CobiT, ITIL and ISO17799 How to use them in conjunction

Angeli Hoekstra & Nicolette Conradie

PRICEWATERHOUSE COPERS 1880

Content

Overview IS O 17799 - Nicolette

Overview CobiT

- Overview ITIL
- How to use them in conjunction
- Conclusion

Cohit IIII a



BS 7799

- Provides guidelines and recommendations for security management.
- Part 1 Standard; and
- Part 2 Certification.

BS7799

2000

ISO 17799

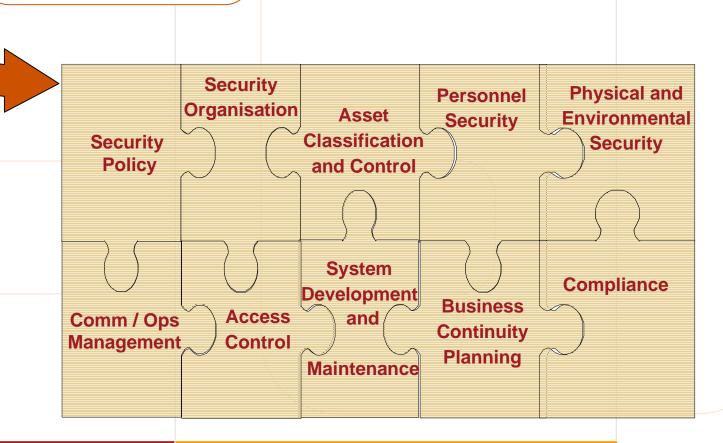
2001

SABS 17799

IS O 17799

- Part 1 accepted as International Standard;
- Part 2 to be accepted end of 2002.

Organisational Risks



Documented & communicate IS policy Regularly reviewed

Allocation of roles & responsibilities 3rd-party access risks/controls
Outsourcing

