COBIT® MAPPING

Overview of International IT Guidance, 2nd Edition

IT GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

IT Governance Institute®

The IT Governance Institute (ITGI™) (*www.itgi.org*) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities. ITGI offers original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclaimer

The IT Governance Institute (the "Owner") and the author have designed and created this publication, titled *COBIT Mapping: Overview of International IT Guidance, 2nd Edition* (the "Work"), primarily as an educational resource for control professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, control professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

Disclosure

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

ISBN 1-933284-31-5
COBIT Mapping: Overview of International IT Guidance, 2nd Edition
Printed in the United States of America

ACKNOWLEDGEMENTS

IT Governance Institute wishes to recognise:

The Researcher

Jimmy Heschl, CISA, CISM

Additional Contributors

Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Stuart Macgregor, Real IRM Solutions, South Africa

The ITGI Board of Trustees

The ITGI Committee

Expert Reviewers

John Ho Chi, CISA, CISM, CBCP, CFE, Ernst & Young, Singapore
Avinash W. Kadam, CISA, CISM, CISSP, CBCP, GSEC, Director, MIEL e-Security Pvt. Ltd., India
Kamal Khan, CISA, Rabobank, London
Debra Mallette, CISA, CSSBB, Kaiser Permanente IT, USA
Ernst J. Oud, CISA, Deloitte Enterprise Risk Services, The Netherlands
Roberto Hernández Rojas, CISA, BS 7799 Lead Auditor, Grupo Scanda, Mexico
Ana Cecilia Pérez Rosales, CISA, Scitum, Mexico City
Lily M. Shue, CISA, CISM, CCP, LMS Associates LLC, USA
Phil Webster, CISA, ACA, Progressive Enterprises Limited, New Zealand

The ITGI Affiliates and Sponsors

ISACA chapters
Commonwealth Association for Corporate Governance
BindView Corporation
CA

Table of Contents

1. Purpose and Scheme for Classification of the Guidance

In 1996, the Information Systems Audit and Control Foundation® created *Control Objectives for Information and related Technology* (CobiT®). The second edition, containing enhancements and additional content, followed in 1998. In 1998, the IT Governance Institute (ITGI) was founded for the purpose of conducting research into the increasingly important area of IT governance, with a special focus on the CobiT framework, processes, control objectives and maturity models. In time, the Information Systems Audit and Control Foundation and ITGI became one entity, and that organisation issued a third edition of CobiT in 2000, followed by version 4.0 in 2005.

The CobiT framework enables CIOs to help stakeholders better understand IT processes and services and easily integrate different standards. For their part, stakeholders can use CobiT as an instrument to govern the information provided by IT to support business processes.

CobiT does not operate in a vacuum. Today, several other standards and collections of best practices are available that prescribe how to manage specific facets of the IT function within organisations. Guidance has been published by international standards organisations as well as several private or partially private organisations. However, no common framework has been available for comparing these various guidance documents. This publication provides a framework to make those comparisons and, as a result, to coherently drive process compliance and improvement. When detailed comparisons can be made, management of the IT function can be enhanced and, consequently, better decisions can be made.

Given the importance of IT within enterprises and the plethora of guidance on its governance, management and control, it is clear that there is a need for a reference that can answer questions such as:
- What should be defined?
- What is an appropriate level of detail?
- What should be measured?
- What should be automated?
- What is best practice?
- Is there a certification available?

Although many of these questions can be addressed using the freely available CobiT guidance, several have remained unresolved, until now. This project addresses the gaps by undertaking to map the most important and commonly used standards[1] and guidance to the CobiT processes and control objectives.

This publication is an update to the first volume of the CobiT mapping series, released in 2004. It focuses on the business drivers for implementing the guidance, as well as the risks of non-compliance with the guidance. Further, it contains a classification of the guidance publications, a short overview of their content, and an explanation of how they align or map to CobiT.

Note, this publication does not contain the result of detailed mappings to the CobiT framework. Those will follow in the near future. A detailed mapping of CobiT and ISO/IEC 17799:2000 is already available at *www.isaca.org*. Other planned mappings include ISO 17799:2005, PRINCE2®, PMBOK©, CMM®, ITIL®, FIPS PUB 200, *IT Baseline Protection Manua*l and ISO 2000.

