and 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 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

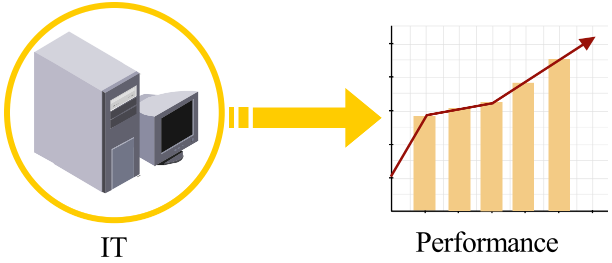


©2007 IT Governance Institute. All rights reserved.

CobiT Cube: IT Domains *(Cont.)*

Monitor and Evaluate (ME)

- Objectives:
  - Performance management
  - Monitoring of internal control
  - Regulatory compliance
  - Governance
- Scope:
  - 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 to business goals?
  - Are risk, control, compliance and performance measured and reported?



©2007 IT Governance Institute. All rights reserved.

COBIT Cube: IT Domains *(Cont.)*

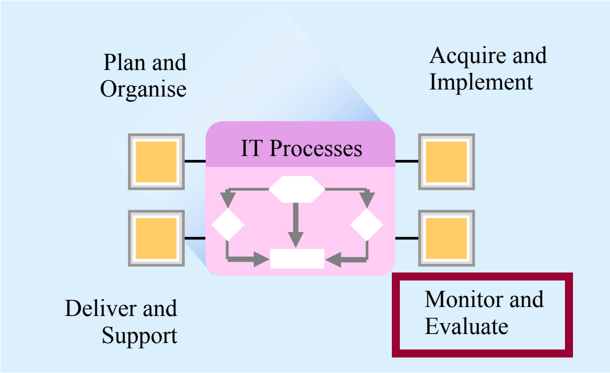
Monitor and Evaluate

ME1 Monitor and evaluate IT performance.

ME2 Monitor and evaluate internal control.

ME3 Ensure compliance with external requirements.

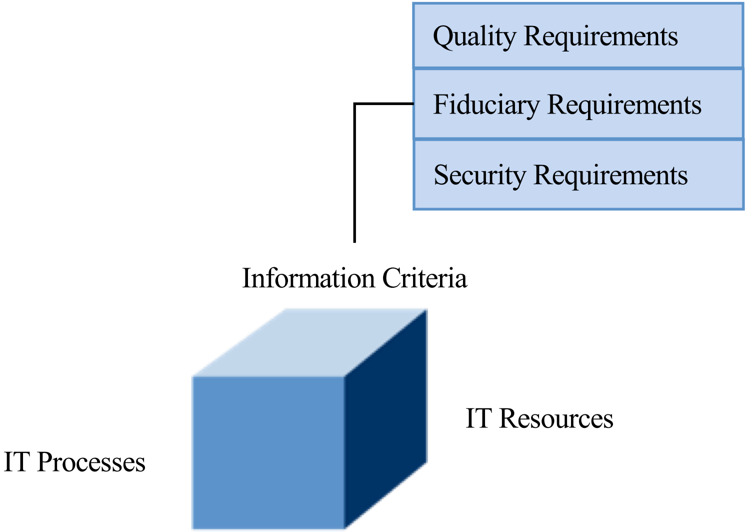
ME4 Provide IT governance.



©2007 IT Governance Institute. All rights reserved.

COBIT Cube: Information Criteria

- To satisfy business objectives, information needs to conform to specific control criteria, which COBIT refers to as business requirements for information.
- Broadly, information criteria are based on the following requirements:
  - Quality
  - Fiduciary (trust)
  - Security



©2007 IT Governance Institute. All rights reserved.