Security Organisation

Asset
Classification
and Control

Security Policy

Inventory of Assets

Classification based on sensitivity/business impact

Awareness & training

Reporting of incidents

Physical security perimeters
Equipment siting
Clear desk & clear screen

Physical and Environmental

Security

Comm / Ops Management Incident procedures

Segregation of duties

System planning & acceptance

Malicious software protection

F-mail controls

Managing Access

- Application Level
- Operating Level
- Network Level

Change control procedures
Segregation of environments
Security requirements



6

System Development

and

Maintenance

CobiT, ITIL and IS O1779



Business Continuity

Planning



Copyright controls

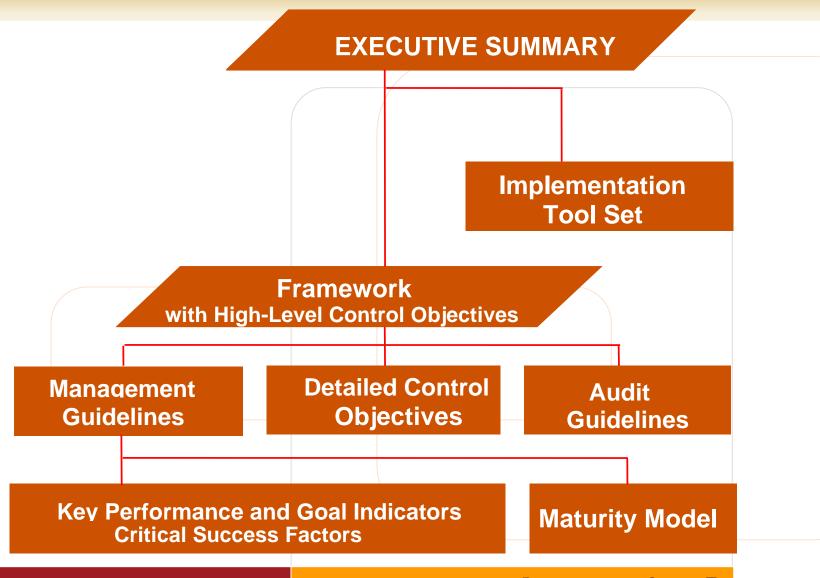
Retention of records and information

Compliance with legislation - Data protection

Compliance with company policy



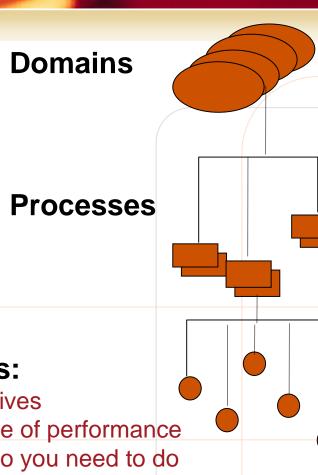
CobiT Product Family



CobiT Principles



CobiT



Acquisition & Implementation

13

- Al 1: Identify automated solutions
- Al 2: Acquire and maintain application software
- Al 3: Acquire and maintain technology infrastructure
- Al 4: Develop and maintain procedures
- Al 5: Install and accredit systems
- Al 6: Manage Changes



Al 6: Manage Changes: Control objectives

- 6.1: Change request initiation and control
- 6.2: Impact assessment
- 6.3: Control of changes
- 6.4: Emergency changes
- 6.5: Documentation and procedures
- 6.6: Authorised maintenance
- 6.7: Software release policy
- 6.8: Distribution of software

Per process:

Control objectives

•KPI's: measure of performance

•CSF's: what do you need to do

•KGI's: measure of outcome

Maturity model

CobiT

Key Goal Indicators: Manage Change

- •Reduced number# of errors introduced into systems due to changes
- •Reduced number# of disruptions (loss of availability) caused by poorly managed change
- •Reduced impact of disruptions caused by change
- •Reduced level of resources and time required as a ratio to number# of changes
- •Number# of emergency fixes/time

Key Performance Indicators: Manage Change

- •Number# of different versions installed at the same time
- •Number# of software release/and distribution methods per platform
- •Number# of deviations from the standard configuration
- •Number# of emergency fixes for which the normal change management process was not applied retro-actively
- •Time lag between availability of fix and implementation of it. .
- •ratio of accepted vs refused change implementation requests.

Critical Success Factors: Manage Change

- Expedient and comprehensive acceptance test procedures are applied prior to making the change.
- There is a reliable hardware and software inventory.
- There is segregation of duties between production and development

. . . .

•....

CobiT. ITIL and

14



The ITIL jigsaw

what service the business requires of the provider in order to provide adequate support to the business users

ensuring that the customer has access to the appropriate

services to support the business functions



understanding and improving IT service provision, as an integral part

of an overall business requirement for high quality IS management

Business Continuity Management

partnerships and outsourcing

surviving change

transformation of business practice through radical change.

Network Service Management

Operations Management

Management of Local Processors

Computer Installation and Acceptance

Systems Management

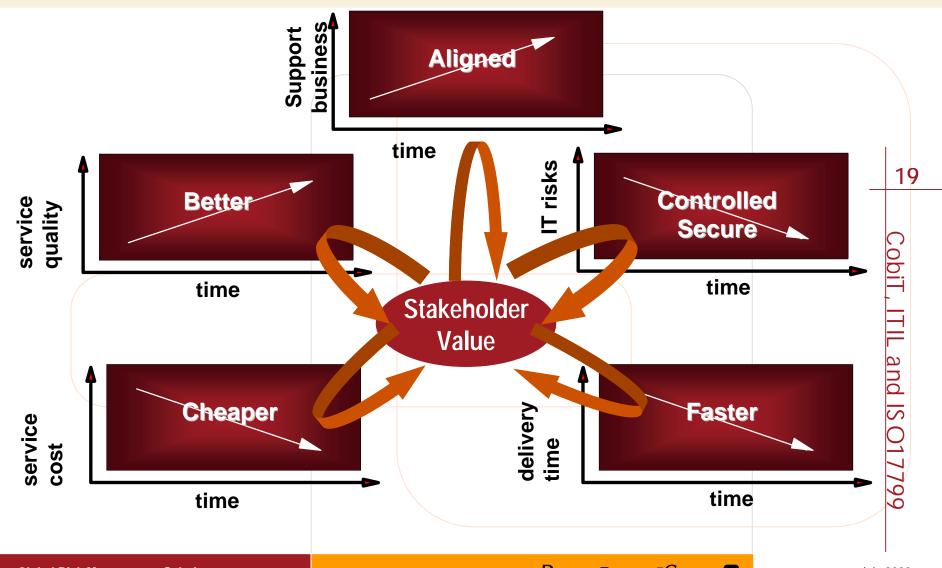
16

ITIL service support & service delivery processes

- Service support:
 - Service desk
 - Incident management
 - Problem management
 - Configuration management
 - Change management
 - Release management
- Service delivery
 - capacity management
 - availability management
 - financial management of IT services
 - service level management
 - IT service continuity management



What do we want to achieve with IT?



