



C12 - COBIT Fundamentals and Uses

Miguel (Mike) O. Villegas, CISA, CISSP

2007 SF ISACA Fall Conference

San Francisco

September 17, 2007

Agenda

- ❖ Mission Statement and Objectives
- ❖ The Need for COBIT
- ❖ COBIT Principle
- ❖ IT Governance Focus Areas
- ❖ COBIT Content Diagram
- ❖ Interrelationships of COBIT Components
- ❖ COBIT Framework
- ❖ COBIT 4.1 Update
- ❖ COBIT Campus
- ❖ LA ISACA COBIT Survey
- ❖ IT Governance Certification

Mission and Objectives

Mission Statement:

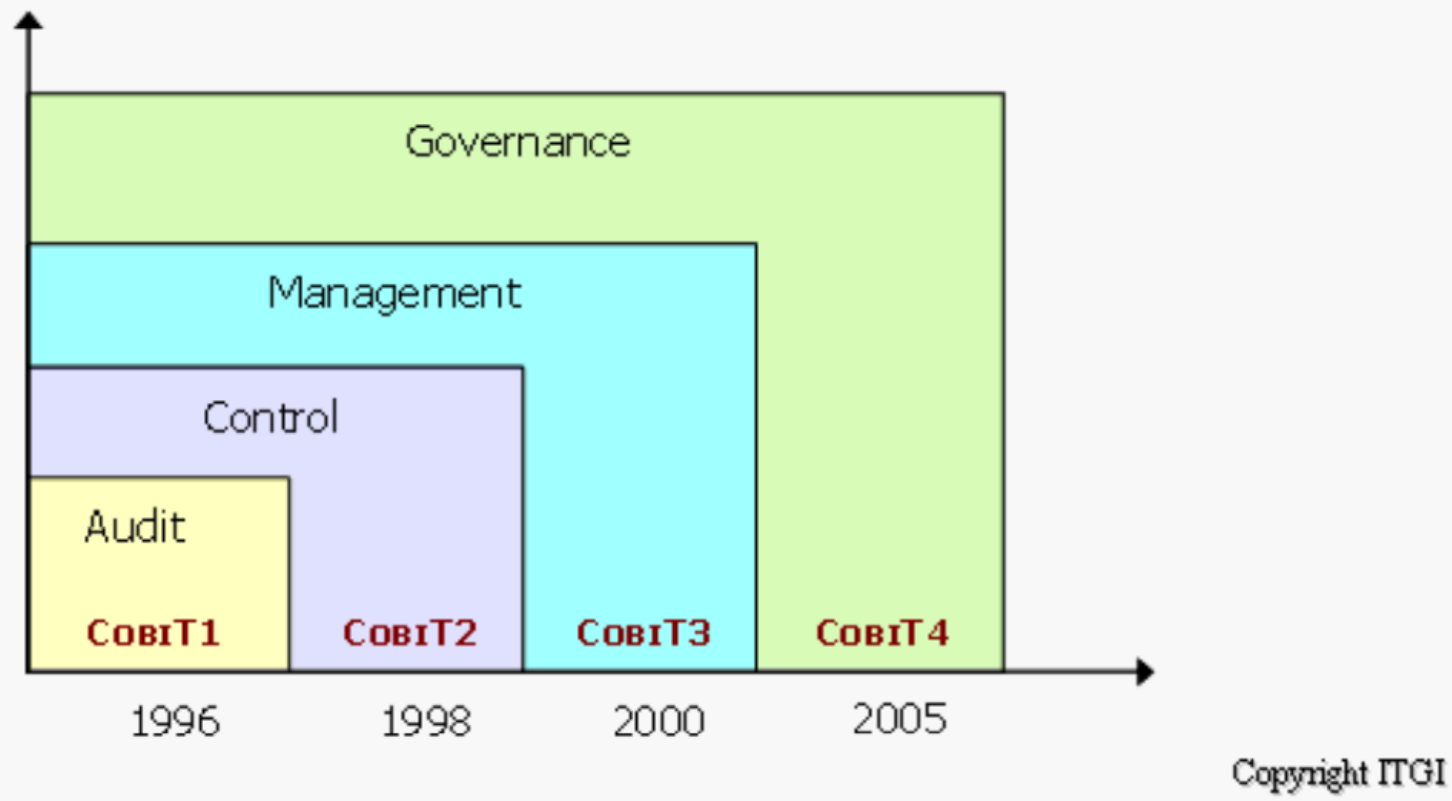
- ❖ To research, develop, publicize and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals

Objectives:

- ❖ Aligning IT strategy with the business strategy
- ❖ Assuring investors and shareholders that a 'standard of due care' around mitigating IT risks is being met by the organization
- ❖ Cascading IT strategy and goals down into the enterprise
- ❖ Obtaining value from IT investments
- ❖ Providing organizational structures that facilitate the implementation of strategy and goals
- ❖ Creating constructive relationships and effective communication between the business and IT, and with external partners
- ❖ Measuring IT's performance

History of CobiT

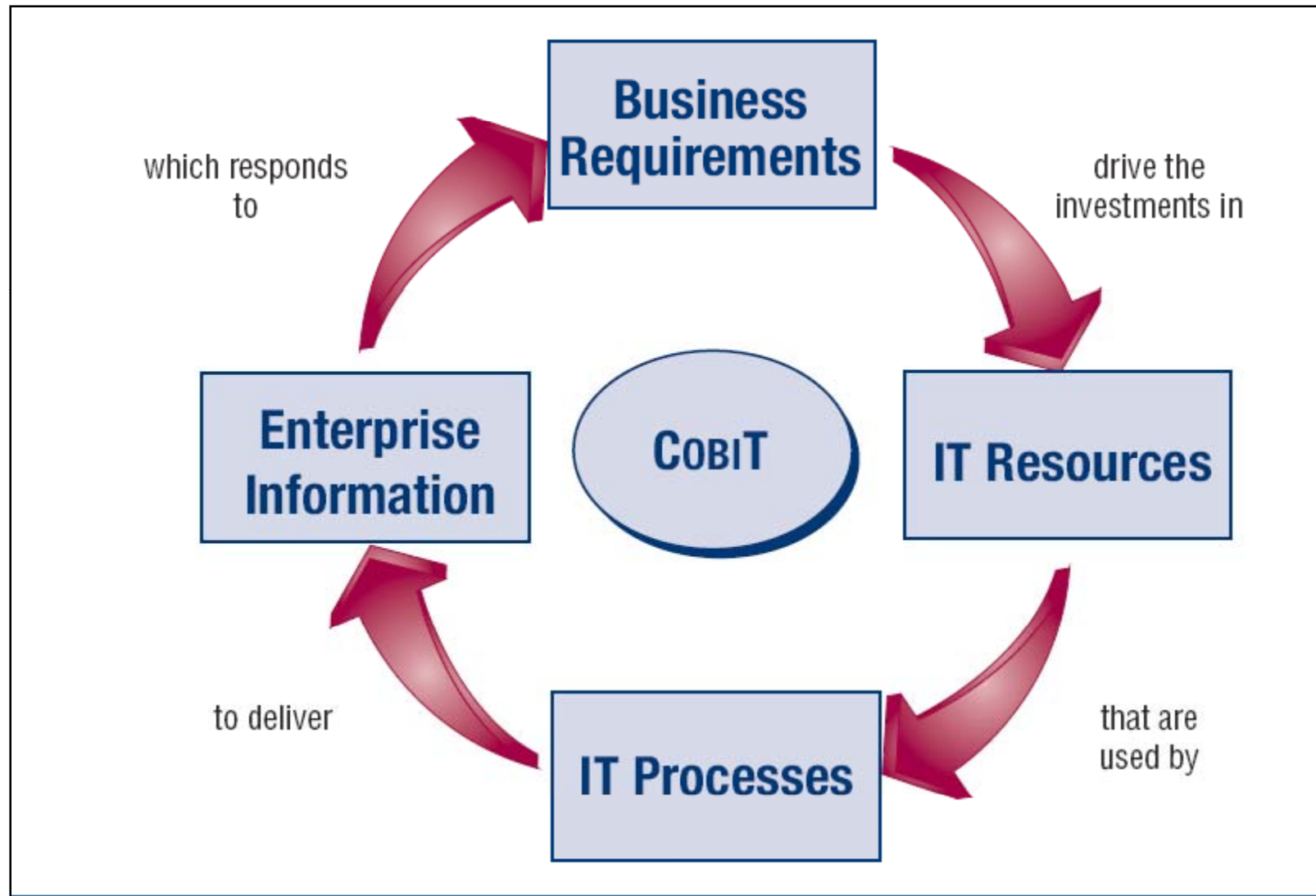
CobiT has evolved from an auditor's tool to an IT governance framework, used increasingly by IT management



The Need for COBIT

- ❖ Better return for IT investment
- ❖ Concern over generally increasing IT expenditure
- ❖ Regulatory requirements for IT controls
- ❖ Service provider and vendor management
- ❖ Increasingly complex IT-related risks
- ❖ IT governance
- ❖ IT activities that increase business value and reduce business risk
- ❖ Need to optimize costs
- ❖ Controls benchmarking
- ❖ Growing acceptance of well-regarded frameworks:
 - ❖ COBIT
 - ❖ ITIL
 - ❖ ISO 27000
 - ❖ ISO 9001:2000
 - ❖ CMMI
 - ❖ PRINCE2
 - ❖ PMBOK

