

# Keynote

## COBIT Library

### Background and History

The Control Objectives for Information and related Technology (COBIT) is a framework for IT management created by the Information Systems Audit and Control Association (ISACA). ISACA is a large international organisation which currently has more than 86,000 members in over 160 countries. In addition, CISA, the professional qualification offered by ISACA is the most highly regarded professional qualification for IT auditing throughout the world.

COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

COBIT was designed by IT auditors for use by IT auditors.

COBIT is widely used throughout the world and has been translated into French, Spanish, German, Italian, Russian, Hungarian, Japanese and Korean. The Securities and Exchange Commission considers COBIT an acceptable control framework standard for governance, security, and internal control best practices for SOX compliance, and it has been adopted by the large accountancy firms. COBIT is the de facto standard for auditing IT environments.

### Structure

COBIT is a process model that subdivides IT into four domains in line with four areas of responsibility: plan; build; run and monitor, thereby providing an end-to-end view of IT. The domains are divided into 34 processes that are further divided into 210 detailed control objectives. These are supported by detailed risks, control practices and suggested audit tests. Considerable time and money can be saved through using the framework in the design of the audit scope and associated work programmes.

### Risk Controls and Audit Tests

A detailed review of the COBIT risks, controls and audit tests reveals that there are no links between risks and controls or between controls and audit tests. These are only linked to the control objective themselves. Indeed, if we try to create the links we will find that some risks do not map well to any of the defined controls and some of the tests do not map well to any of the controls. Also, that some of the risks do not have any obvious defined controls and some of the controls do not have any obvious defined audit tests.

We have addressed this linking problem within PAWS by creating a single risk for each of the 210 control objectives. This is either the risk considered most appropriate or formed as a composite risk containing a number of the individual risks. The controls and audit tests are then linked to the PAWS COBIT risks.

A library containing the COBIT risks, controls and audit tests has been created for use within PAWS. The PAWS COBIT Library contains the entire domain, process and control objective framework with over 1,000 control practices and 1,500 audit tests. The power of COBIT is available from within PAWS. The auditor can select any control process and the audit programme will be automatically populated with the relevant risks, controls and audit tests.

# Keynote

## Implementation Guidance

Most audit departments will already have defined an IT audit universe which will be recognised by the auditors, auditees and audit committee. When implementing the COBIT framework we should not disregard this work. We should take the universe and then use the COBIT framework to define the scope for the individual audits. This can be achieved by mapping the COBIT framework to the audit entities.

An initial review of a typical IT audit universe would identify a number of audits which would appear to map directly to the COBIT framework. For example: the audit entities operating systems, continuity planning and change management would appear to map directly to the COBIT processes 'DS5 Ensure System Security', 'DS4 Ensure Continuity of Service' and 'A16 Manage Changes'. However on further consideration we would discover that a number of other processes and objectives are also relevant to these audits. Consider for example an operating system review, this could also include 'DS3 Manage Performance and Capacity', 'A16 Manage Changes', 'DS9 Manage the Configuration', 'DS11 Manage Data', 'DS12 Manage the Physical Environment', 'PO2 Define the Information Architecture', and even specific control objectives from 'PO4 Define the IT Processes, Organisation and Relationships' in the consideration of roles and responsibilities, segregation of duties, and reliance on key IT personnel. When we have defined all of our audit entities in terms of the relevant COBIT processes and control objectives, we will see that one IT audit may contain many COBIT objectives and processes and conversely that each COBIT objective and process may form part of many audits. There is a many to many relationship between audit entities and COBIT objectives and processes.

When these audit entities are entered into PAWS we will have the entire IT audit universe available for the IT auditor. Now when we select an IT audit in PAWS it will automatically be populated with the appropriate risks, controls and audit tests from COBIT. Think of the time you will have saved in the planning phase of your audit. You will also be using an internationally recognised approach and one that will be familiar to the external auditors.

## How Pentana Can Help

Pentana can provide you with a standard PAWS library containing all the COBIT objectives, risks, controls and sample tests. It is distributed as a SQL script that adds the library items into your standard PAWS application. The library is sold for a one-time fee under license from ISACA. New COBIT versions will be made available at a discount to existing users.

Pentana can also provide consulting help in mapping your own IT audit universe to COBIT. When all of the audit entities are scoped in terms of COBIT we would produce a report of the audit entities with associated COBIT objectives and processes. We would provide a report of any objectives or processes that were not covered by any audit and suggest changes to the scope of existing audits or the addition of new audits to fill the gaps. We would provide you with a COBIT compliant audit universe specific to your organisation.

# Keynote

We can help in the design of reports to show audit opinions based on COBIT objectives and processes. We can design reports for management that present clearly and concisely areas of deficiency against the COBIT framework, and highlight improvements or deterioration over time. Management would be able to quickly focus on the areas of most concern.