

**Whitepaper**

# **Combining ITIL with COBIT and ISO/IEC 17799:2000**

**Version 1.0: November 2004**

**John Wallhoff**

**Scillani Information AB**

# Combining ITIL with COBIT and ISO/IEC 17799:2000

By John Wallhoff (CISA, CISM, CISSP). founder and Managing Director of Scillani Information AB. Prior to this position, he worked both as an IT-auditor, IS-consultant and with Security management practices within enterprises like Ernst & Young and AddTrust. He has over fourteen years experience in the IT field as an IT/IS consultant and in IS audit/IT-security.

## Summary

ITIL is a powerful framework to support the delivery of IT-services but by combining ITIL with recommendations in COBIT and ISO/IEC 17799:2000 your toolkit will become even stronger.

The current version of ITIL is especially strong when it comes down to the description of concept and processes that outlines how IT-services are delivered. In return COBIT is strong when the issue is controls and metrics, which cover metrics (KPI, KGI) and benchmarking (CMM). Neither ITIL nor COBIT is especially strong when we talk about security even it is described in a broad manner. To compensate this, there are now complimentary publications available for both ITIL and COBIT that cover security aspects.

A broad description of how you may combine ITIL with COBIT and ISO/IEC 17799:2000 is:

<b>ITIL</b>	<b>COBIT</b>	<b>ISO/IEC 17799:2000</b>
Concept/Process	Critical Success Factors	Information Security
Activities	Metrics (KGI, KPI)	
Cost/Benefit	Benchmarking (CMM)	
Planning for implementation	Controls	
	Audit	

To implement a process to deliver IT-services without clearly defining measures for monitoring and to enable recurrent reviews to ensure compliance will lead to a higher risk that it will not be efficient and effective. This is one argument to combine ITIL with COBIT. We have also seen how security issues have become more important for products as well as services where a combination of ITIL and ISO/IEC 17799:2000 will provide you with a strong toolkit to enable delivery of high quality IT-services.

## About the study

For a long time several standards have emerged, all with IT as a focal point. Each of them has its own objectives and is based on different assumptions. At the same time there are several areas where they are complimentary.

In this study we have focused on following standards/methods

- ITIL - IT Infrastructure Library
- COBIT - Control Objectives for Information and related Technology
- ISO/IEC 17799:2000 - The Code of Practice for Information Security Management

The study is based upon ITIL where Service Delivery and Service Support are compared against COBIT and ISO/IEC 17799:2000. The objective for the study is to describe how these standards can be combined and how they specify requirements. ITIL consists of several publications, but we have limited our scope to only address Service Delivery and Service Support.

The target group for the study is IT managers, IT-auditors and IT-/Information security managers, but it may also be valuable for consultants within management, IT and security. It has been made within the research & development at Scillani Information AB.

We have chosen to describe the standards at a high level to identify where these requirements and recommendation can be combined. Then we have continued with more detailed analysis of two different sections. We have chosen not to present detailed requirements and recommendations as these are clearly described within their own publications.

In the study we have made assessments that may not meet conditions that are relevant for an individual enterprise or organization. Although these descriptions will give you an indication of how a combination can be utilized. We will therefore stress that it is important that an assessment like this is performed within each individual project when implementing ITIL, COBIT or ISO/IEC 17799:2000.

All references to ITIL, COBIT or ISO/IEC 17799:2000 are presented as described in their publication.

## Short introduction

### ITIL

#### *IT Infrastructure Library*

ITIL is published by the British Office of Government Commerce (OCG) and have emerged to become a standard for Service Management.

Goal:

The goal is the development of a vendor-independent approach for service management. The ethos behind the development was the recognition of increased dependence on IT, which has to be managed by highquality IT services.

Publications available within the ITIL framework are:

- Service Support
- Service Delivery
- Security Management
- ICT Infrastructure Management
- Applications Management
- The Business Perspective

Together they support implementation, assessment and development of IT-services.