COBIT Cube: Information Criteria *(Cont.)*

Effectiveness Deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner

Efficiency Concerns the provision of information through the optimal (most productive and economical) use of resources

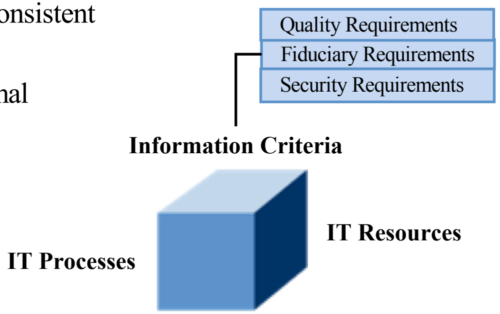
Confidentiality Concerns the protection of sensitive information from unauthorised disclosure

Integrity Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations

Availability Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Compliance Deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies

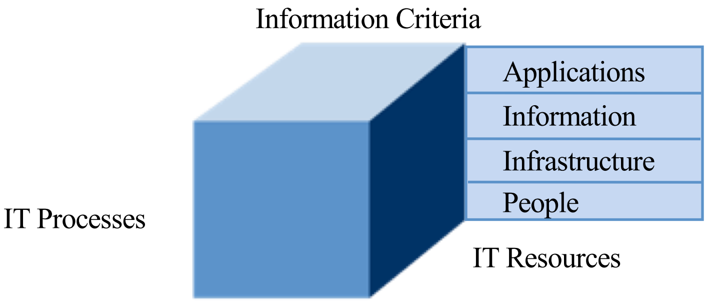
Reliability Relates to the provision of appropriate information for management to operate the entity and to exercise its fiduciary and governance responsibilities



©2007 IT Governance Institute. All rights reserved.

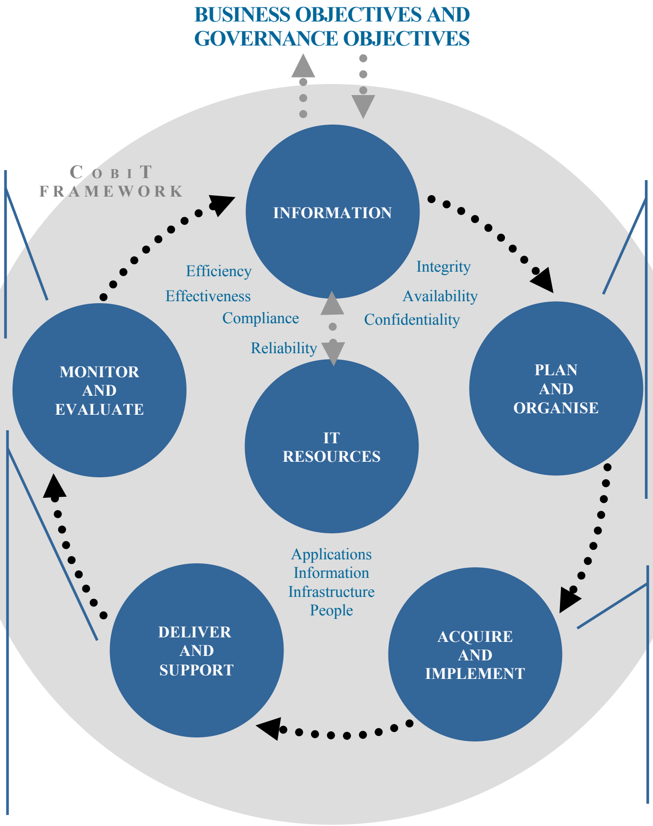
COBIT Cube: IT Resources

- IT processes manage IT resources to generate, deliver and store the information that the organisation needs to achieve its objectives.
- The IT resources identified in COBIT are defined as:
  - **Applications** are automated user systems and manual procedures that process information.
  - **Information** is data that are input, processed and output by information systems, in whatever form used by the business.
  - **Infrastructure** includes the technology and facilities, such as hardware, operating systems and networking, that enable the processing of applications.
  - **People** are the personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate information systems and services. They may be internal, outsourced or contracted, as required.



©2007 IT Governance Institute. All rights reserved.

