

CobiT - A Practical Toolkit for IT Governance

Why IT Governance?

IT governance can be defined as 'a structure of relationships and processes to direct and control the enterprise in order to achieve the goals of a business by adding value while balancing risk versus return over IT and its processes'.

For many organisations, information and the technology that supports it represent their most valuable assets. Moreover, in today's competitive and rapidly changing business environment, management requires increased quality, functionality and ease of use from their IT, delivered faster and faster, constantly available and at lower costs than ever before.

The benefits of technology are in no doubt. However, to be successful, organisations have to understand and manage the risks associated with implementing new technologies. Fortunately, help is at hand in the form of CobiT®.

What is CobiT?

Control Objectives for Information and related Technology (CobiT) bridges the gaps between business risks, control needs and technical issues. It presents IT activities in a manageable and logical structure, and documents good practice across this structure. CobiT's 'good practices' are the consensus of the world's experts - they will help optimise information investments and provide a benchmark to be judged against when things do go wrong - and indeed to prevent things from going wrong in the first place. CobiT is independent of the technical IT platforms adopted in an organisation.

CobiT's main theme is business orientation. It provides comprehensive guidance for management and business process owners and is firmly based in business objectives.

CobiT is designed to help three distinct audiences:

Management, who need to balance risk and control investment in an often unpredictable IT environment.

Users, who need to obtain assurance on the security and controls of the IT services upon which they

depend to deliver their products and services to internal and external customers.

Auditors, who can use it to substantiate their opinions and/or provide advice to management on internal controls.

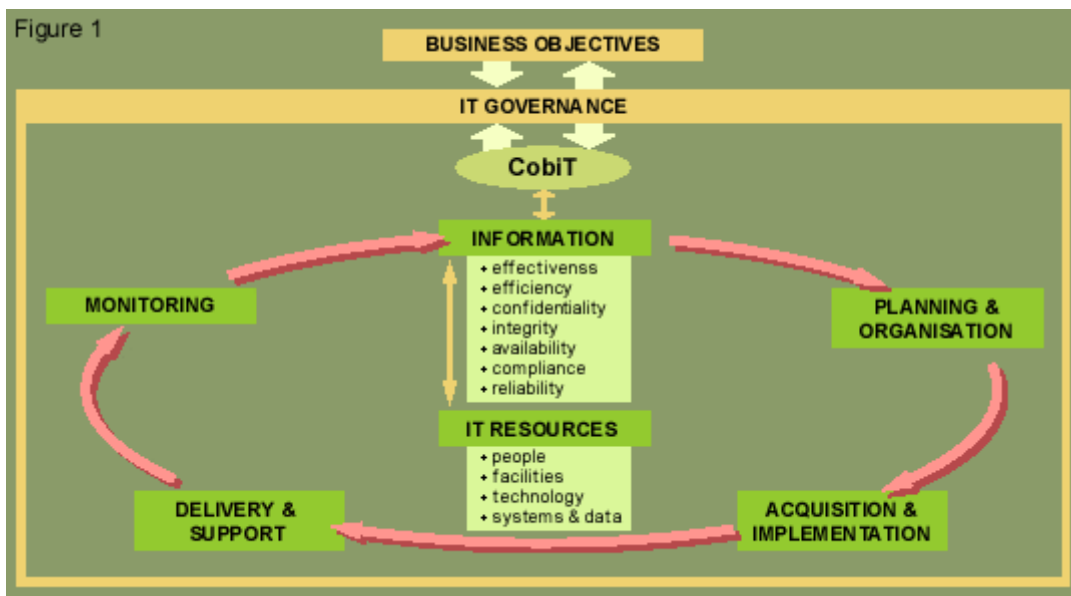
CobiT starts by grouping IT processes into four broad groups:

Planning and Organisation.

Acquisition and Implementation.