This research project is limited to the publications in the following list. The list is not intended to be exhaustive; there are other documents and information sources available. The following is a brief overview of the guidance discussed in this research:
- **CobiT**—Originally released as an IT process and control framework linking IT to business requirements, it was initially used mainly by the assurance community in conjunction with business and IT process owners. With the addition of *Management Guidelines* in 1998, CobiT is now used more and more as a framework for IT governance, providing management tools such as metrics and maturity models to complement the control framework.
- **COSO** *Internal Control—Integrated Framework* defines a framework that initiates an integrated process of internal control.
- **ITIL**—The IT Infrastructure Library® is a collection of best practices in IT service management. It is focused on the service processes of IT and considers the central role of the user.
- **ISO/IEC 17799:2005**—The *Code of Practice for Information Security Management* is an international standard based on BS 7799-1/ISO/IEC 17799:2000. It is presented as best practice for implementing information security management.
- **FIPS PUB 200**—The *Minimum Security Requirements for Federal Information and Information Systems* is applicable to federal government organisations in the US. It defines categories for systems and guidelines for information security controls.

[1] The term ‘standard’ is used in this document to encompass guidance publications.

- **ISO/IEC TR 13335**—The technical report *Guidelines for the Management of IT Security* contains information on IT security management not only from the planning perspective, but also from the implementation and maintenance perspectives.
- **ISO/IEC 15408:2005**—*Security Techniques—Evaluation Criteria for IT Security* is used as a reference to evaluate and certify the security of IT products and services.
- **PRINCE2**—Projects in Controlled Environments (PRINCE) provides a structured method for effective project management, published in a single document, *Managing Successful Projects With PRINCE2*.
- **PMBOK**— *A Guide to the Project Management Body of Knowledge* (PMBOK© Guide) is described as 'the sum of knowledge within the profession of project management'. It is an American National Standard, ANSI/PMI 99-001-2004.
- **TickIT**—It provides a scheme for the certification of the software quality management system. It intends to improve the effectiveness of the quality management system and targets customers, suppliers and assurance professionals.
- **CMMI**—*Capability Maturity Model Integration*® combines three source models—Capability Maturity Model for Software (SW-CMM) v2.0 draft C, Electronic Industries Alliance Interim Standard (EIA/IS) 731 and Integrated Product Development Capability Maturity Model (IPD-CMM) v0.98—into a single improvement framework for use by organisations pursuing enterprisewide process improvement.
- **TOGAF 8.1**—It provides a detailed method and a set of supporting tools for developing an enterprise architecture.
- ***IT Baseline Protection Manual***—It provides IT security standard safeguards.
- **NIST 800-14**—The US National Institute of Standards and Technology special publication *Generally Accepted Principles and Practices for Securing Information Technology Systems* contains information for establishing a comprehensive IT security programme.

SCHEME FOR CLASSIFICATION OF THE GUIDANCE

To enable a proper comparison of each standard or guidance publication, a scheme for classification to be used in evaluating all the guidance was defined as follows.

Document Taxonomy

This section lists the type of guidance, such as an international or a national standard or a collection of best practices.

Issuer

The issuer refers to the issuing body of the paper and lists the organisation standing behind the guidance and keeping the document up to date.

Goal(s) of the Standard or Guidance Publication

This section lists the primary goals of the document. For example, the guidance may focus on information security management, baseline protection, guidance for software development or management of tactical issues.

Business Drivers for Implementing the Guidance, Including Typical Situations

The business case for implementing the guidance and the typical situations indicating implementation of the guidance are listed here.

Related Risks of Non-compliance

Some of the business risks of not implementing the guidance are considered in this section.

Target Audience

This section discusses whether there is a special target audience for the guidance. For example, are public organisations, assurance professionals, security management or general IT professionals the target audience?

Timeliness

Timeliness considers whether the guidance is up to date and how frequently it is revised.

Certification Opportunities

This section considers the certification path, what can be certified and the certification body, if applicable.

Circulation

Circulation considers whether the guidance is used internationally or limited to a certain region, and whether information on usage is available.

Completeness

The completeness is classified using two dimensions:

- **Vertical**—The detail of the guidelines in terms of technical or operational profundity. The higher the level of detail, the higher the document is classified.
- **Horizontal**—Guidance completeness, e.g., the extent to which COBIT is addressed by the guidance. The higher the level of detail, the higher the document is classified.

Availability

Availability addresses how and where the information can be obtained.

COBIT Processes Addressed

A high-level mapping of COBIT processes addressed by the respective guidance is presented. The COBIT processes are described in the section on COBIT in this publication. Those areas of COBIT that are frequently addressed are colored blue.

Information Criteria Addressed

This section addresses which of the following COBIT information criteria are referenced within the particular guidance:

- Efficiency
- Effectiveness
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

IT Resources Concerned

This section focuses on which of the COBIT IT resources are addressed by the respective guidance:

- Applications
- Information
- Infrastructure
- People

Description of the Guidance and Its Content

The fundamental concepts covered by the guidance are discussed.