COBIT Principle

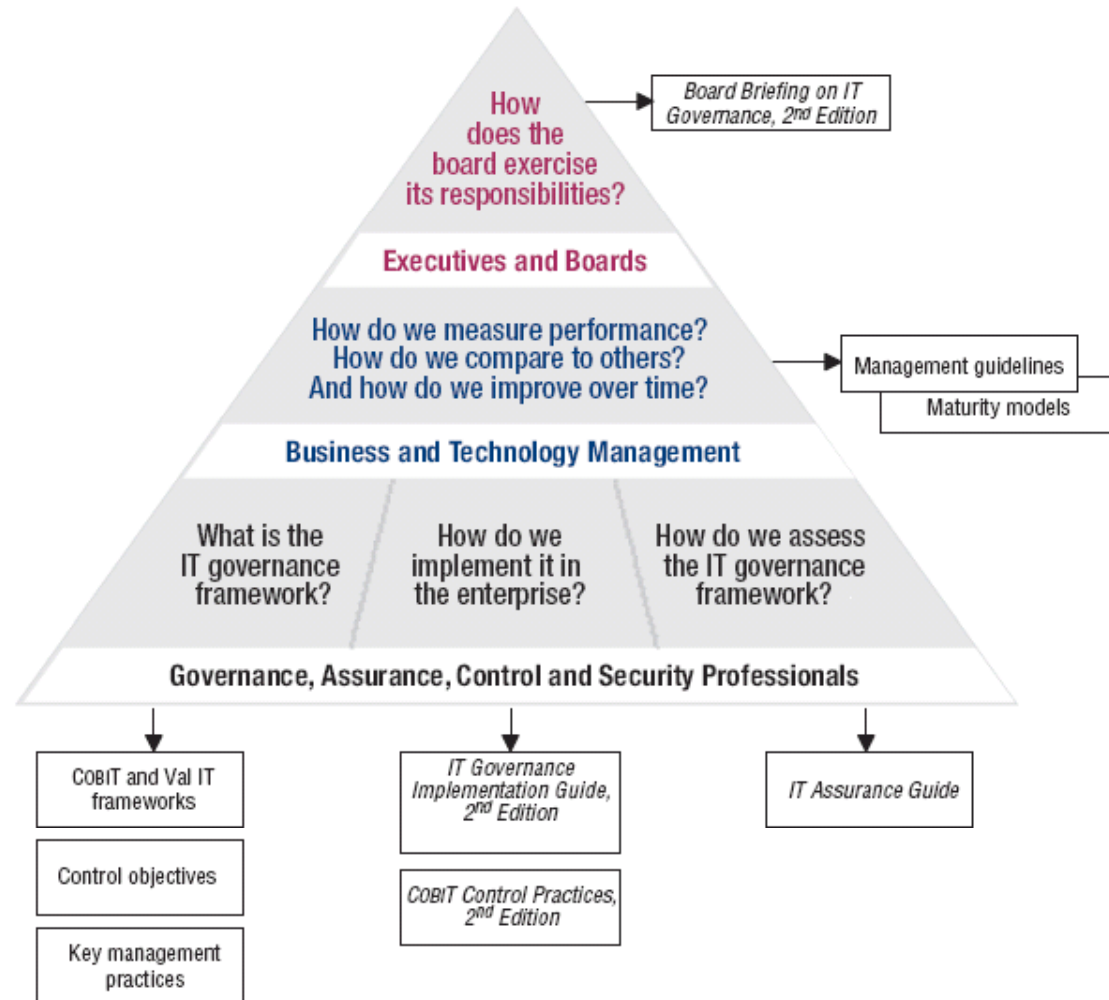


IT Governance Focus Areas



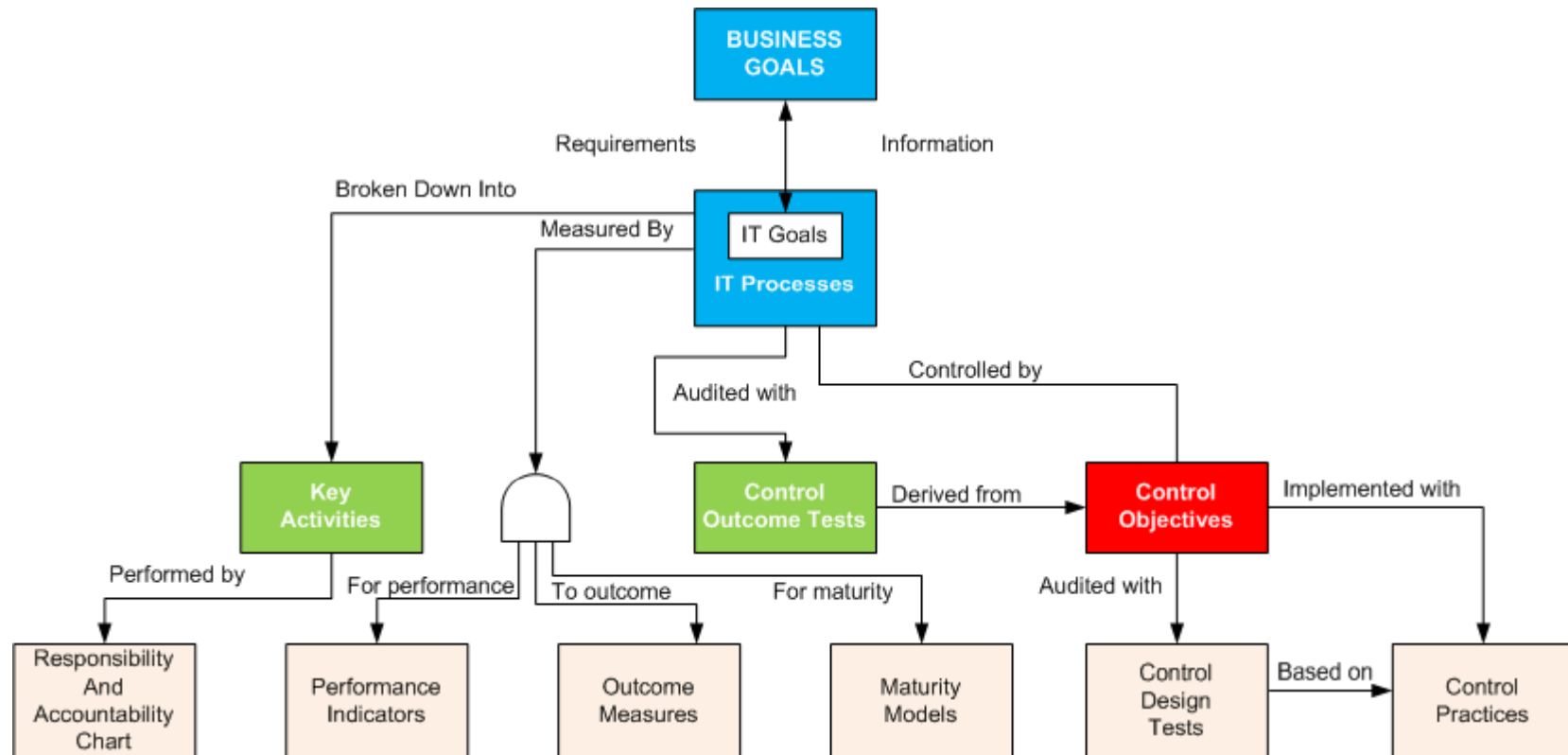
- ❖ Strategic Alignment
- ❖ Value Delivery
- ❖ Resource Management
- ❖ Risk Management
- ❖ Performance Measures

COBIT Content Diagram



This COBIT-based product diagram presents the generally applicable products and their primary audience. There are also derived products for specific purposes (*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*), for domains such as security (*COBIT Security Baseline* and *Information Security Governance: Guidance for Boards of Directors and Executive Management*), or for specific enterprises (*COBIT Quickstart* for small and medium-sized enterprises or for large enterprises wishing to ramp up to a more extensive IT governance implementation).