When you study a publication it will consist of several sub-areas that in turn, depending on what sub-area you are looking at, can cover some of following sections: Concept description, process description, activities, cost/benefit issues, proposal for review & monitoring and interface with other sub-areas within ITIL. For some sub-areas other sections have been defined to support the design of how to deliver high quality services.

In this study we have focused on Service Support and Service Delivery to identify how it can be combined with COBIT and ISO/IEC 17799:2000.

## COBIT

### *Control Objectives for Information and related Technology*

The third edition that is currently available was issued by the IT Governance Institute.

Goal:

“The COBIT Mission: To research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance profession”

COBIT is based on four domains described in 6 different publications. For each domain, sub-domains have been defined to describe requirements and tools to monitor the IT-process. The domains cover:

- Planning and organisation
- Acquisition and implementation
- Delivery and support
- Monitoring

The sub-domains that have been defined will provide you with guidance to manage the IT-process. It covers issues like Critical Success Factors (CSF), Key Performance Indicators (KPI), Key Goal Indicators (KGI) and Maturity Models (CMM).

The framework can be approached from three vantage points, described as dimensions in a cube that consists of IT-processes (domains, processes, activities), IT-resources (people, applications/systems, technology, facilities, data) and Information Criteria (quality, fiduciary, security).

Publications currently available cover COBIT Framework, COBIT Executive Summary, COBIT Management Guidelines, COBIT Control Objectives, COBIT Audit Guidelines and COBIT Implementation Tool Set. Additional publications have also been issued for COBIT Security Baseline, COBIT Quickstart and IT Governance Implementation Guide.

In this study we have focused on Management Guidelines, Control Objectives and Audit Guidelines to identify how it can be combined with ITIL and ISO/IEC 17799:2000.

## ISO/IEC 17799:2000

### *The Code of Practice for Information Security Management*

Is an international standard, based on BS 7799-1. The standard consists of two parts where the first is an ISO standard covering “should” requirements while the second part with “must” requirements still not has been approved as an ISO standard.

#### Scope:

ISO/IEC 17799:2000 provides information to parties responsible for implementing information security within an organization. It can be seen as a basis for developing security standards and management practices within an organization to improve reliability on information security in interorganizational relationships

The standard is divided into 10 sections, describing controls and activities that “must” or “should” be implemented to achieve a desired level of security. The sections covered are:

1. Security policy
2. Security organization
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

As a starting point information security has been defined as the preservation of

- a) *Confidentiality* – ensuring that information is accessible only to those authorized to have access
- b) *Integrity* – Safeguarding the accuracy and completeness of information and processing methods
- c) *Availability* – Ensuring that authorized users have access to information and associated assets when required.

In this study we have addressed all sections within ISO/IEC 17799:2000 to identify how it can be combined with ITIL and COBIT.

## Combining standards at a high level

With the IT-processes described in ITIL we have identified following correspondence in COBIT and ISO/IEC17799:2000. As a definition for correspondence we have used:

- Primary: Sub-processes or sections correspond to a high extent.
- Secondary: Sub-processes or sections correspond to some extent.

### ITIL – COBIT

#### *Service Support*

ITIL	COBIT Primary	COBIT Secondary
Service Desk	DS8 Assist and Advise Customers	AI4 Develop and Maintain Procedures DS7 Educate and Train Users
Incident Management	DS10 Manage Problems and Incidents	
Problem Management	DS10 Manage Problems and Incidents	DS8 Assist and Advise Customers
Configuration Management	DS9 Manage the Configuration	AI6 Manage Changes DS10 Manage Problems and Incidents
Change Management	AI6 Manage Changes	AI3 Acquire and Maintain Technology Infrastructure DS9 Manage the Configuration
Release Management		AI6 Manage Changes DS9 Manage the Configuration