Further References

This section lists sources of additional information.

2. COBIT

For purposes of this document, COBIT is the framework to which the other guidance is compared.

DOCUMENT TAXONOMY

COBIT represents a collection of documents that can be classified as generally accepted best practice for IT governance, control and assurance.

ISSUER

The first edition of COBIT was issued by the Information Systems Audit and Control Foundation® (ISACF®) in 1996. In 1998, the second edition was published with additional control objectives and the *Implementation Tool Set*. The third edition was issued by ITGI in 2000, and included the *Management Guidelines* and several new detailed control objectives. In 2005, ITGI finalised a complete rework of the COBIT content and published the current version, COBIT® 4.0.

GOAL OF THE PUBLICATION

'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 professionals'.[2]

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE, INCLUDING TYPICAL SITUATIONS

COBIT is usually implemented subject to one or more of the following business cases:

- There is a need for IT governance.
- Services delivered by IT are to be aligned with business goals.
- IT processes are to be standardised/automated.
- A framework for overall IT processes is needed.
- Processes are to be unified.
- There is a need for a framework for a quality management system.
- A structured audit approach is to be defined.
- Mergers and acquisitions are occurring.
- IT cost-control initiatives are desired.
- Part or all of the IT function is to be outsourced.
- Compliance with external requirements (e.g., regulators, organisations or third parties) is of concern.

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing COBIT include:

- Misaligned IT services, divergence
- Weak support of business goals due to misalignment
- Wasted opportunities due to misalignment
- Persistence of the perception of IT as a black box
- Shortfall between management's measurements and expectations
- Know-how tied to key individuals, not to the organisation
- Excessive IT cost and overhead
- Erroneous investment decisions and projections
- Dissatisfaction of business users with IT services supplied

[2] IT Governance Institute, COBIT 3rd Edition, 2000

TARGET AUDIENCE

All types of organisations, public and private companies, and external assurance professionals form the relevant target group for COBIT. Within organisations, three levels are addressed: management, IT users and professionals, and assurance professionals.

TIMELINESS

The core content of COBIT was updated in 2005, resulting in the December 2005 release of COBIT 4.0. Research addressed components of the control objectives and the management guidelines. Some specific areas that were addressed are:

- COBIT's IT governance bottom-up and top-down alignment
- COBIT and other detailed standards—Detailed mapping between COBIT and ITIL, CMM, COSO, PMBOK, ISF and ISO 17799 to enable harmonisation with those standards in language, definitions and concepts
- Key goal indicator (KGI) and key performance indicator (KPI) causal relationships analysis
- Review of the quality of the KGIs/KPIs/RACI charts—Based on the KPI/KGI causal relationship analysis, splitting critical success factors (activity goals) into 'what you need from others' and 'what you need to do yourself'
- Detailed analysis of metrics concepts—Detailed development with metrics experts to enhance the metrics concepts, building up a cascade of 'process-IT-business' metrics and defining quality criteria for metrics
- Linking of business goals, IT goals and IT processes—Detailed research into eight different industries, resulting in a more detailed insight into how COBIT processes support the achievement of specific IT goals and, by extension, business goals. Results were then generalised.
- Review of maturity model contents—Ensured consistency and quality of maturity levels between and within processes, including better definitions of maturity model attributes

The latest COBIT derivatives at the time of this publication include:

- COBIT® *Quickstart*
- COBIT Online®
- *IT Governance Implementation Guide*
- *Control Practices*
- COBIT Foundation Course™
- *IT Control Objectives for Sarbanes-Oxley*
- COBIT® *Security Baseline*
- *Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit*
- *COBIT® Mapping: Mapping ISO/IEC 17799:2000 With COBIT*

CERTIFICATION OPPORTUNITIES

COBIT's audit guidelines contain information for auditing and self-assessment against the control objectives, but there is no certification for organisations available. However, the COBIT framework is used frequently by Certified Public Accountants (CPAs) and Chartered Accountants (CAs) when performing a Statement on Auditing Standards (SAS) No. 70 Service Organisations review, Systrust certification or Sarbanes-Oxley compliance.

For certification of individuals, the COBIT Foundation Course is offered.

Non-COBIT certification is available through ISACA, ITGI's affiliate, in the form of the Certified Information Systems Auditor™ (CISA®) and Certified Information Security Manager® (CISM®) certifications.