Interrelationships of COBIT Components

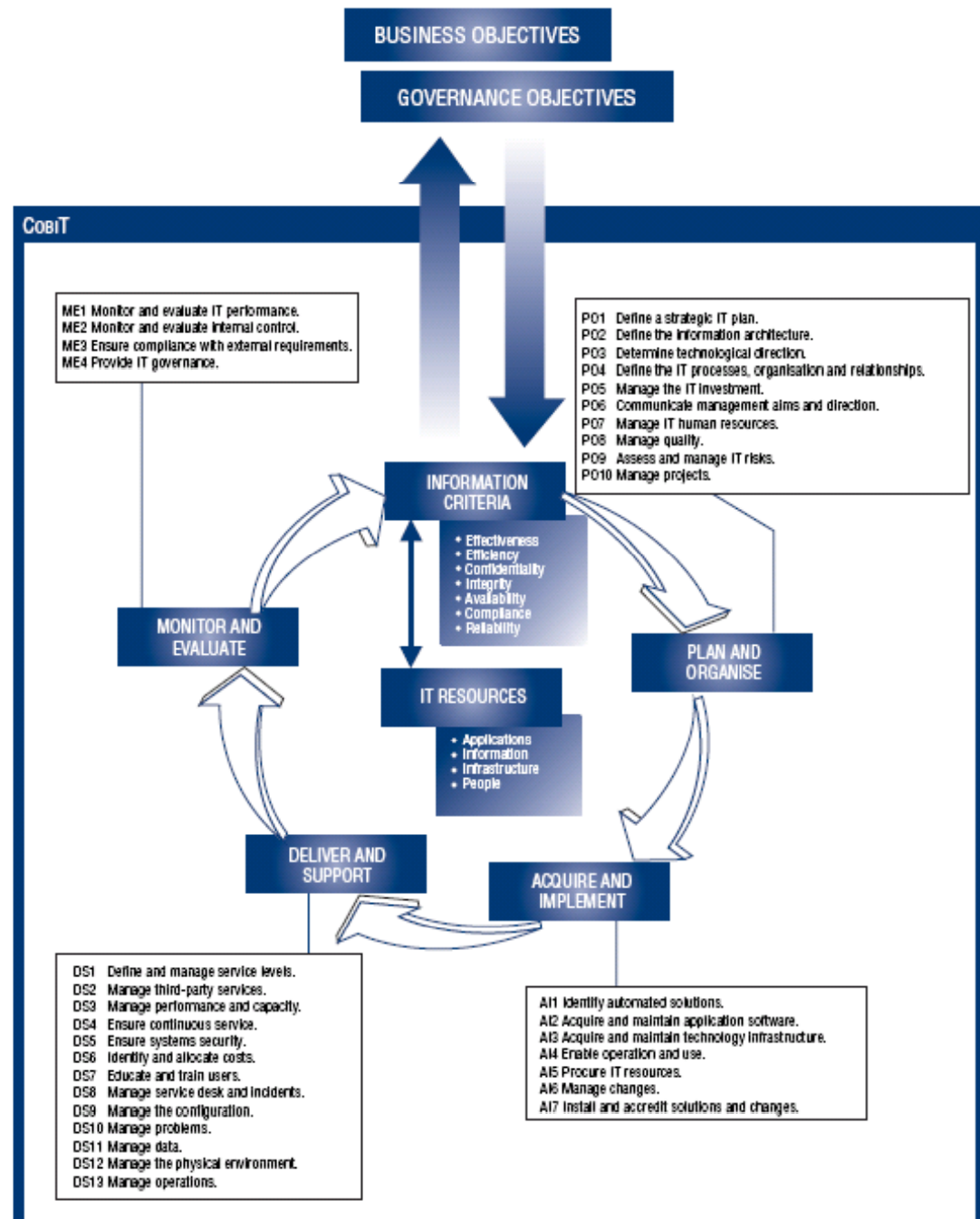


COBIT Framework

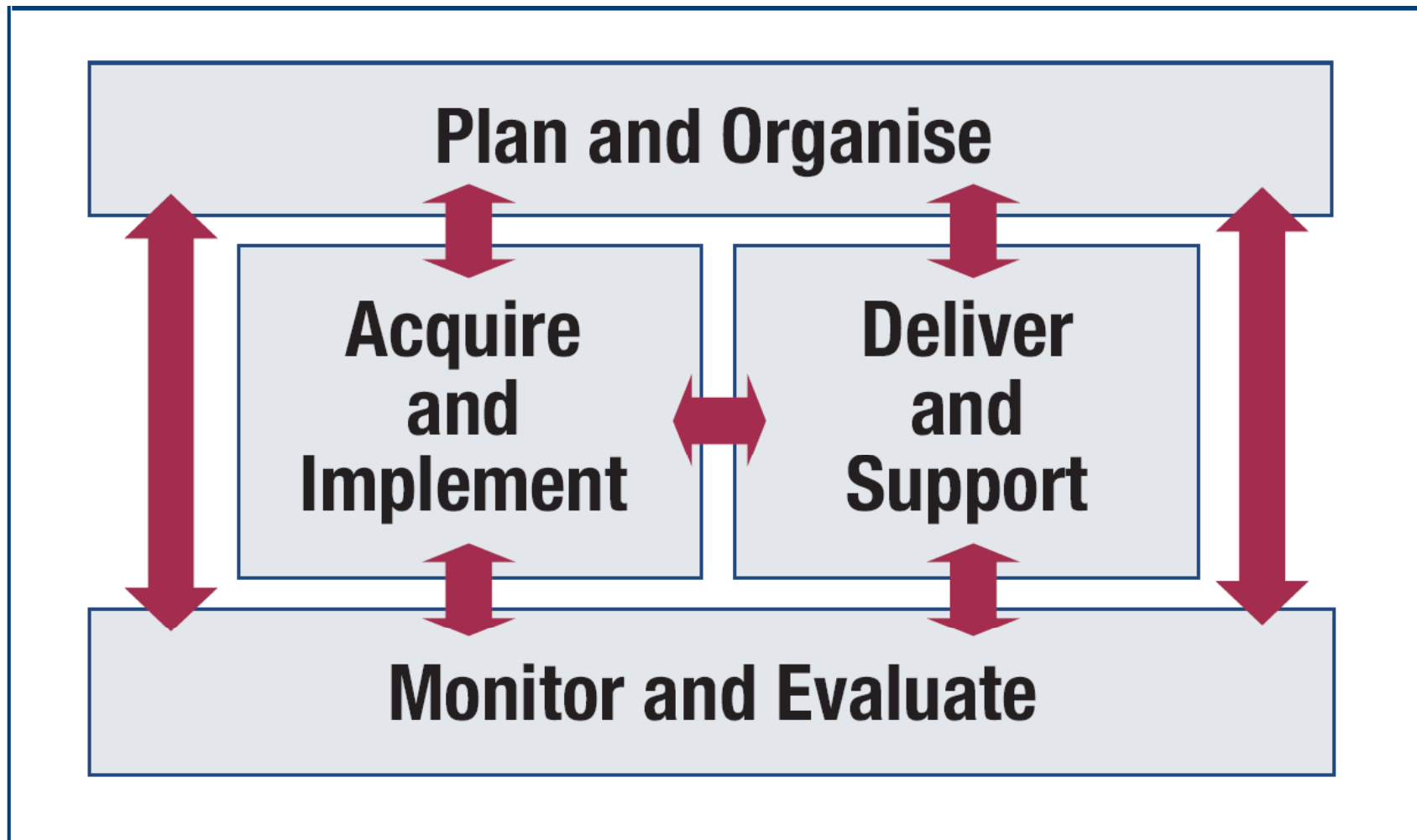
In more detail, the overall COBIT framework can be shown graphically, as depicted in this schematic. It shows the COBIT process model of four domains containing 34 generic processes, managing the IT resources to deliver information to the business according to business and governance requirements.

Four Domains:

- ❖ PO – Plan and Organize
- ❖ AI – Acquire and Implement
- ❖ DS – Deliver and Support
- ❖ ME – Monitor and Evaluate



COBIT Framework (Cont'd)



Plan and Organize

Process	Description
PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization 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

Acquire and Implement

Process	Description
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 Accredite Solutions and Changes

Deliver and Support

Process	Description
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

Monitor and Evaluate

Process	Description
ME1	Monitor and Evaluate IT Performance
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Compliance With External Requirements
ME4	Provide IT Governance

Framework, Control Objectives and Management Guidelines now one integrated book

[Home](#) [Browsing](#) [Benchmarking](#) [Community](#) [Sign Out](#)

[Browsing](#) > [Browse All Contents](#)

[Feedback](#) [Print Friendly](#) [Legend](#)

	Framework	C.O.	I/O	RACI	G&M	M.M.	C.P.	A.S.																										
Process Controls PC Process Controls 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 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 Accredite Solutions and Changes 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	DS5 Deliver and Support Ensure Systems Security							Process Importance																										
	<p>The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.</p> <p>Control over the IT Process of</p> <p>Ensure Systems Security</p> <p>that satisfies the business requirement for IT of</p> <p>maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents</p> <p>by focusing on</p> <p>defining IT security policies, plans and procedures, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents</p> <p>is achieved by</p> <ul style="list-style-type: none"> Understanding security requirements, vulnerabilities and threats Managing user identities and authorisations in a standardised manner Testing security regularly <p>and is measured by</p> <ul style="list-style-type: none"> Number of incidents damaging the organisation's reputation with the public Number of systems where security requirements are not met Number of violations in segregation of duties 	<p>Information Criteria</p> <table border="1"> <tr><td><input type="checkbox"/></td><td>Effectiveness</td></tr> <tr><td><input type="checkbox"/></td><td>Efficiency</td></tr> <tr><td><input type="checkbox"/></td><td>Confidentiality</td></tr> <tr><td><input type="checkbox"/></td><td>Integrity</td></tr> <tr><td><input type="checkbox"/></td><td>Availability</td></tr> <tr><td><input type="checkbox"/></td><td>Compliance</td></tr> <tr><td><input type="checkbox"/></td><td>Reliability</td></tr> </table> <p>Used Resources</p> <table border="1"> <tr><td><input checked="" type="checkbox"/></td><td>Applications</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Information</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>Infrastructure</td></tr> <tr><td><input checked="" type="checkbox"/></td><td>People</td></tr> </table> <p>IT Governance</p> <table border="1"> <tr><td><input type="checkbox"/></td><td>Strategic Alignment</td></tr> <tr><td><input type="checkbox"/></td><td>Value Delivery</td></tr> <tr><td><input type="checkbox"/></td><td>Risk Management</td></tr> <tr><td><input type="checkbox"/></td><td>Resource Management</td></tr> <tr><td><input type="checkbox"/></td><td>Performance Measurement</td></tr> </table>	<input type="checkbox"/>	Effectiveness	<input type="checkbox"/>	Efficiency	<input type="checkbox"/>	Confidentiality	<input type="checkbox"/>	Integrity	<input type="checkbox"/>	Availability	<input type="checkbox"/>	Compliance	<input type="checkbox"/>	Reliability	<input checked="" type="checkbox"/>	Applications	<input checked="" type="checkbox"/>	Information	<input checked="" type="checkbox"/>	Infrastructure	<input checked="" type="checkbox"/>	People	<input type="checkbox"/>	Strategic Alignment	<input type="checkbox"/>	Value Delivery	<input type="checkbox"/>	Risk Management	<input type="checkbox"/>	Resource Management	<input type="checkbox"/>	Performance Measurement
<input type="checkbox"/>	Effectiveness																																	
<input type="checkbox"/>	Efficiency																																	
<input type="checkbox"/>	Confidentiality																																	
<input type="checkbox"/>	Integrity																																	
<input type="checkbox"/>	Availability																																	
<input type="checkbox"/>	Compliance																																	
<input type="checkbox"/>	Reliability																																	
<input checked="" type="checkbox"/>	Applications																																	
<input checked="" type="checkbox"/>	Information																																	
<input checked="" type="checkbox"/>	Infrastructure																																	
<input checked="" type="checkbox"/>	People																																	
<input type="checkbox"/>	Strategic Alignment																																	
<input type="checkbox"/>	Value Delivery																																	
<input type="checkbox"/>	Risk Management																																	
<input type="checkbox"/>	Resource Management																																	
<input type="checkbox"/>	Performance Measurement																																	

[Feedback](#) [Print Friendly](#) [Legend](#)

Deliver and Support

Process	Description
DS5.1	Management of IT Security
DS5.2	IT Security Plan
DS5.3	Identity Management
DS5.4	User Account Management
DS5.5	Security Testing, Surveillance and Monitoring
DS5.6	Security Incident Definition
DS5.7	Protection of Security Technology
DS5.8	Cryptographic Key Management
DS5.9	Malicious Software Prevention, Detection and Correction
DS5.10	Network Security
DS5.11	Exchange of Sensitive Data

Control Objectives

[Home](#) [Browsing](#) [Benchmarking](#) [Community](#) [Sign Out](#)

[Feedback](#) [Print Friendly](#) [Legend](#)

Browsing ▶ [Browse All Contents](#)

F.W.	Control Objectives	I/O	RACI	G&M	M.M.	C.P.	A.S.
Process Controls							
PC	Process Controls						
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						
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 Accredited Solutions and Changes						
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						

DS5 Deliver and Support
Ensure Systems Security

Process Importance **H**

5.1 Management of IT Security

Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.