How we can achieve these IT goals

The assignment of responsibility for performing specified activities to specific groups or individuals

The people that support effective and efficient IT service management

People

Roles

Structure

&

Metrics

Processes

The assignment of measurements to people, processes, technology and controls to ensure they comply to what they are intended for

The assignment of controls to IT processes to ensure that they deliver efficiently and effectively in line with clients requirements

Controls

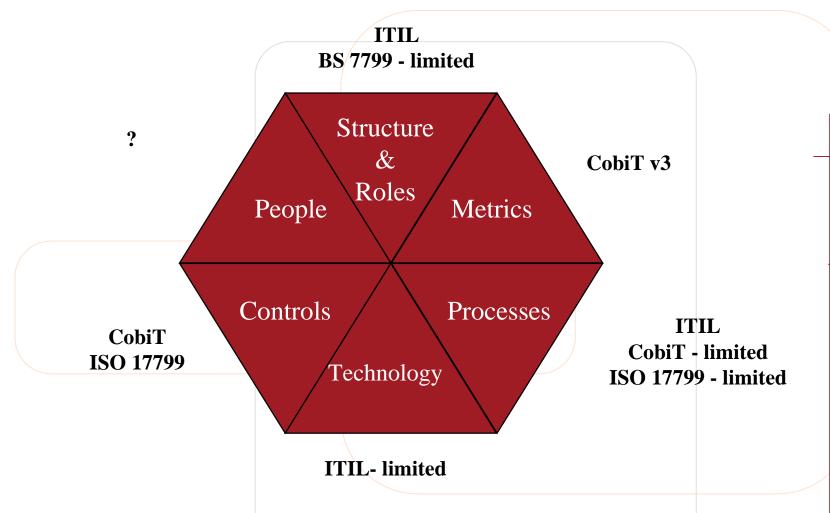
Technology

The interrelated series of activities that combine to produce products or services for internal & external clients

The technology that is supporting the IT delivery



How we can achieve these IT goals

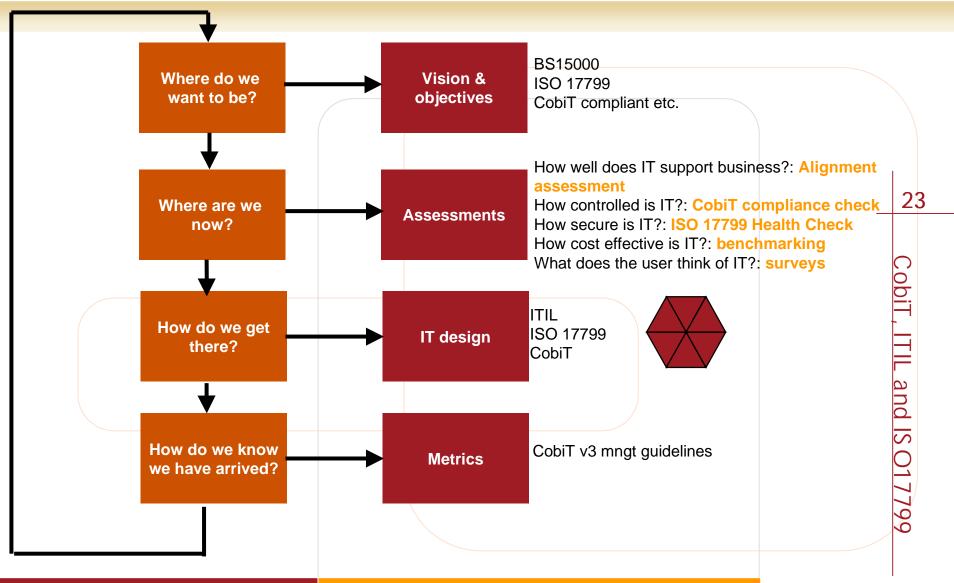


21

How we can achieve these IT goals: Where are the methods strong in?