CIRCULATION

COBIT is used worldwide. In addition to the English versions of the publications, it has been translated into Spanish, German, French and several other languages.

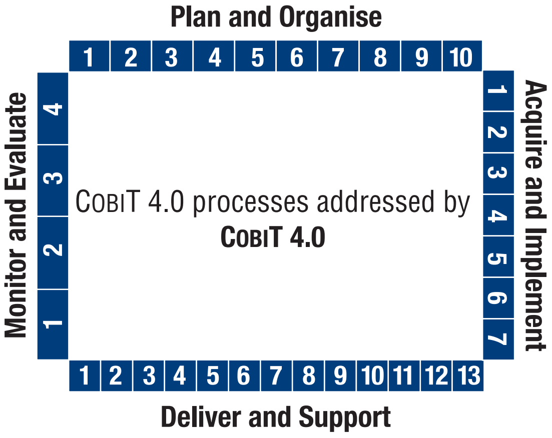
COMPLETENESS

COBIT addresses a broad spectrum of duties in IT governance and management. COBIT includes the most significant parts of IT management, including those covered by other standards. Although no technical details have been included, the necessary tasks for complying with the control objectives are self-explanatory. Therefore, it is classified as relatively high-level, aiming to be generically complete but not specific.

AVAILABILITY

COBIT 4.0 is open and readily accessible for complimentary electronic download on the ITGI and ISACA web sites, *www.itgi.org* and *www.isaca.org/cobit*. COBIT Online can be purchased at *www.isaca.org/cobitonline*. The audit guidelines are posted for complimentary download for ISACA members, and a project is in development to update them to COBIT 4.0. Alternatively, the print version of COBIT 4.0 can be purchased from the ISACA Bookstore, *www.isaca.org/bookstore*.

COBIT PROCESSES ADDRESSED



Note: The chart is not a comparison; this is COBIT itself.

INFORMATION CRITERIA ADDRESSED

	Information Criteria
+	Effectiveness
+	Efficiency
+	Confidentiality
+	Integrity
+	Availability
+	Compliance
+	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

Note: The chart is not a comparison; this is COBIT itself.

IT RESOURCES CONCERNED

IT Resources
+ Applications
+ Information
+ Infrastructure
+ People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

Note: The chart is not a comparison; this is COBIT itself.

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

Enterprise governance (the system by which organisations are governed and controlled) and IT governance (the system by which the organisation's IT is governed and controlled) are—from a COBIT point of view—highly interdependent. Enterprise governance is inadequate without IT governance and *vice versa*. IT can extend and influence the performance of the organisation, but it has to be subject to adequate governance. On the other hand, business processes require information from the IT processes, and this interrelationship has to be governed as well.

In this context, the plan-do-check-act (PDCA) cycle becomes evident. The concept of the PDCA cycle is usually used in structured problem-solving and continuous improvement processes. The PDCA cycle is also known as the Deming cycle or the Deming wheel of a continuous improvement process. Both the information need (corporate governance) and the information offer (IT governance) have to be planned with measurable and constructive indicators (plan). The information and, possibly, information systems have to be implemented, delivered and used (do). The outcome of the information delivered and used is measured against the indicators defined in the planning phase (check). Deviation is investigated and corrective action is taken (act).

Considering these interdependencies, it is apparent that the IT processes are not an end in themselves. They are a means to an end that is highly integrated with the management of business processes. The following definition is from ITGI:

> *IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.*[3]

COBIT Framework

Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimise the use of available IT resources, including applications, information, infrastructure and people. To discharge these responsibilities and achieve its objectives, management should understand the status of its enterprise architecture for IT and decide what governance and control it should provide.

COBIT provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices represent the consensus of experts. They are strongly focused on control and less on execution. They help optimise IT-enabled investments and provide a measure against which to judge when things do go wrong.

Control Objectives

COBIT provides a set of 34 high-level control objectives, one for each of the IT processes, grouped into four domains: Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

[3] ITGI, *IT Governance Implementation Guide*, 2003, p. 19

Management Guidelines

The COBIT management guidelines, now integrated into COBIT 4.0, provide a link between IT control and IT governance. They are action-oriented and generic, and they provide management specific guidance and direction for getting the enterprise's information and related processes under control, monitoring achievement of organisational goals, monitoring and improving performance within each IT process, and benchmarking organisational achievement. They help provide answers to the following typical management questions:

- How far should we go in controlling IT, and is the cost justified by the benefit?
- What are the goals and key metrics?
- Who is responsible, accountable, consulted and informed?
- What are the risks of not achieving our objectives?
- What do others do?
- How do we measure and compare the organisation's maturity to others in the industry?
- What is the organisation's strategy for improvement?