CobiT Framework



ME1	Monitor and evaluate IT performance.
ME2	Monitor and evaluate internal control.
ME3	Ensure compliance with external requirements.
ME4	Provide IT governance.

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	Manage service desk and incidents.
DS9	Manage the configuration.
DS10	Manage problems.
DS11	Manage data.
DS12	Manage the physical environment.
DS13	Manage operations.

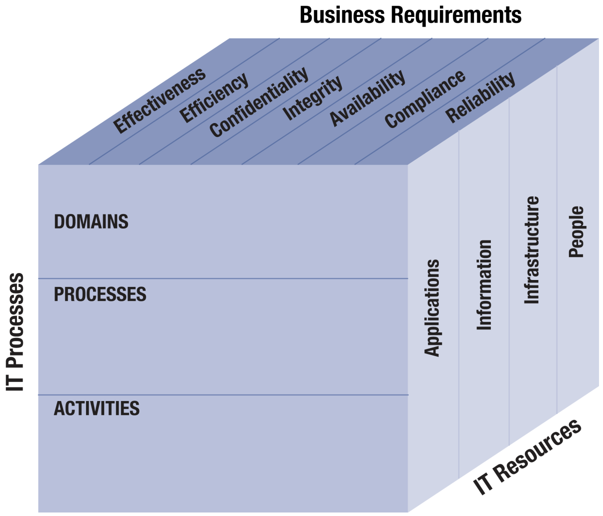
PO1	Define a strategic IT plan.
PO2	Define the information architecture.
PO3	Determine technological direction.
PO4	Define the IT processes, organisation and relationships.
PO5	Manage the IT investment.
PO6	Communicate management aims and direction.
PO7	Manage IT human resources.
PO8	Manage quality.
PO9	Assess and manage IT risks.
PO10	Manage projects.

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.
AI6	Manage changes.
AI7	Install and accredit solutions and changes.

©2007 IT Governance Institute. All rights reserved.