Effectiveness: **H**
 Expedience: **M**
 Sustainability: **M**

→

Contribution: **H**
 Effort: **VH**

5.2 IT Security Plan

Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.

Effectiveness: **M**
 Expedience: **M**
 Sustainability: **M**

→

Contribution: **L**
 Effort: **L**

5.3 Identity Management

Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

Effectiveness: **H**
 Expedience: **L**
 Sustainability: **H**

→

Contribution: **H**
 Effort: **VH**

Inputs and Outputs

[Home](#) [Browsing](#) [Benchmarking](#) [Community](#) [Sign Out](#)

Feedback
 Print Friendly
 Legend

[Browsing](#) > [Browse All Contents](#)

F.W.	C.O.	Inputs and Outputs	RACI	G&M	M.M.	C.P.	A.S.																																				
<div> DS5 Deliver and Support Ensure Systems Security Process Importance </div> <div> <table border="1"> <thead> <tr> <th>from</th> <th>INPUTS</th> </tr> </thead> <tbody> <tr><td>PO2</td><td>Assigned data classifications</td></tr> <tr><td>PO2</td><td>Information architecture</td></tr> <tr><td>PO3</td><td>Technology standards</td></tr> <tr><td>PO4</td><td>IT process framework, documented roles and ALL responsibilities</td></tr> <tr><td>PO6</td><td>IT policies</td></tr> <tr><td>PO6</td><td>Enterprise IT control framework</td></tr> <tr><td>PO7</td><td>Roles and responsibilities</td></tr> <tr><td>PO8</td><td>Quality standards and metrics requirements</td></tr> <tr><td>PO9</td><td>Risk assessment</td></tr> <tr><td>AI2</td><td>Application security controls specification</td></tr> <tr><td>DS1</td><td>OLAs</td></tr> </tbody> </table> <table border="1"> <thead> <tr> <th>OUTPUTS</th> <th>to</th> </tr> </thead> <tbody> <tr><td>Security incident definition</td><td>DS8 </td></tr> <tr><td>Specific training requirements on security awareness</td><td>DS7 </td></tr> <tr><td>Process performance reports</td><td>ME1 </td></tr> <tr><td>Required security changes</td><td>AI6 </td></tr> <tr><td>Security threats and vulnerabilities</td><td>DS11 </td></tr> </tbody> </table> </div>								from	INPUTS	PO2	Assigned data classifications	PO2	Information architecture	PO3	Technology standards	PO4	IT process framework, documented roles and ALL responsibilities	PO6	IT policies	PO6	Enterprise IT control framework	PO7	Roles and responsibilities	PO8	Quality standards and metrics requirements	PO9	Risk assessment	AI2	Application security controls specification	DS1	OLAs	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	DS11
from	INPUTS																																										
PO2	Assigned data classifications																																										
PO2	Information architecture																																										
PO3	Technology standards																																										
PO4	IT process framework, documented roles and ALL responsibilities																																										
PO6	IT policies																																										
PO6	Enterprise IT control framework																																										
PO7	Roles and responsibilities																																										
PO8	Quality standards and metrics requirements																																										
PO9	Risk assessment																																										
AI2	Application security controls specification																																										
DS1	OLAs																																										
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	DS11																																										

Feedback
 Print Friendly
 Legend

Process Controls
 PC Process Controls
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
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 Accredited Solutions and Changes
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

Added RACI chart (Responsible, Accountable, Consulted, Informed)

[Home](#) [Browsing](#) [Benchmarking](#) [Community](#) [Sign Out](#)

Feedback
 Print Friendly*
 Legend

[Browsing](#) > [Browse All Contents](#)

F.W.	C.O.	I/O	RACI Chart	G&M	M.M.	C.P.	A.S.
------	------	-----	-------------------	-----	------	------	------

Process Controls
 PC Process Controls
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
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 Accredited Solutions and Changes
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

DS5 Deliver and Support
Ensure Systems Security

Process Importance

Float mouse over function to see truncated text

Activities	Business Functions										
	Chief executive...	Chief financial...	Business Execut...	Chief informati...	Business Proces...	Head Operations	Chief Architect	Head Developmen...	Head IT Adminis...	The project man...	Compliance, Aud...
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.				A	I	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 **R**esponsible, **A**ccountable, **C**onsulted, and/or **I**nformed

Feedback
 Print Friendly*
 Legend

* Consider changing the page setup to landscape (in your browser) when printing this page.

Goals and Metrics

[Home](#) [Browsing](#) [Benchmarking](#) [Community](#) [Sign Out](#)

[Feedback](#) [Print Friendly*](#) [Legend](#)

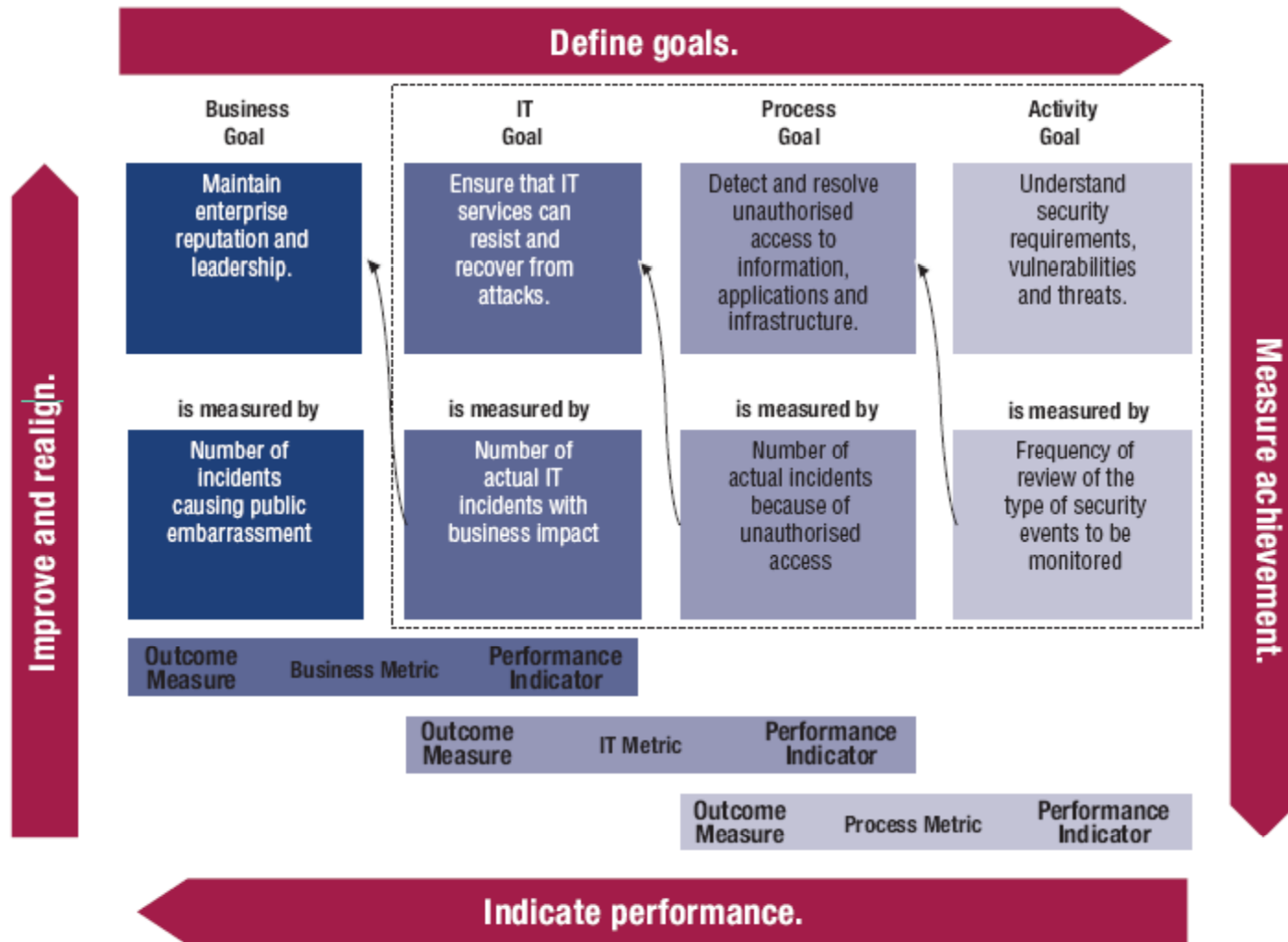
[Browsing](#) > [Browse All Contents](#)

	F.W.	C.O.	I/O	RACI	Goals & Metrics	M.M.	C.P.	A.S.
Process Controls PC Process Controls 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 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 Accredite Solutions and Changes 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					DS5 Deliver and Support Ensure Systems Security			

Process Importance

	IT	PROCESS	ACTIVITY
Goals	<ul style="list-style-type: none"> Ensure that critical and confidential information is withheld from those who should not have access to it. Ensure that automated business transactions and information exchanges can be trusted. Maintain the integrity of information and processing infrastructure. Account for and protect all IT assets. Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster. 	<ul style="list-style-type: none"> Permit access to critical and sensitive data only to authorised users. Identify, monitor and report security vulnerabilities and incidents. Detect and resolve unauthorised access to information, applications and infrastructure. Minimise the impact of security vulnerabilities and incidents. 	<ul style="list-style-type: none"> Understanding security requirements, vulnerabilities and threats Managing user identities and authorisations in a standardised manner Defining security incidents Testing security regularly
	Set	Set	
	Measure	Measure	Measure
	Drive	Drive	
Metrics	<ul style="list-style-type: none"> Number of incidents with business impact Number of systems where security requirements are not met Time to grant, change and remove access privileges 	<ul style="list-style-type: none"> Number and type of suspected and actual access violations Number of violations in segregation of duties Percent of users who do not comply with password standards Number and type of malicious code prevented 	<ul style="list-style-type: none"> Frequency and review of the type of security events to be monitored Number and type of obsolete accounts Number of unauthorised IP addresses, ports and traffic types denied Percent of cryptographic keys compromised and revoked Number of access rights authorised, revoked, reset or changed