Control Practices

Control practices expand the capabilities of COBIT by providing the practitioner with an additional level of detail. The COBIT IT processes, business requirements and detailed control objectives define *what* needs to be done to implement an effective control structure. The control practices provide the more detailed *how* and *why* needed by management, service providers, end users and control professionals to implement highly specific controls based on an analysis of operational and IT risks.

Audit Guidelines

To achieve its desired goals and objectives, the enterprise must constantly and consistently audit its procedures: analyse, assess, interpret, react and implement. Audit guidelines outline and suggest actual assessment activities to be performed, corresponding to each of the 34 high-level IT control objectives, to evaluate control processes, assess compliance and substantiate the risk of control objectives not being met.

COBIT Quickstart

This special version is a baseline for many small to medium-sized enterprises (SMEs) and other entities where IT is not mission-critical or essential for survival, but it also can serve as a starting point for other enterprises in their move toward an appropriate level of control and governance of IT. For purposes of this project, SMEs have not been defined according to any financial or staffing measurement. Instead, the strategic nature of IT to the business is evaluated, a self-assessment form is presented and exceptions are reviewed. Those enterprises for which the strategic nature of IT is relatively low, that fall within certain ranges on the self-assessment and that do not have any of the exceptions that might indicate a higher level of dependence on IT are considered SMEs.

This project was undertaken in response to comments that COBIT, in its complete form, can be a bit overwhelming. Those who operate with a small IT staff often do not have the resources to implement all of COBIT. This version of COBIT constitutes a subset of the entire COBIT volume. Only those control objectives that are considered the most critical are included, so that implementation of COBIT 's fundamental principles can take place easily, effectively and relatively quickly.

COBIT Online

This online version of COBIT allows users to customise a version of COBIT that suits their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys and benchmarking. A discussion facility for sharing experiences and questions was added in 2004.

IT Governance Implementation Guide

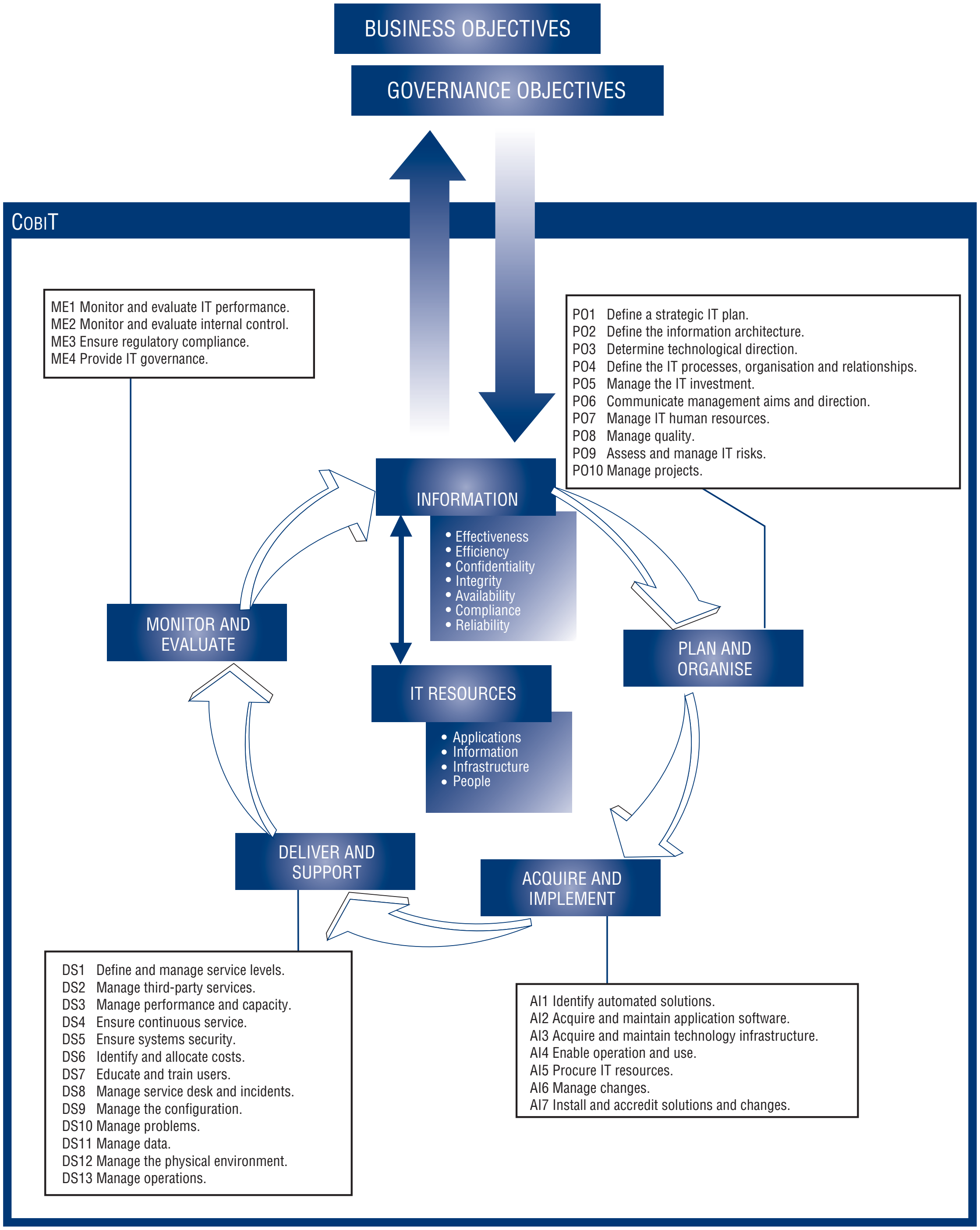
The objective of the *IT Governance Implementation Guide* is to provide readers with a methodology for implementing and improving IT governance, using COBIT. The guide is focused on a generic methodology for implementing IT governance, covering the following subjects:

- Why IT governance is important and why organisations should implement it
- The IT governance life cycle
- The COBIT framework
- How COBIT is linked to IT governance and how COBIT enables the implementation of IT governance
- The stakeholders who have an interest in IT governance
- A road map for implementing IT governance using COBIT

CobiT IT PROCESSES

The processes are grouped into four domains, as indicated in **figure 1**.

Figure 1—CobiT IT Processes Defined Within the Four Domains



ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure regulatory compliance.
ME4 Provide IT governance.

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.

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.

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 accredit solutions and changes.

Any service delivered by IT, as well as all services provided to the core processes, have to be integrated into the IT service life cycle, as indicated in **figure 1**. Plans and organisational structures already developed could be adopted, depending on the significance of each service, rather than developing a new plan for the IT service. Services are subsequently implemented, and all necessary precautions for ongoing service, delivery and monitoring are to be considered.

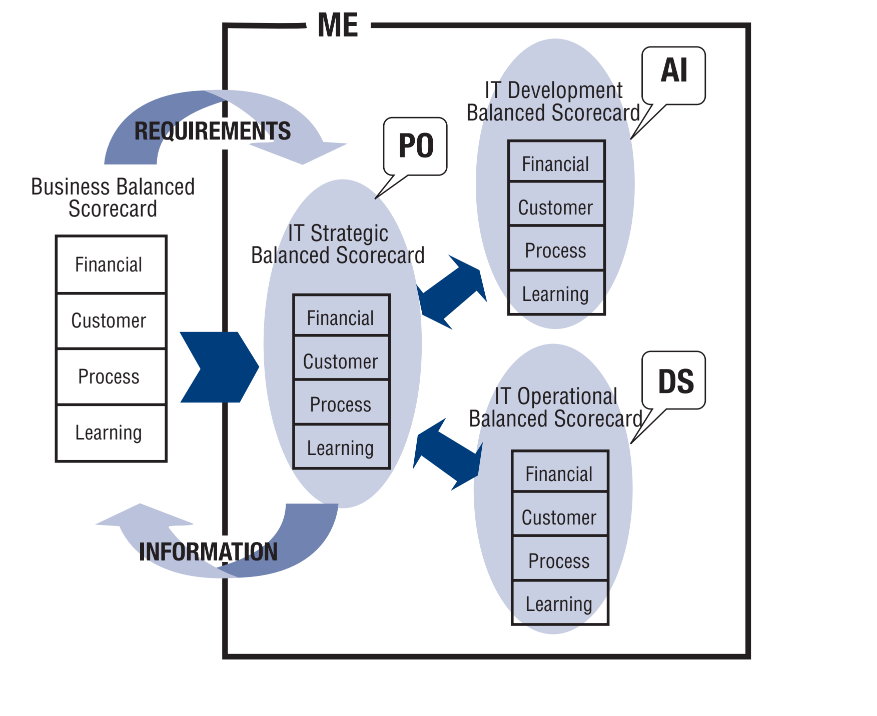
From the IT governance point of view, single services are merely in the background. The focus must be on the PDCA cycle discussed previously, for the sum of services delivered by and with IT. **Figure 2** illustrates the superordinate role of monitoring, which could be seen as a concept for a balanced scorecard.