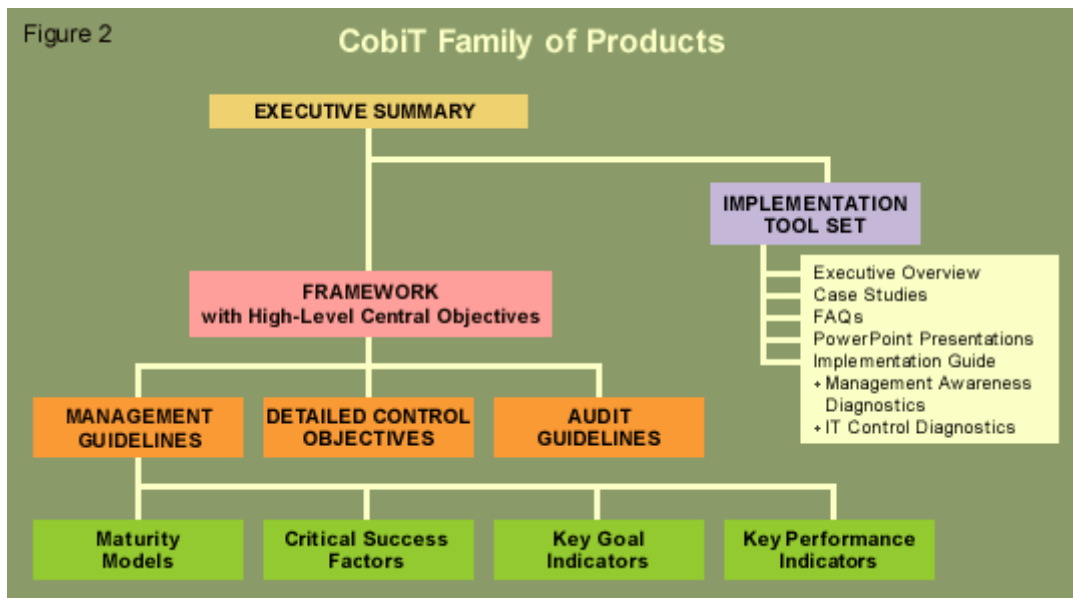
Delivery and Support.

Monitoring.



It then defines high-level Business Control Objectives for the processes, clearly linked to business objectives, and supports these with Detailed Control Objectives to provide management assurance and/or advice for improvement. The CobiT framework is illustrated in Figure 1 above.

The Control Objectives are supported by Audit Guidelines which enable auditors and managers to review specific IT processes against these in order to help assure management where controls are sufficient, or to advise management where processes need to be improved. The third main component is CobiT's Management Guidelines. CobiT's components are shown in Figure 2 below.



CobiT Management Guidelines

Managers in every organisation need to understand the status of their own IT systems and decide what security and control they should provide. Neither aspect of this issue - understanding of and deciding on the required level of control - is straightforward. It is far from easy for managers to obtain an objective measure of an organisation's own level of control and risk - what should be measured and how? As well as the need to measure where an organisation is, there is a need for continuous improvement in IT security and control, and for a management toolkit to monitor this improvement. It is equally difficult to decide what the right level of security and control is. Senior managers are frequently asked to consider a business case for expenditure to improve their control over, and the security of, their organisation's information infrastructure. While few would argue that this is not a good thing, all must occasionally ask themselves: 'How far should we go, and is the cost justified by the benefit?'

This question can be answered by using the CobiT Management Guidelines which define the following:

Benchmarks for IT control practices (expressed as Maturity Models).

Performance and key goal indicators of the IT processes for their outcome and their performance.

Critical success factors for getting these processes under control.

Development of CobiT

First published by the Information Systems Audit and Control Foundation in 1996, CobiT is now in its third edition. The second edition, in 1998, broadened the resource base on which the control objectives are based and added a practical implementation toolkit. The current edition marked a transfer to the IT Governance Institute and, with the addition of the management guidelines, from the field of IT auditing into that of corporate governance.

The research and publication activities were supported by significant grants from PriceWaterhouseCoopers, donations from ISACA chapters and members worldwide, research material from the European Security Forum (ESF) and quality assurance and other support from The Gartner Group.

CobiT is a genuine distillation of global best practice from a wide range of sources including:

Technical standards from ISO, EDIFACT, etc.

Codes of Conduct issued by the Council of Europe, OECD, ISACA, etc.

Qualification criteria for IT systems and processes: ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria, etc.

Professional standards for internal control and auditing: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, etc.

Industry practices and requirements from industry forums (ESF, I4) and government-sponsored platforms (IBAG, NIST, DTI), etc.

Emerging industry-specific requirements from banking, electronic commerce, and IT manufacturing.

Benefits of CobiT

In an age of increasing electronic business and technology dependence, organisations will have to demonstrably attain increasing levels of security and control. Every organisation must understand its own performance and must measure its progress. Benchmarking and measuring progress against peers and the enterprise strategy is one way of achieving a competitive level of IT security and control. The CobiT Management Guidelines provide management not only with pragmatic guidance via these maturity models, but also critical success factors and suggested performance

measures to answer the perpetual question: 'What is the right level of control for my IT such that it supports my enterprise objectives?'