Relationship Between Processes, Goals and Metrics (DS5)



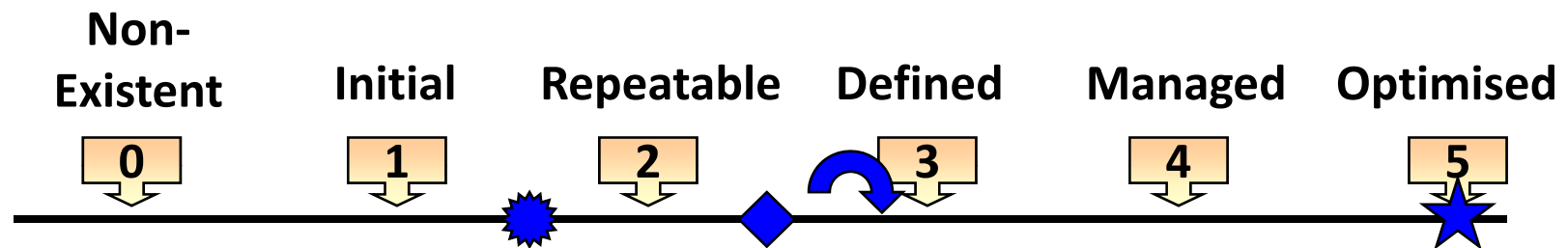
Maturity Model

[Home](#)
[Browsing](#)
[Benchmarking](#)
[Community](#)
[Sign Out](#)





[Browsing](#) > [Browse All Contents](#)

	F.W.	C.O.	I/O	RACI	G&M	Maturity Models	C.P.	A.S.
Process Controls PC Process Controls 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 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 Accredited Solutions and Changes 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	<div> <div> DS5 </div> <div> Deliver and Support Ensure Systems Security </div> <div> Process Importance </div> </div> <p>Management of the process of <i>Ensure Systems Security</i> that satisfies the business requirements for IT of <i>maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents</i> is</p> <p>0 Non-existent when The organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognisable system security administration process.</p> <p>1 Initial/Ad Hoc when The organisation recognises the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.</p> <p>2 Repeatable but Intuitive when Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analysed. Services from third parties may not address the specific security needs of the organisation. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT and the business does not see IT security as within its domain.</p> <p>3 Defined when Security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. Ad hoc security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business, but is only informally scheduled and managed.</p> <p>4 Managed and Measurable when Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and procedures are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorisation are standardised. Security certification is pursued for staff members who are responsible for the audit and management of security. Security testing is completed using standard and formalised processes, leading to improvements of security levels. IT security processes are co-ordinated with an overall organisation security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT. IT security training is planned and managed in a manner that responds to business needs and defined security risk profiles. Goals and metrics for security management have been defined but are not yet measured.</p> <p>5 Optimised when IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of the implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analysed. Adequate controls to mitigate risks are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and</p>							

Maturity Model



Legend for symbols used

-  Enterprise current status
-  International standard guidelines
-  Industry best practice
-  Enterprise strategy

Legend for rankings used

- 0 - Management processes are not applied at all
- 1 - Processes are ad hoc and disorganised
- 2 - Processes follow a regular pattern
- 3 - Processes are documented and communicated
- 4 - Processes are monitored and measured
- 5 - Best practices are followed and automated

Control Practices

[Home](#)
[Browsing](#)
[Benchmarking](#)
[Community](#)
[Sign Out](#)

[Browsing](#) > [Browse All Contents](#)

Feedback
 Print Friendly*
 Legend

	F.W.	C.O.	I/O	RACI	G&M	M.M.	Control Practices	A.S.
Process Controls PC Process Controls 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 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 Accredited Solutions and Changes 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	<div> DS5 Deliver and Support Ensure Systems Security Process Importance </div> <div> <div>5.1 Management of IT Security</div> <div>5.2 IT Security Plan</div> <div>5.3 Identity Management</div> <div>5.4 User Account Management</div> <div>5.5 Security Testing, Surveillance and Monitoring</div> <div>5.6 Security Incident Definition</div> <div>5.7 Protection of Security Technology</div> <div>5.8 Cryptographic Key Management</div> <div>5.9 Malicious Software Prevention, Detection and Correction</div> <div>5.10 Network Security</div> <div>5.11 Exchange of Sensitive Data</div> </div> <div> Feedback Print Friendly* Legend </div>							

* Consider changing the page setup to landscape (in your browser) when printing this page.

Control Practices – DS5.1

[Home](#)
[Browsing](#)
[Benchmarking](#)
[Community](#)
[Sign Out](#)

Feedback
 Print Friendly*
 Legend

[Browsing](#) > [Browse All Contents](#)

F.W.	C.O.	I/O	RACI	G&M	M.M.	Control Practices	A.S.
						DS5 Deliver and Support Ensure Systems Security	Process Importance
5.1 Management of IT Security							
Control Objective Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.		Value Drivers <ul style="list-style-type: none"> • Critical IT assets protected • IT security strategy supporting business needs • IT security strategy aligned with the overall business plan • Appropriately implemented and maintained security practices consistent with applicable laws and regulations 		Risk Drivers <ul style="list-style-type: none"> • Lack of IT security governance • Misaligned IT and business objectives • Unprotected data and information assets 			
Control Practices <ol style="list-style-type: none"> 1. Define a charter for IT security, defining for the security management function: <ul style="list-style-type: none"> • Scope and objectives for the security management function • Responsibilities • Drivers (e.g., compliance, risk, performance) 2. Confirm that the board, executive management and line management direct the policy development process to ensure that the IT security policy reflects the requirements of the business. 3. Set up an adequate organisational structure and reporting line for information security, ensuring that the security management and administration functions have sufficient authority. Define the interaction with enterprise functions, particularly the control functions such as risk management, compliance and audit. 4. Implement an IT security management reporting mechanism, regularly informing the board and business and IT management of the status of IT security so that appropriate management actions can be taken. 							
Generic Control Practices <ol style="list-style-type: none"> 1. Approach Design the control approach for achieving this control objective and define and maintain the set of control practices that implement this design. 2. Accountability and responsibility Define and assign accountability and responsibility for the control objective as a whole, and responsibility for the different control practices (see RACI chart). Make sure personnel have the right skills and necessary resources to execute these responsibilities. 3. Communication and understanding Ensure that the manner in which the control practices implement the control objective is communicated and understood. 							
5.2 IT Security Plan							
5.3 Identify Management							

Process Controls

PC	Process Controls
----	------------------

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

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 Accredited Solutions and Changes

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

Control Practices 5.7

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
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 Accredited Solutions and Changes
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
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
Application Controls	
AC	Application Controls

5.3 Identity Management

5.4 User Account Management

5.5 Security Testing, Surveillance and Monitoring

5.6 Security Incident Definition

5.7 Protection of Security Technology

Control Objective

Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.

Value Drivers

- Corporate security technology protected
- Reliable information secured
- Corporate assets protected

Risk Drivers

- Exposure of information
- Breach of trust with other organisations
- Violations of legal and regulatory requirements

Control Practices

1. Ensure that all hardware, software and facilities related to the security function and controls, e.g., security tokens and encryptors, are tamperproof.
2. Secure security documentation and specifications to prevent unauthorised access. However, do not make security of systems reliant solely on secrecy of security specifications.
3. Make the security design of dedicated security technology (e.g., encryption algorithms) strong enough to resist exposure, even if the security design is made available to unauthorised individuals.
4. Evaluate the protection mechanisms on a regular basis (at least annually) and perform updates to the protection of the security technology, if necessary.

Generic Control Practices

1. Approach

Design the control approach for achieving this control objective and define and maintain the set of control practices that implement this design.

2. Accountability and responsibility

Define and assign accountability and responsibility for the control objective as a whole, and responsibility for the different control practices (see RACI chart). Make sure personnel have the right skills and necessary resources to execute these responsibilities.

3. Communication and understanding

Ensure that the manner in which the control practices implement the control objective is communicated and understood.

5.8 Cryptographic Key Management

5.9 Malicious Software Prevention, Detection and Correction

5.10 Network Security

5.11 Exchange of Sensitive Data

Assurance Steps

[Home](#)
[Browsing](#)
[Benchmarking](#)
[Community](#)
[Sign Out](#)

[Browsing](#) > [Browse All Contents](#)

[Feedback](#)
[Print Friendly*](#)
[Legend](#)

	F.W.	C.O.	I/O	RACI	G&M	M.M.	C.P.	Assurance Steps
Process Controls PC Process Controls 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 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 Accredite Solutions and Changes 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	<div> DS5 Deliver and Support Ensure Systems Security </div> <div> Process Importance </div> <div> Testing The Control Design <ul style="list-style-type: none"> 5.1 Management of IT Security 5.2 IT Security Plan 5.3 Identity Management 5.4 User Account Management 5.5 Security Testing, Surveillance and Monitoring 5.6 Security Incident Definition 5.7 Protection of Security Technology 5.8 Cryptographic Key Management 5.9 Malicious Software Prevention, Detection and Correction 5.10 Network Security 5.11 Exchange of Sensitive Data Testing the Outcome of the Control Objective Documenting the Impact of Control Weaknesses </div>							

[Feedback](#)
[Print Friendly*](#)
[Legend](#)

Testing the Outcome of Control Objective

[Home](#) [Browsing](#) [Benchmarking](#) [Community](#) [Sign Out](#)

[Browsing](#) > [Browse All Contents](#)

[Feedback](#) [Print Friendly*](#) [Legend](#)

	F.W.	C.O.	I/O	RACI	G&M	M.M.	C.P.	Assurance Steps
Process Controls PC Process Controls 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 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 Accredited Solutions and Changes 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								