The COBIT domains are represented in the figure by their abbreviations:
- **PO**—Plan and Organise
- **AI**—Acquire and Implement
- **DS**—Deliver and Support
- **ME**—Monitor and Evaluate

The strict top-down approach according to COBIT is depicted in **figure 3**.

Each process is described by using the following information:
- High-level control objectives
- Detailed control objectives
- Information criteria affected by the process
- IT resources used by the process
- Typical characteristics depending on the maturity level
- Activity goals
- Key performance indicators
- Key goal indicators

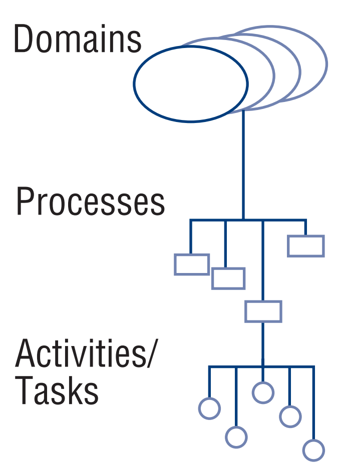
Figure 2—Balanced Scorecard



INFORMATION CRITERIA

Information delivered to the core business processes has to fulfill certain criteria, which are summarily characterised as follows:
- **Quality requirements:**
  - **Effectiveness**—Deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner
  - **Efficiency**—Concerns the provision of information through the optimal (most productive and economical) use of resources
- **Security requirements:**
  - **Confidentiality**—Concerns the protection of sensitive information from unauthorised disclosure
  - **Integrity**—Relates to the accuracy and completeness of information, as well as to its validity in accordance with business values and expectations
  - **Availability**—Relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- **Fiduciary requirements:**
  - **Compliance**—Deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria, as well as internal policies
  - **Reliability**—Relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities

Figure 3—Top-down Approach



IT RESOURCES

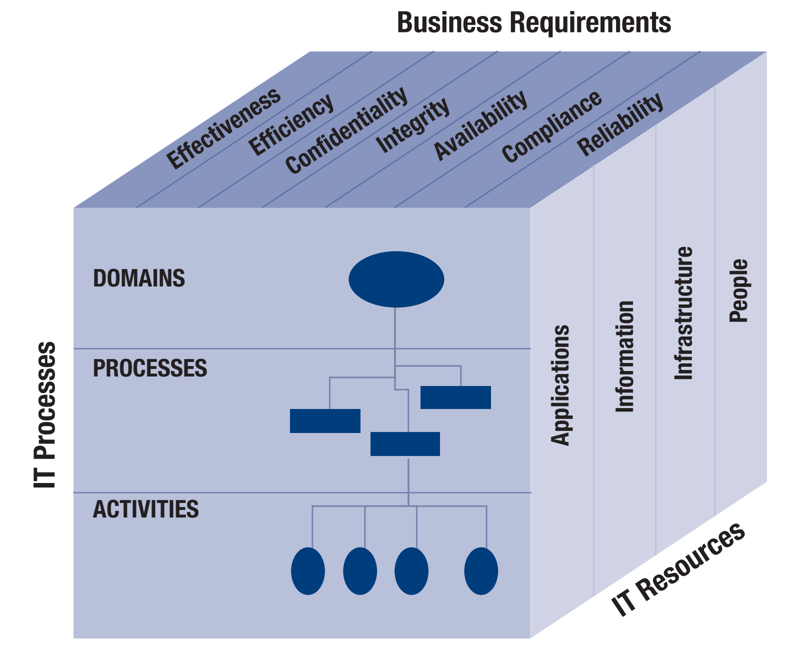
CobiT defines, the resources used by IT as follows:

- **Applications** are automated user systems and manual procedures that process the information.
- **Information** is the data (in all their forms) input, processed and output by the information systems in whatever form is used by the business.
- **Infrastructure** is the technology and facilities (hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them) that enable the processing of the applications.
- **People** are the personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services. They may be internal, outsourced or contracted as required.

CobiT CUBE

The previously mentioned components (IT processes, information criteria and resources) are three-dimensional, thus illustrating the IT function. These dimensions, as shown in **figure 4**, represent the CobiT cube.