- ITIL strong in IT processes, but limited in security and system development
- CobiT strong in IT controls and IT metrics, but does not say how (i.e. process flows) and not that strong in security
- ISO 17799 strong in security controls, but does not say how (i.e. process flows)
- Conclusion:
 - No contradictions or real overlaps
 - None identify people requirements
 - Not strong on organisational side (structure & roles)
 - Not strong on technology side

How can we achieve these IT goals: continuous IT improvement



Materiality		Control Risk	Control	Effectiveness	Efficiciency	Confidential	Integrity	Availibility	Compliance	Reliability	./
Planning and organisation											
Define a strategic IT plan	Dlanni			4	4	4	1.5	1.5	1.5	1.5	H
PO 2 Define the information architecture			2	C							
PO 3 Determine the technological direction		• .				C	0				
PO 4 Define organisation and relationships 2 C H	_					C	U				
PO 5 Manage the investment PO 6 Communicate management aims and direction Manage human resources PO 8 Ensure compliance with external requirements PO 10 Manage projects PO 11 Manage projects PO 11 Manage quality PO 11 Manage quality PO 11 Manage quality PO 11 Manage quality PO 12 Acquire and maintain application software A1 1 Identify automated solutions A1 2 Acquire and maintain application software A1 3 Acquire and maintain application software A1 4 Develop and maintain procedures A1 4 Develop and maintain procedures A1 5 Install and accredit systems A1 6 Managing changes A1 7 E E O O O O O O O O O O O O O O O O O		ű .									
PO 6 Communicate management aims and direction 1										0	
PO 7 Manage human resources PO 8 Ensure compliance with external requirements PO 9 Assess risk PO 10 Manage projects PO 11 Manage quality PO 12 Manage quality PO 12 Manage and maintain application software PO 13 Acquire and maintain technology architecture PO 14 Acquire and maintain technology architecture PO 15 Manage data Po 16 Managing changes PO 16 Managing changes PO 17 Manage third-party services PO 18 Manage performance and capacity PO 19 Manage third-party services PO 19 Manage third-party services PO 10 Manage performance and capacity PO 10 Manage performance and capacity PO 10 Manage performance and train users PO 10 Manage the configuration PO 10 Manage data PO					0		-		0		
PO 8 Ensure compliance with external requirements PO 9 Assess risk 1 C C E C C C O O PO 90 Assess risk 1 C C C E C C O O PO 90 Manage projects 1 E E C C O O PO 90 Manage projects 1 E E C C O O PO 90 Manage quality 1 E E C C O O PO 90 Manage quality 1 E E C C O O PO 90 Manage quality 1 E E C C O O PO 90 Manage quality 1 E E C C O O PO 90 Manage quality 1 E E C C O O O O O O PO 90 Manage quality 1 E E C C C C C C C C C C C C C C C C C		ŭ			F						
PO 9 Assess risk PO 10 Manage projects 1		-							С	Ο	
PO 10 Manage projects					С	F	С	С			
PO 11 Manage quality			-			_	Ŭ	Ü	Ŭ	Ŭ	
Acquisition and implementation Al 1 Identify automated solutions Al 2 Acquire and maintain application software Al 3 Acquire and maintain technology architecture Al 4 Develop and maintain procedures Al 5 Install and accredit systems Al 6 Managing changes Al 6 Managing changes Al 7 C							С			0	
Al											
Al 2											
Al 3		,		Е							
Al 4 Develop and maintain procedures Al 5 Install and accredit systems Al 6 Managing changes 2 C C C c c C Delivery and support S 1 Define service levels 1 E E C O O O O S 2 Manage third-party services 1 E E C O O O O S 3 Manage performance and capacity 1 E E C O O O O S 4 Ensure continuous service 2 C H C C C O O O O S 5 Ensure systems security 2 C C C O O O O O S 6 Identify and allocate costs 1 E C C O O O O O S 7 Educate and train users 1 E C C O O O O O S 8 Assist and advice customers 1 E C C O O O O O S 10 Manage problems and incidents 1 E C C C O O O O O Manage facilities 2 C C C O O O O O Manage adata 2 C C C O O O O O Manage operations Monitoring M 1 Monitor the process 1 E C C O O O O O M 2 Assess internal control adequacy M 4 Provide for Independent Audit Legend: E Exposure C Concern O K		• • • • • • • • • • • • • • • • • • • •							0	0	