DS5 Deliver and Support
Ensure Systems Security

Process Importance

Testing The Control Design

Testing the Outcome of the Control Objective

- Through inquiry and observation, determine if the security management function effectively interacts with key enterprise functions, including areas such as risk management, compliance and audit.
- Review the process for identifying and responding to security incidents, selecting a sample of recorded incidents. Through inquiry and review of supporting documentation, determine whether appropriate management action has been taken to resolve the incident.
- Select a sample of employees and determine if computer usage and confidentiality (non-disclosure) agreements have been signed as part of their initial terms and conditions of employment.
- Review the IT security strategy, plans, policies and procedures to determine their relevance to the organisation's current IT landscape, and determine when they were last reviewed and updated.
- Review the IT security strategy, plans, policies and procedures, and verify that they reflect the data classification.
- Interview stakeholders and users on their knowledge of the IT security strategy, plans, policies and procedures, and determine if stakeholders and users find them to be relevant to risks and organisational practices.
- Ask executive management about any recent or planned changes to the organisation (e.g., business unit acquisitions/dispositions, new systems, changes in regulatory environment), and determine if the IT security plan is properly aligned.
- Determine if security processes have been implemented to uniquely identify and control the actions of all users and processes through review of system (development, test and production systems) and application accounts, job queues and services, and security software mode settings.
- Through a sample of access control lists (ACLs), determine whether the security provisioning process appropriately considers the following:
 - Sensitivity of the information and applications involved (data classification)
 - Policies for information protection and dissemination (legal, regulatory and contractual requirements)
 - The 'need-to-have' of the function
 - Standard user access profiles for common job roles in the organisation
 - The need for segregation for the access rights involved
 - Data owner and management's authorisation for access
 - The documentation of identity and access rights in a central repository
 - Creation, communication and change of initial passwords
- Through inquiry and review of sampled ACLs, determine if a process exists for resolving access provisioning requests that are not commensurate with established security authentication practices and roles.
- Determine if a risk assessment process was utilised to identify possible segregation of duties and if an escalation process was utilised to obtain added levels of management authorisation.
- Determine if authentication and authorisation mechanisms exist to enforce access rights according to the sensitivity and criticality of information (e.g., password, token, digital signature).
- Determine if trust relationships enforce comparable security levels and maintain user and process identities.
- Select a sample of user and system accounts and a sample ACL to determine existence of the following:
 - Clearly defined requested role and/or privileges
 - Business justification for assignment
 - Data owner and management authorisation
 - Business/risk justification and management approval for non-standard requests
 - Access requested commensurate with job function/role and required segregation of duties
 - Documentation evidencing adherence to and completion of the provisioning process

Documenting the Impact of Control Weaknesses

[Home](#)
[Browsing](#)
[Benchmarking](#)
[Community](#)
[Sign Out](#)

[Browsing](#) > [Browse All Contents](#)

	F.W.	C.O.	I/O	RACI	G&M	M.M.	C.P.	Assurance Steps
Process Controls PC Process Controls 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 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 Accredited Solutions and Changes 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								

DS5 Deliver and Support
Ensure Systems Security
 Process Importance

Testing The Control Design

Testing the Outcome of the Control Objective

Documenting the Impact of Control Weaknesses

- Determine the level of security consciousness within the organisation by reviewing functional and operational documentation for the existence of security considerations (e.g., involvement of the security management function within the SDLC).
- Benchmark the information security organisation (e.g., size, lines of reporting) against similar organisations, and benchmark formalised policies, standards and procedures to international standards/recognised industry best practices.
- Determine if the security management function is commensurate with the size and complexity of the IT landscape. Consider the following:
 - Size, complexity and diversity of the IT landscape
 - Use of security administration tools and technology
 - Alignment of security management to business lines (e.g., do organisation segments have competing security functions?)
 - Skills and training of security management personnel
- Determine if members of executive management communicate the importance and their support of the security management organisation. Consideration should be given to executive management or security steering committee approval of formalised security policies.
- Determine the existence of a management-approved security charter and policies, standards and procedures that address logical security for all relevant aspects of the organisation's IT landscape.
- Determine if the IT security plan has adequately considered the security profile of the organisation, including any regulatory and compliance requirements.
- Assess the ability of the security management organisation to execute and monitor compliance with the plan. Consideration should be given to the size of the organisation, use of security assessment and administration technology and tools, and required experience levels and ongoing training received by security personnel.
- Select policy, standards and procedural documentation from various financial, operational and compliance areas within the organisation, and determine if key provisions of the IT security plan have been appropriately reflected in the documentation.
- Determine if a security review process has been integrated into the organisation's AI and DS processes, requiring security management's involvement and approval of any IT changes that would impact the design or operation systems security.
- Determine if the organisation's AI processes and controls are supported by segregated development, test and assurance, and production environments.
- Identify the existence and reasonableness of anonymous and group accounts (e.g., nobody, web user, everybody), remote processes and started tasks. Consideration should be given to the nature and scope of transaction authorities, the risk of possible escalation of privileges, the process origin (e.g., trusted, non-trusted), or if a security design review was performed for system and application initiated jobs and processes.
- Determine if security software, applications and supporting systems software has been configured to enforce user authentication or propagate user and process identities. Determine if default accounts exist to authenticate anonymous users or processes.
- Determine sources of non-trusted access (e.g., business partners, vendors), and determine how access has been assigned to provide uniquely identifiable account holders and appropriate protection of information.
- Through the use of audit software tools or scripts, identify the existence of inactive or unused accounts and determine the existence of a business justification.
- Identify active vendor or contractor accounts, and determine if access is commensurate with the terms and duration of the contract.
- Determine if vendor-supplied accounts have been appropriately safeguarded (e.g., default passwords changed, accounts revoked).
- Assess the reasonableness of the nature and frequency of verification and vulnerability assessment processes utilised, considering the organisation's risk profile, size, complexity and diversity.
- Determine if security scripts and tools are utilised to test the existence of common vulnerabilities, the effectiveness of security mechanisms and the

Linking Business Goals To IT Goals

	Business Goals		IT Goals							
Financial Perspective	1	Provide a good return on investment of IT-enabled business investments.	24							
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22
	3	Improve corporate governance and transparency.	2	18						
Customer Perspective	4	Improve customer orientation and service.	3	23						
	5	Offer competitive products and services.	5	24						
	6	Establish service continuity and availability.	10	16	22	23				
	7	Create agility in responding to changing business requirements.	1	5	25					
	8	Achieve cost optimisation of service delivery.	7	8	10	24				
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26			
Internal Perspective	10	Improve and maintain business process functionality.	6	7	11					
	11	Lower process costs.	7	8	13	15	24			
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27	
	13	Provide compliance with internal policies.	2	13						
	14	Manage business change.	1	5	6	11	28			
	15	Improve and maintain operational and staff productivity.	7	8	11	13				
Learning and Growth Perspective	16	Manage product and business innovation.	5	25	28					
	17	Acquire and maintain skilled and motivated people.	9							

Linking IT Goals to IT Processes

LINKING IT GOALS TO IT PROCESSES

IT Goals	Processes											COBIT Information Criteria						
	P01	P02	P04	P010	AI1	AI6	AI7	DS1	DS3	ME1		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1 Respond to business requirements in alignment with the business strategy.	P01	P02	P04	P010	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2 Respond to governance requirements in line with board direction.	P01	P04	P010	ME1	ME4							P	P					
3 Ensure satisfaction of end users with service offerings and service levels.	P08	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4 Optimise the use of information.	P02	DS11											S		P			S
5 Create IT agility.	P02	P04	P07	AI3								P	P		S			
6 Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6									P	P				S	
7 Acquire and maintain integrated and standardised application systems.	P03	AI2	AI5									P	P				S	
8 Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5										S	P					
9 Acquire and maintain IT skills that respond to the IT strategy.	P07	AI6										P	P					
10 Ensure mutual satisfaction of third-party relationships.	DS2											P	P	S	S	S	S	S
11 Ensure seamless integration of applications into business processes.	P02	AI4	AI7									P	P		S	S		
12 Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	P05	P06	DS1	DS2	DS6	ME1	ME4					P	P				S	S
13 Ensure proper use and performance of the applications and technology solutions.	P06	AI4	AI7	DS7	DS8							P	S					
14 Account for and protect all IT assets.	P09	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15 Optimise the IT infrastructure, resources and capabilities.	P03	AI3	DS3	DS7	DS9							S	P					
16 Reduce solution and service delivery defects and rework.	P08	AI4	AI6	AI7	DS10							P	P		S	S		
17 Protect the achievement of IT objectives.	P09	DS10	ME2									P	P	S	S	S	S	S
18 Establish clarity of business impact of risks to IT objectives and resources.	P09											S	S	P	P	P	S	S
19 Ensure that critical and confidential information is withheld from those who should not have access to it.	P06	DS5	DS11	DS12										P	P	S	S	S
20 Ensure that automated business transactions and information exchanges can be trusted.	P06	AI7	DS5									P			P	S	S	
21 Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	P06	AI7	DS4	DS5	DS12	DS13	ME2					P	S		S	P		
22 Ensure minimum business impact in the event of an IT service disruption or change.	P06	AI6	DS4	DS12								P	S		S	P		
23 Make sure that IT services are available as required.	DS3	DS4	DS8	DS13								P	P			P		
24 Improve IT's cost-efficiency and its contribution to business profitability.	P05	DS6										S	P					S
25 Deliver projects on time and on budget, meeting quality standards.	P08	P010										P	P		S			S
26 Maintain the integrity of information and processing infrastructure.	AI6	DS5										P	P		P	P		S
27 Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4										S	S		P	S
28 Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	P05	DS6	ME1	ME4								P	P					P