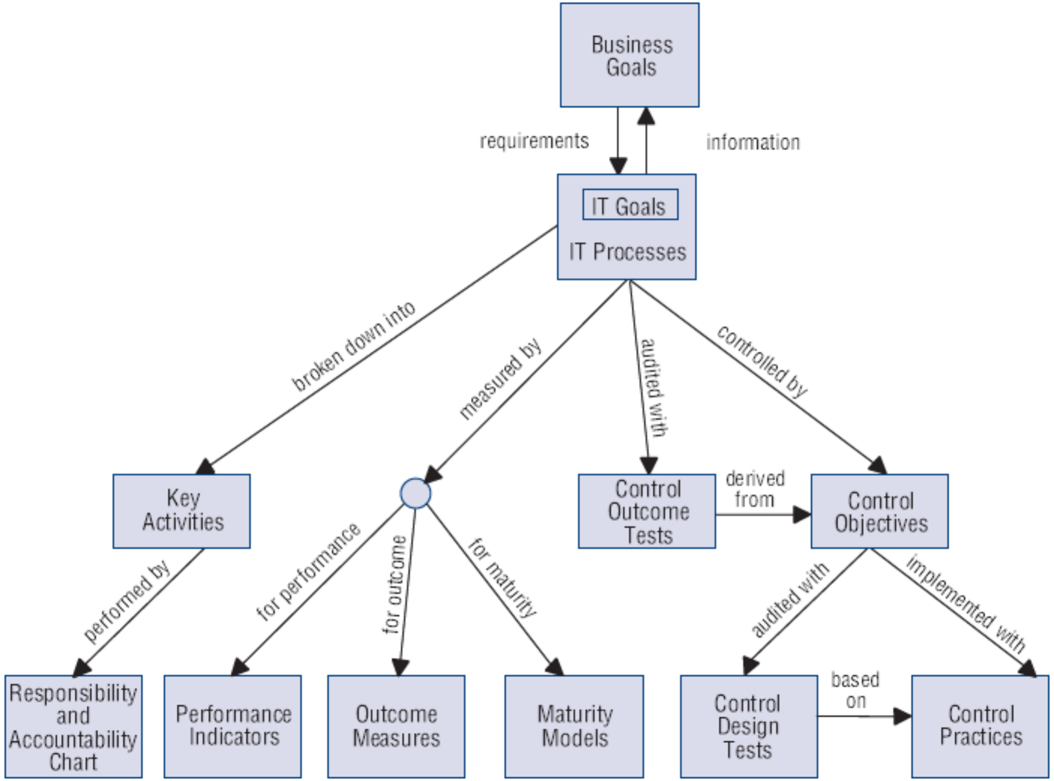
COBIT Cube

IT resources are managed by IT processes to achieve IT goals that respond to the business requirements. This is the basic principle of the COBIT framework, as illustrated by the COBIT cube.



©2007 IT Governance Institute. All rights reserved.

Interrelationship of the COBIT Components



©2007 IT Governance Institute. All rights reserved.

Reading

Brotby 12

Questions?

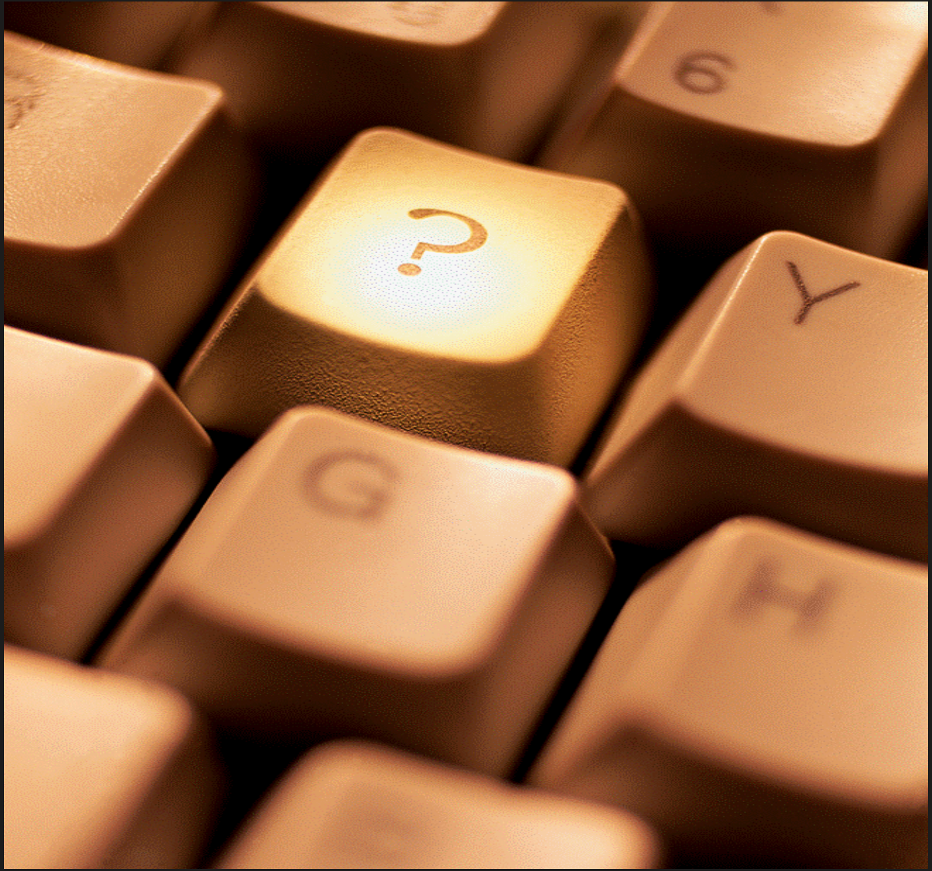
Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics

mlhale@unomaha.edu

Twitter: @mlhale_



Some material © 2013 Jones and Bartlett Learning, LLC

All else © 2014-2016 Matthew L. Hale