Al 5 Install and accredit systems Al 6 Managing changes 2 C C C C C C Delivery and support DS 1 Define service levels 1 E E C O O O O DS 2 Manage third-party services 1 E E C O O O O DS 3 Manage performance and capacity 1 E E C O O O O DS 4 Ensure continuous service 2 C H C C O O O DS 5 Ensure systems security 2 C C C O O O DS 6 Identify and allocate costs 1 E C C DS 7 Educate and train users 1 E C C DS 8 Assist and advice customers 1 E C C DS 9 Manage the configuration 1 E E C O O O DS 10 Manage problems and incidents 1 E E C O O DS 11 Manage data 2 C C C DS 12 Manage facilities 2 C C C DS 13 Manage operations 1 E E C O O O M1 Monitor the process 1 E C C O O O O M1 Monitor the process 1 E C C O O O O M3 Obtain independent assurance 1 E E C O O O O M4 Provide for Independent Audit 1 E E Exposure C Concern O K			-				_				
Al 6 Managing changes 2 C C C C C C C C C C C C C C C C C C		·			Е				0	0	
Delivery and support		-					0	0			
Define service levels	Al 6	Managing changes	2	С	С		С	С		0	
Define service levels	Delive	ry and support									
DS 3 Manage performance and capacity 1 E E O DS 4 Ensure continuous service 2 C H C DS 5 Ensure systems security 2 C C O O O DS 6 Identify and allocate costs 1 E C C O O O DS 7 Educate and train users 1 E C C O </td <td>DS 1</td> <td>Define service levels</td> <td>1</td> <td>Е</td> <td>Е</td> <td>С</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td></td>	DS 1	Define service levels	1	Е	Е	С	0	0	0	0	
DS 4 Ensure continuous service 2 C H C C O O O	DS 2	Manage third-party services	1	Е	Е	С	0	0	0	0	
DS 5	DS 3	Manage performance and capacity	1	Е	Е			0			
DS 6 Identify and allocate costs 1	DS 4	Ensure continuous service	2	С	Н			С			
DS 7 Educate and train users 1 E C	DS 5	Ensure systems security	2			С	С	0	0	0	
DS 8 Assist and advice customers 1 E 0 0 DS 9 Manage the configuration 1 E 0 0 DS 10 Manage problems and incidents 1 E E 0 0 DS 11 Manage data 2 c c c 0 DS 12 Manage facilities 2 c c c c DS 13 Manage operations 1 E E 0 0 0 Monitoring M 1 Monitor the process 1 E C C 0 0 0 M 2 Assess internal control adequacy 1 E E C 0 0 0 M 3 Obtain independent assurance 1 E E C 0 0 0 M 4 Provide for Independent Audit 1 E E C 0 0 0		Identify and allocate costs	1		Е					С	
DS 9 Manage the configuration 1 E		Educate and train users	1		C						
DS 10 Manage problems and incidents 1 E E 0 DS 11 Manage data 2 C C DS 12 Manage facilities 2 C C DS 13 Manage operations 1 E E O O Monitoring M 1 Monitor the process 1 E C C O O O M 2 Assess internal control adequacy 1 E E C O O O O M 3 Obtain independent assurance 1 E E C O O O O M 4 Provide for Independent Audit 1 E E C O O O O Legend: E Exposure H Housekeeping OK O	DS 8	Assist and advice customers	1								
DS 11 Manage data 2 C C DS 12 Manage facilities 2 C C DS 13 Manage operations 1 E E O O Monitoring M 1 Monitor the process 1 E C C O O O M 2 Assess internal control adequacy 1 E E C O O O O M 3 Obtain independent assurance 1 E E C O O O O M 4 Provide for Independent Audit 1 E E C O O O O Legend: E Exposure H Housekeeping OK										0	
DS 12 Manage facilities 2 C C C DS 13 Manage operations 1 E E 0 0 Monitoring M 1 Monitor the process 1 E C C 0 0 0 M 2 Assess internal control adequacy 1 E E C 0 0 0 0 M 3 Obtain independent assurance 1 E E C 0 0 0 0 M 4 Provide for Independent Audit 1 E E C 0 0 0 0 Legend: E Exposure H Housekeeping OK				Е	Е			0			
Namage operations							С				
Monitoring M 1 Monitor the process 1 E C C O O O M 2 Assess internal control adequacy 1 E E C O O O O M 3 Obtain independent assurance 1 E E C O											
M 1 Monitor the process 1 E C C O O O M 2 Assess internal control adequacy 1 E E C O O O O M 3 Obtain independent assurance 1 E E C O O O O M 4 Provide for Independent Audit 1 E E C O O O O Legend: E Exposure H Housekeeping OK	DS 13	Manage operations	1	E	Е		0	0			
M 2 Assess internal control adequacy 1 E E C O O O M 3 Obtain independent assurance 1 E E C O O O O M 4 Provide for Independent Audit 1 E E C O O O O Legend: E Exposure H Housekeeping OK	Monito	l pring									
M 3 Obtain independent assurance 1 E E C O O O M 4 Provide for Independent Audit 1 E E C O O O Legend: E Exposure H Housekeeping C Concern O OK	M 1	Monitor the process	1		С	С	0	0	0	0	
M 4 Provide for Independent Audit 1 E C O O O Legend: E Exposure H Housekeeping C Concern O OK	M 2	Assess internal control adequacy	1		Е	С	0	0	0	0	
Legend: E Exposure H Housekeeping C Concern O OK	М 3	Obtain independent assurance	1		Е	С	0	0	0	0	
C Concern O OK	M 4	Provide for Independent Audit	1	Е	Е	С	0	0	0	0	
C Concern O OK								-			-
C Concern O OK		I eaend-	E	Exnos	osure H Housekeeping			a			
		<u> Logona.</u>									
				2 2 0		С		rn +			