IT Process to IT Goals Matrix

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Plan and Organise																												
P01 Define a strategic IT plan.	✓	✓																										
P02 Define the information architecture.	✓			✓	✓						✓																	
P03 Determine technological direction.							✓																					
P04 Define the IT processes, organisation and relationships.	✓	✓			✓																							
P05 Manage the IT investment.																												
P06 Communicate management aims and direction.												✓	✓							✓	✓	✓	✓		✓			✓
P07 Manage IT human resources.					✓				✓																			
P08 Manage quality.			✓														✓											
P09 Assess and manage IT risks.															✓			✓	✓							✓		
P010 Manage projects.	✓	✓																								✓		
Acquire and Implement																												
A01 Identify automated solutions.	✓					✓																						
A02 Acquire and maintain application software.					✓	✓	✓																					
A03 Acquire and maintain technology infrastructure.				✓				✓							✓													
A04 Enable operation and use.			✓								✓		✓			✓												
A05 Procure IT resources.							✓	✓	✓	✓																		
A06 Manage changes.	✓				✓											✓						✓				✓		
A07 Install and accredit solutions and changes.	✓										✓		✓			✓				✓	✓							
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.			✓																		✓	✓	✓					
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.		✓										✓														✓	✓	✓

CobiT 4.x Release

- ❖ Detailed control objectives now covers IT governance more completely, better harmonized and more concise (About 30% fewer controls). Reduced from 320 (CobiT 3.0) to 215 (CobiT 4.0)
- ❖ Generic process-related control objectives moved to the *Framework* as part of Process Goals/Objectives
 - ❖ Goals and objectives
 - ❖ Ownership
 - ❖ Repeatability
 - ❖ Roles and Responsibility
 - ❖ Policy, Plans and Procedures
 - ❖ Process Performance Improvement
- ❖ Application controls moved into the *Framework* section from Delivery & Support

COBIT 4.1 Update

- ❖ Enhanced *Executive Overview* section

Very minor changes

- ❖ Explanation of goals and metrics in the *Framework* section

Minor, mostly rearrangement for presentation and additional clarification

- ❖ Better definitions of the core concepts. It is important to mention that the definition of a control objective changed, shifting more toward a management practice statement.

This has been true since CobiT 3.0 to 4.0 update. Progressive verbiage changes were made for clarification or generalizing purposes.

COBIT 4.1 Update (Cont'd)

- ❖ Improved control objectives resulting from updated control practices and Val IT development activity. Some control objectives were grouped and/or reworded to avoid overlaps and make the list of control objectives within a process more consistent. Specific revisions include:

- ❖ AI5.5 and AI5.6 were combined with AI5.4

Software Acquisition + Acquisition of Development Resources + Acquisition of Infrastructure, Facilities, and Related Services = IT Resources Acquisition

- ❖ AI7.9, AI7.10 and AI7.11 were combined with AI7.8

Software Release + System Distribution + Recording and Tracking of Changes = Promotion to Production

- ❖ ME3 was revised to include compliance with contractual requirements in addition to legal and regulatory requirements

ME3 = Ensure Compliance With External Requirements.
More generic with details moved to Control Practices

COBIT 4.1 Update (Cont'd)

- ❖ Application controls have been reworked to be more effective, based on work to support controls effectiveness assessment and reporting. 6 application controls replaced the 18 application controls in COBIT 4.0, with further detail provided in COBIT Control Practices, 2nd Edition.
- ❖ The list of business goals and IT goals in Appendix I was improved, based on new insights obtained during validation research executed by the University of Antwerp Management School (Belgium).
- ❖ The pull-out has been expanded to provide a quick reference list of the COBIT processes, and the overview diagram depicting the domains has been revised to include reference to the process and application control elements of the COBIT framework.
- ❖ Improvements identified by COBIT users (COBIT 4.0 and COBIT Online) have been reviewed and incorporated as appropriate.

Impact on Users: CobiT 3.x to 4.0 Update

- ❖ CobiT 4.0 is an evolution from the 3rd edition based on the same core principals and structure – no need to “throw away” current work
- ❖ CobiT 4.0 build on and extends 3rd edition with stronger business focus and governance practices
- ❖ The metrics build on the same principles, are integrated with goals and provide more and better examples to help users design their own
- ❖ Full x-references provided in appendices showing how processes and control objectives map in both directions to help conversions

Impact on Users: CobiT 3.x to 4.0 Update

- ❖ Still 4 Domains and 34 Processes
- ❖ An incremental update to CobiT 4.0
- ❖ IT Assurance Guide and CobiT Control Practices were updated with CobiT 4.1

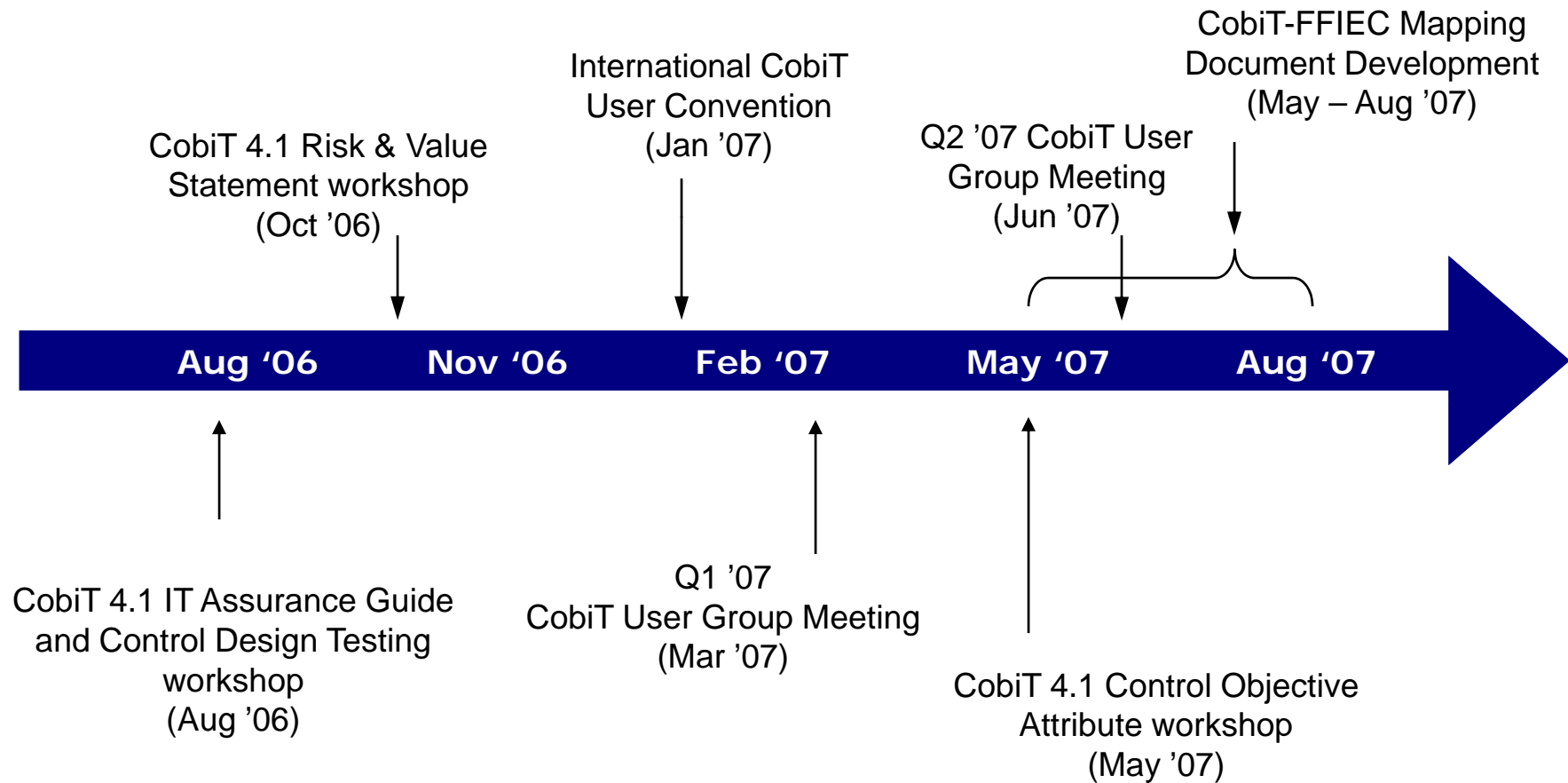
COBIT Campus

With the growing adoption of COBIT, ISACA recognized the need for structured and formal education and worked together with *ITpreneurs* to develop authentic COBIT learning solutions. COBIT training courses help professionals master COBIT and utilize this knowledge for effective implementation within their organizations. Sustainable COBIT competencies help IT organizations and departments align with the goals and objectives of the business and generate strategic value from IT.

The COBIT curriculum includes the following courses:

- ❖ COBIT Awareness Course (2 hours, self paced e-learning)
- ❖ COBIT Foundation Course (8 hours, self paced e-learning or 14 hours, classroom)
- ❖ COBIT Foundation Exam (1 hour, online 40 questions)
- ❖ IT Governance Implementation Course (14 hours, classroom)
- ❖ COBIT for Sarbanes-Oxley Compliance (5 hours, self paced e-learning)

COBIT Timeline '06 – '07



LA ISACA Felt Need to Further COBIT - Why and How

Input

- ❖ CobiT increasingly accepted and adopted as standard IT Governance Framework.
- ❖ Opportunity to better serve our constituents – Validated the need during the Christmas party, distributed CobiT survey to determine interest.
- ❖ Lack of support for successful adoption in companies / need for evangelizing of CobiT
- ❖ Realize valuable resources available (Big “4”, representations from major local corporations in key roles, etc)
- ❖ Strong relationship with ISACA International
- ❖ Identify need to organize chapter initiatives around CobiT

Los Angeles ISACA Survey

Survey in 4th Quarter 2006

- ❖ Survey Response Rate: 43%
 - ❖ 72 attendees (excluding speaker)
 - ❖ 32 responses received
- ❖ 22 companies represented

Survey Results

Survey Questions	Statistics
Enough interest?	78% say Yes!
CobiT Education Opportunities	72% are “Somewhat Familiar” or “Not Familiar” with CobiT
CobiT User Group Format	44% would like combination of presenters, case studies, and round-table discussions. Appears that there is a preference toward passive meetings
CobiT adoption by companies	Only 14% Formally Adopted 41% Not Adopted 41% Somewhere In Between
How does companies use CobiT?	Approx 50% use for Internal Audit, SOX, and IT Governance
Meeting format	81% would prefer dinner