CobiT Management Guidelines focus on performance management by using the principles of the Balanced Business Scorecard. Their Key Goal Indicators identify and measure outcomes of processes, and Key Performance Indicators to assess how well processes are performing. IT is the major enabler of business. Hence, the relationship between business goals and measures, and IT goals and measures is very important.

CobiT Management Tools

MATURITY MODELS are used for control over IT processes and provide a method of scoring so that an organisation can grade itself from non-existent to optimised (from 0 to 5). This approach has been derived from the Software Engineering Institute's Maturity Model for software development capability. Against these levels, developed for each of CobiT's 34 IT processes, management can map:

- Where the organisation is today
- The current status of (best-in-class in) the industry
- The current status of international standards
- Where the organisation wants to be.

CRITICAL SUCCESS FACTORS define the most important issues or actions for management to achieve control over and within its IT processes. They identify the most important things management must do, strategically, technically, organisationally or procedurally.

KEY GOAL INDICATORS define measures that tell management - after the fact - whether an IT process has achieved its business requirements, usually expressed in terms of the following information criteria:

- Availability of information needed to support the business needs
- Absence of integrity and confidentiality risks
- Cost-efficiency of processes and operations
- Confirmation of reliability, effectiveness and compliance.

KEY PERFORMANCE INDICATORS define measures to determine how well the IT process is performing in enabling the goal to be reached; are lead indicators of whether a goal will likely be reached or not; and are good indicators of capabilities, practices and skills.

In CobiT's Management Guidelines, the Critical Success Factors, Key Goal Indicators and Key Performance Indicators are short and focused, complementing the high-level control guidance provided by the CobiT Framework which states that IT enables the business by delivering the information the business needs.

Does CobiT Work in the Real World?

Definitely - here are just a few examples.

Philips International BV uses CobiT as part of a company-wide quality improvement programme.

Philips has developed a scoring process that uses CobiT's maturity models to reflect its own specific organisational and process needs. Scoring results are also used to submit an annual Statement on Business Controls.

The CEDEL Group is a Luxembourg based clearing organisation founded by a number of the world's major financial institutions to minimise risk in the settlement of cross-border securities trading, particularly in the Eurobond market. CEDEL's Michael P. Ras says 'A new, strong focus on practical business and efficiency priorities was the most notable difference when we implemented CobiT. I encourage colleagues to take a close look at CobiT with their management. CobiT is a highly flexible and credible approach to maintaining and improving a controlled environment'.

Eric Guldentops of SWIFT, the Brussels-based global co-operative for secure interbank financial messaging services and interface software found CobiT to be immediately useful: 'When looking for input on defining the mission and objectives for a new systems planning group, the Chief Information Officer came to me and said, 'Give me your CobiT Detailed Objectives to help do this!' I only had to point him to the planning and organisation sections. He had asked me for input on this mission and objectives previously, so why hadn't I thought of this myself?'

The Executive Directions advisory service of the META Group have researched CobiT. Vice president Al Passori says 'We believe by 2002-03, more than 30-40 per cent of Global 2000 companies deploying new technologies and entering new markets with e-products and services will have adopted a CobiT-like risk assessment and balanced risk/reward reporting process. All CIOs should

adopt a CobiT risk management process model and identify, train and support the needed implementation staff.' The resulting report entitled 'Risk Without Remorse', can be accessed online and downloaded from the ISACA web site (see below for details).

Finding out More

Much of CobiT is an open standard, available as a free download from the IT Governance Institute's website www.itgovernance.org or from the Information Systems Audit & Control Association www.isaca.org

For convenience, the full CobiT product, comprising all the components is available for sale in printed form, complete with a fully searchable CD-ROM.

To purchase CobiT, visit www.isaca.org and follow the links to the bookstore. Delivery from the US is usually within a week.

Key Points

Effective corporate governance and risk management requires effective IT governance and risk management.

Managers' skill and energy need to be concentrated on their business, and they need help with risk managing the IT on which their businesses depend.

CobiT is designed to help management to balance risk and control investment in an IT environment which is often unpredictable.

CobiT addresses (through its Management Guidelines) concerns about performance measurement, IT control profiling, awareness and benchmarking.

It is a genuine distillation of global best practice from a wide range of sources and experts.

CobiT answers the perpetual question: 'What is the right level of control for my IT such that it supports my enterprise objectives?'

CobiT is already used to support both governance and IS auditing activities in many successful enterprises, within both private and public sectors, all over the world.

(Source: IT Adviser)