#### *Service Delivery*

ITIL	COBIT Primary	COBIT Secondary
Service Level Agreement	DS1 Define and Manage Service Levels	AI4 Develop and Maintain Procedures DS2 Manage Third-party Services DS4 Ensure Continuous Service DS6 Identify and Allocate Costs M3 Obtain Independent Assurance
Financial Management for IT Services		M2 Monitor the Processes
Capacity Management	DS3 Manage Performance and Capacity	
IT Service Continuity Management	DS4 Ensure Continuous Service	AI6 Manage Changes
Availability Management	DS3 Manage Performance and Capacity	AI2 Acquire and Maintain Application Software

## ITIL – ISO/IEC 17799:2000

### *Service Support*

<b>ITIL</b>	<b>ISO/IEC 17799:2000 Primary</b>	<b>ISO/IEC 17799:2000 Secondary</b>
Service Desk		6.3.2 Reporting security weaknesses
Incident Management	8.1.3 Incident management procedures	6.3 Responding to security incidents and malfunctions
Problem Management		
Configuration Management		
Change Management	10.5.1 Change control procedures	4.2.2 Security requirements in third party contracts 8.1.2 Operational change control 8.3.1 Controls against malicious software
Release Management		10.4.1 Control of operational software 10.5.2 Technical review of operating system changes

### *Service Delivery*

<b>ITIL</b>	<b>ISO/IEC 17799:2000 Primary</b>	<b>ISO/IEC 17799:2000 Secondary</b>
Service Level Agreement		4.2.2 Security requirements in third party contracts
Financial Management for IT Services		
Capacity Management	8.2.1 Capacity planning	8.2.2 System planning and acceptance
IT Service Continuity Management	11 Business continuity management	
Availability Management		4.3.1 Security requirements in outsourcing contracts 8.2 System planning and acceptance 8.5.1 Network controls 8.7.4 Security of electronic mail 9.5.5 Use of system utilities 12.1.7.3 Quality and completeness of evidence

## Combining standards at an intermediate level

For each IT-process within ITIL we have chosen two sub-processes, Change Management (Service Support) and Configuration Management (Service Delivery). Within these sub-processes we have done a detailed assessment to describe what sections that may be combined with each other.

### Change Management

Following sections within ITIL, COBIT and ISO 17799:2000 may be combined for Change Management.

#### *ITIL*

Basic concepts:	<ul style="list-style-type: none"> <li>• Basic Change Management procedures</li> <li>• Request for Change (RFC)</li> <li>• Change Advisory Board (CAB)</li> </ul>
Activities	<ul style="list-style-type: none"> <li>• Planning the implementation of operational processes</li> <li>• Change logging and filtering</li> <li>• Allocation of priorities</li> <li>• Change categorisation</li> <li>• CAB meetings</li> <li>• Impact and resource assessment</li> <li>• Change approval</li> <li>• Change scheduling</li> <li>• Change building, testing and implementation</li> <li>• Urgent changes</li> <li>• Urgent changes building, testing and implementation</li> <li>• Change review</li> <li>• Reviewing the Change Management process for efficiency and effectiveness</li> <li>• Roles and responsibilities</li> </ul>
Cost/Benefit:	<ul style="list-style-type: none"> <li>• Costs</li> <li>• Benefit</li> <li>• Possible problems</li> </ul>
Planning for implementation	<ul style="list-style-type: none"> <li>• Designating the Change Manager role</li> <li>• Deciding on a Change Management system</li> <li>• Planning system reviews</li> <li>• Implementation planning</li> <li>• Guidance</li> </ul>