Survey (Con't)

Topic Suggestions

- ❖ CobiT Training 101, Getting Started
- ❖ CobiT Revision Updates, What's New?
- ❖ CobiT Implementation
- ❖ Selling CobiT to C-Level Management
- ❖ Lessons Learned (Case Studies)
- ❖ CobiT as IT Governance
- ❖ CobiT as SDLC/Change Management
- ❖ Potential CobiT gaps/weaknesses
- ❖ CobiT/COSO mapping
- ❖ SOX & CobiT
- ❖ IT Audit & CobiT
- ❖ Similarities/differences between IT Audit & IT Operations leveraging CobiT

Survey (Con't)

Output

- Formed a CobiT User Group – Asked for interested members in survey. Email distribution: cobituser@isacala.org
- CobiT User Group Format:
 - 2 hour meetings
 - Presenter for 1st hour, moderated open floor discussion for 2nd hour
 - Sponsors
 - Meeting minutes taken and distributed
- Communication with CobiT International:
 - Meeting minutes from CobiT User Group are distributed to International
 - Received responses to user queries and good feedback from International
- Organize local CobiT experts and volunteers:
 - cobit@isacala.org is for volunteers on the CobiT committee
 - cobitdev@isacala.org is for CobiT experts in the local area (dynamic)

LA ISACA Survey Action Plans

- ❖ Dedicated CobiT chair with CobiT knowledge and real life experience. Committees of volunteers with a wide range of CobiT knowledge and experience from various industries.
- ❖ Organization of CobiT experts and volunteers. Marketing and communication to local constituents
- ❖ Create a community / forum for questions and answers (provide education and support for acceptance and adoption at organizations as well as sharing of knowledge)
- ❖ Utilize local credential trainers to offer education at cost (no intention to make profit on CobiT activities, subsidize where possible or find sponsors).
- ❖ Strengthen and formalize relationship with International (Brian Selby, Director of CobiT Initiatives) and CobiT Steering Committee through communications and support of CobiT development initiatives.
- ❖ Capitalize on chapters' strength – committed volunteers (bench strength) and community relationships.
- ❖ CobiT User Group meetings are “FREE”!

LA ISACA COBIT Future Events

- ❖ Continued CobiT User Group Meetings
- ❖ Conduct “C” level roundtables around CobiT and IT Governance
- ❖ Invitation to speak at Campus events on CobiT (e.g., part of USC curriculum)
- ❖ CobiT Foundations Course and Certificate Exam
 - ❖ Originally scheduled for July 11- 13, 2007, did not market and provide sufficient lead time to obtain the minimum 12. Plan to reschedule for the first quarter of 2008.
 - ❖ CobiT Foundation course with local trainer: \$3,650 for 16 people. Minimum of 12. Plus food and beverage.
- ❖ CobiT User Convention will be held concurrently with the ISACA-LA Spring Conference
 - ❖ Include as additional conference track to utilize existing conference resources.
 - ❖ Combination of Presentations/Case Studies and facilitated sessions.
- ❖ Implementing IT Governance with CobiT and Val IT Workshop
 - ❖ Will be offered as a pre-conference workshop as part of the CobiT User Convention.

Continued Efforts

- ❖ What other opportunities are there for broader adoption and application?
- ❖ How can we support membership in adoption, implementation and sustainable usage?
- ❖ Act as a conduit to the CobiT Steering Committee to communicate membership needs - What needs to change in CobiT? Influence CobiT 5.0
- ❖ What additional guidance is needed for adopters?
- ❖ What training is needed? CPEs for upcoming IT Governance Certification
- ❖ How can CobiT work better with other standards and frameworks? (additional mapping projects)
- ❖ Stay connected with other CobiT User Groups (Atlanta, Toronto etc.) learn from each other
- ❖ Develop CobiT page on chapter website to provide CobiT resources.

Current LA ISACA COBIT Initiative

FFIEC Handbook	In Scope?	Reviewer Assigned
Audit	Yes	Mark Stanley
Business Continuity Planning	Yes	Thomas Phelps
Development and Acquisition	Yes	Miguel Villegas
E-Banking	No	N/A
FedLine	No	N/A
Information Security	Yes	Cheryl Santor
Management	Yes	David Melnick
Operations	Yes	Jack Flaherty
Outsourcing Technology Services	Yes	Amanda Xu
Retail Payment Systems	No	N/A
Supervision of Technology Service Providers	No	N/A
Wholesale Payment Systems	No	N/A

- ❖ Common FFIEC Index
- ❖ FFIEC to COBIT
- ❖ COBIT to FFIEC

Tab Color Legend
Foundational Prep Work
Reviewer's tab
Core Team's Development
Analysis

FFIEC Mapping Projects

Common FFIEC Index

FFIEC Index	FFIEC IT Handbook	FFIEC Section	FFIEC Subsection	FFIEC Subsection Level 2
1.1.0.0	Audit	Introduction		
2.2.0.0	Audit	IT Audit Roles and Responsibilities		
2.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management	
2.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management	
2.2.3.0	Audit	IT Audit Roles and Responsibilities	Internal IT Audit Staff	
2.2.4.0	Audit	IT Audit Roles and Responsibilities	Operating Management	
2.2.5.0	Audit	IT Audit Roles and Responsibilities	External Auditors	
2.3.0.0	Audit	Independence Staffing of Internal IT Audit		
2.3.1.0	Audit	Independence Staffing of Internal IT Audit	Independence	
2.3.2.0	Audit	Independence Staffing of Internal IT Audit	Staffing	
2.4.0.0	Audit	Internal Audit Program		

COBIT to FFIEC

Process	Process Description	CO	COBIT Control Objective	Coverage	FFIEC Index	FFIEC IT Handbook	FFIEC Section	FFIEC Subsection	FFIEC Subsection Level 2
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	2.3.4.1	Outsourcing Technology Services	Risk Management	Ongoing Monitoring	Key Service Level Agreements and Contract Provisions
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	2.3.3.0	Outsourcing Technology Services	Risk Management	Contract Issues	
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	4.3.2.2	E-Banking	Risk Management of E-Banking Activities	Managing Outsourcing Relationships	Contracts for Third-Party Services
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	10.4.6.4	Retail Payment Systems	Retail Payment System Risk Management	Operational (Transaction) Risk	Vendor and Third-Party Management
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	12.5.6.5	Wholesale Payment Systems	Wholesale Payment Systems Risk Management	Operational (Transaction) Risk	Vendor and Third-Party Management
DS1	Define and manage service levels.	DS1.1	Service level management framework	A	7.5.0.2	Management	Management Considerations for Technology Service Providers		Contracts
DS1	Define and manage service levels.	DS1.2	Definition of services	A	2.3.4.1	Outsourcing Technology Services	Risk Management	Ongoing Monitoring	Key Service Level Agreements and Contract Provisions

FFIEC to COBIT

FFIEC Index	FFIEC IT Handbook	FFIEC Section	FFIEC Subsection	FFIEC Subsection Level 2	COBIT #	COBIT Control Objective	Coverage
1.1.0.0	Audit	Introduction			PO6.2	Enterprise IT Risk and Control Framework	A
2.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management		ME1.1	Monitoring approach	A
2.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management		PO4.2	IT Strategy Committee	A
2.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management		PO4.3	IT Steering Committee	A
2.2.1.0	Audit	IT Audit Roles and Responsibilities	Board of Directors and Senior Management		PO4.8	Responsibility for Risk, Security and Compliance	A
2.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management		ME2.2	Supervisory review	A
2.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management		ME4.7	Independent assurance	A
2.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management		PO4.8	Responsibility for Risk, Security and Compliance	A
2.2.2.0	Audit	IT Audit Roles and Responsibilities	Audit Management		PO7.4	Personnel Training	A
2.2.3.0	Audit	IT Audit Roles and Responsibilities	Internal IT Audit Staff		ME4.7	Independent assurance	A
2.2.3.0	Audit	IT Audit Roles and Responsibilities	Internal IT Audit Staff		PO4.8	Responsibility for Risk, Security and Compliance	A
2.2.4.0	Audit	IT Audit Roles and Responsibilities	Operating Management		ME2.7	Remedial actions	C
2.2.4.0	Audit	IT Audit Roles and Responsibilities	Operating Management		ME3.4	Positive assurance of compliance	A
2.2.4.0	Audit	IT Audit Roles and Responsibilities	Operating Management		ME4.7	Independent assurance	A

IT Governance Certification



**CGEIT - Certified in the
Governance of Enterprise IT**

- ❖ Promoted in the last Expressline and CobiT Focus newsletter.
- ❖ CobiT is a key reference in forming the foundation of this certification
- ❖ Take advantage of ITPrenuers chapter offering of CobiT education courses (reduced pricing).
- ❖ Initial exam is targeted for December 2008 (grandfathering will also be available)

CGEIT Grandfathering

- ❖ ISACA/ITGI is not accepting grandfathering applications at this time, but plan to do so in the future. Additional information and details will be posted at a future date when this provision is active. The following is being provided to give you a general sense of this provision.
- ❖ Highly experienced professionals who have had a significant management, advisory and/or assurance role relating to the governance of IT will be allowed to apply for CGEIT certification without being required to pass the CGEIT examination.
- ❖ To earn the CGEIT certification during this grandfathering period, an applicant must:
- ❖ Have and submit evidence of eight (8) years of experience associated with the governance of the IT-related contribution to an enterprise, with a minimum of three (3) of these years performing tasks directly related to any two or more of the aforementioned CGEIT domains.
- ❖ Describe (200-500 words) their experience managing, providing advisory and/or assurance services, and/or otherwise supporting the governance of an enterprise's information technology.
- ❖ Adhere to the ISACA [Code of Professional Ethics](#)
- ❖ Agree to comply with the [CGEIT Continuing Education Policy](#)
- ❖ Pay an application fee:
 - ❖ US \$595—for ISACA members
 - ❖ US \$660—for non-ISACA member credential holders in good standing
 - ❖ US \$725—for all others

Thank You!

Questions?

Miguel (Mike) O. Villegas, CISA, CISSP
(626) 200-5049
villegas-mo@sbcglobal.net