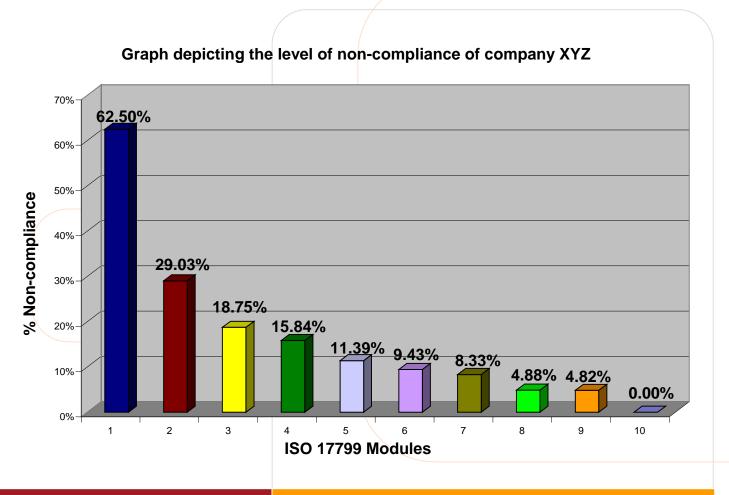
CobiT compliance check

CobiT, ITIL and IS O17799

25

How can we achieve these IT goals: continuous IT improvement

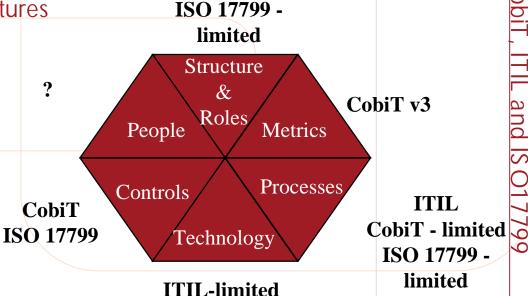
ISO 17799 Health Check



- Use CobiT and ISO 17799 health check to determine current status
- Identify weaknesses in processes and controls
- Use ITIL to improve IT processes & controls, use ISO 17799 to improve security processes & dontrols (although not strong on process side)
- Use ITIL to determine technology, although not complete



Query ITIL on possible structures



ITIL

PRICEV/ATERHOUSE COPERS 1880

Nicolette Conradie:

Nicolette.Conradie@za.pwcglobal.com

082 891 8648

Angeli Hoekstra

Angeli.Hoekstra@za.pwcglobal.com

082 783 1371