## **COBIT**

Control objectives - Primary:	AI6 Manage Change 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
Control objectives - Secondary:	AI3 Acquire and maintain technology infrastructure 3.1 System Software Change Controls DS9 Manage the Configuration 9.1 Configuration Recording
Management Guidelines	AI6 Manage Change <ul style="list-style-type: none"> <li>• Critical Success Factors</li> <li>• Key Goal Indicators</li> <li>• Key Performance Indicators</li> <li>• Maturity Models</li> </ul>
Audit Guidelines - Primary:	AI6 Manage Change 1 Change Request Initiation and Control 2 Impact Assessment 3 Control of Changes 4 Emergency Changes 5 Documentation and Procedures 6 Authorised Maintenance 7 Software Release Policy 8 Distribution of Software
Audit Guidelines - Secondary:	AI3 Acquire and maintain technology infrastructure 6 System Software Change Controls DS9 Manage the Configuration 1 Configuration Recording

## **ISO/IEC 17799:2000**

Security requirements - Primary:	10.5.1 Change control procedures
Security requirements - Secondary:	4.2.2 Security requirements in third party contracts 8.1.2 Operational change control 8.3.1 Controls against malicious software

## Capacity Management

Following sections within ITIL, COBIT and ISO 17799:2000 may be combined for Capacity Management.

### *ITIL*

Process description:	<ul style="list-style-type: none"> <li>• Input</li> <li>• Sub-processes: <ul style="list-style-type: none"> <li>BCM – Business Capacity Management</li> <li>SCM – Service Capacity Management</li> <li>RCM – Resource Capacity Management</li> </ul> </li> <li>• Output</li> </ul>
Activities:	<ul style="list-style-type: none"> <li>• Monitoring</li> <li>• Analysis</li> <li>• Tuning</li> <li>• Implementation</li> <li>• Storage of Capacity Management data</li> <li>• Demand Management</li> <li>• Modelling</li> <li>• Application sizing</li> <li>• Production of Capacity Plan</li> </ul>
Cost/Benefit:	<ul style="list-style-type: none"> <li>• Costs</li> <li>• Benefit</li> <li>• Possible problems</li> </ul>
Planning for implementation	<ul style="list-style-type: none"> <li>• Review what exists already</li> <li>• Planning the process</li> <li>• Implementation of the process</li> </ul>

### *COBIT*

Control objectives - Primary source:	DS3 Manage Performance and Capacity 3.1 Availability and Performance Requirements 3.2 Availability Plan 3.3 Monitoring and Reporting 3.4 Modeling Tools 3.5 Proactive Performance Management 3.6 Workload Forecasting 3.7 Capacity Management of Resources 3.8 Resources Availability 3 9 Resources Schedule
Management Guidelines	DS 3 Manage Performance and Capacity <ul style="list-style-type: none"> <li>• Critical Success Factors</li> <li>• Key Goal Indicators</li> <li>• Key Performance Indicators</li> <li>• Maturity Models</li> </ul>

Audit Guidelines - Primary:	DS3 Acquire and maintain technology infrastructure 1 Availability and Performance Requirements 2 Availability Plan 3 Monitoring and Reporting 4 Modeling Tools 5 Proactive Performance Management 6 Workload Forecasting 7 Capacity Management of Resources 8 Resources Availability 9 Resources Schedule
--------------------------------	--

### ***ISO/IEC 17799:2000***

Security requirements Primary:	8.2.1 Capacity planning
Security requirements Secondary:	8.2.2 System acceptance

## **References**

### ***ITIL***

- ITIL Service Delivery, OCG
- ITIL Service Support, OCG

### ***COBIT***

- COBIT 3<sup>rd</sup> Edition Management Guidelines, ITGovernance Institute
- COBIT 3<sup>rd</sup> Edition Control Objectives, ITGovernance Institute
- COBIT 3<sup>rd</sup> Edition Audit Guidelines, ITGovernance Institute

### ***ISO/IEC 17799:2000***

- Information security management – Part 1 Code of practice for information security management

### ***Other sources***

- ITIL Security Management, OCG
- COBIT Security Baseline, ITGovernance Institute
- COBIT mapping - Overview of International IT Guidance, ITGovernance Institute
- BS7799 Information security management – Part 2 Specification for information security management systems