Figure 4—CobiT Cube



IT GOVERNANCE USING CobiT

By definition, governance of IT and its processes is an ongoing and periodic measurement of deviations to the defined standard and timely and consequent implementation of corrective measures. This approach follows the cybernetic principle, i.e., everyone understands the process of setting the room temperature (standard) for the heating system (process), which will constantly check (compare) ambient room temperature (control information) and will signal (act) the heating system to provide more heat. This model and its principles identify a number of KGIs and KPIs that usually apply to all processes as they deal with what the standard is, who sets it, and who controls or needs to act.

FURTHER REFERENCES

Internet	
ISACA®	*www.isaca.org/cobit*
IT Governance Institute	*www.itgi.org*
CMMI®	*www.sei.cmu.edu/cmmi*

3. COSO

DOCUMENT TAXONOMY

Committee of Sponsoring Organisations of the Treadway Commission (COSO) *Internal Control—Integrated Framework* is a report that consists of four volumes. It is dedicated to improving the quality of financial reporting and ethics through effective internal control.

ISSUER

The report was issued by COSO, which is a voluntary, private-sector organisation. The committee was formed in 1985 to sponsor an initiative of the US National Commission on Fraudulent Financial Reporting to study causal factors that can lead to fraud. The sponsoring organisations are the American Accounting Association, American Institute of Certified Public Accountants, Financial Executives Institute, Institute of Internal Auditors and Institute of Management Accountants.

GOAL OF THE PUBLICATION

The goal is to improve the ways of controlling enterprises by defining an integrated control system. It enables senior executives to put internal controls in place to assure the achievement of the mission and profitability goals and manage risks. It is the most comprehensive study on internal control.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

COSO is usually implemented subject to one or more of the following business areas:

- Need for a structured approach when defining a control system
- Improvement of the efficiency of internal controls
- Assessment and evaluation of the internal controls
- Need to structure the internal controls
- Guideline for reporting to external parties, such as organisations required to comply with the US Sarbanes-Oxley Act

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing COSO include:

- Non-systematic approach for controls
- Incomplete controls
- Weak control environment
- Inefficient controls
- Inadequate processes and reporting due to a lack of controls

TARGET AUDIENCE

The responsible parties for internal control are addressed by the guidance. They range from senior management, boards of directors and internal auditors to every individual in the organisation.

TIMELINESS

COSO published *Internal Control—Integrated Framework* in 1992, but the content is still up to date.

CERTIFICATION OPPORTUNITIES

There is no opportunity for a certification.

CIRCULATION

The report is referenced as the international baseline for internal control systems; however, it is available in English only.

COMPLETENESS

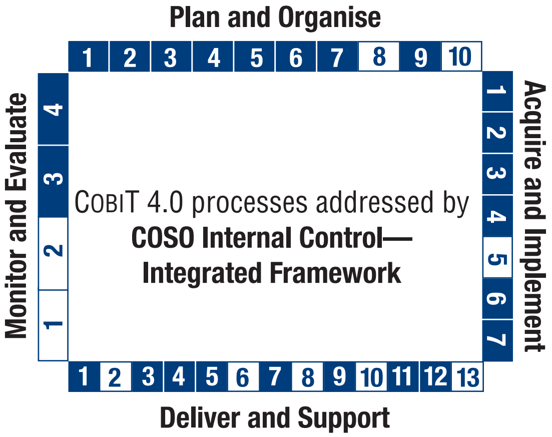
The report covers the topic of controls in a comprehensive manner. As it is focused on a management and control framework point of view, it may be seen as an additional reference for a framework for IT governance efforts. It is on a very high level and does not address IT requirements in a comprehensive manner, but its key concepts and definitions may be applied to control and management of diversified IT issues.

AVAILABILITY

The report can be purchased from AICPA at *www.cpa2biz.com*.

COBIT PROCESSES ADDRESSED

As mentioned previously, the COSO report is focused on internal controls and is not IT-specific. Thus, the mapping is on a higher level than other guidance in this document.



INFORMATION CRITERIA ADDRESSED

Information Criteria	
+	Effectiveness
+	Efficiency
+	Confidentiality
+	Integrity
+	Availability
+	Compliance
+	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

IT Resources	
+	Applications
+	Information
+	Infrastructure
+	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

The report consists of four volumes:
- *Executive Summary* gives a high-level overview of the framework of internal control. The executive summary is also included in *Framework*.
- *Framework* defines the framework of internal control and its components and contains criteria to assess the internal control system of the organisation.
- *Reporting to External Parties* provides guidance to establish reports in a properly controlled manner. It is addressed to organisations that publish their financial statements and to entities receiving those statements.
- The fourth volume, *Evaluation Tools*, consists of material that might be useful for an evaluation of the internal control system.

Framework is the core part of the report in terms of establishing and maintaining an internal control system for corporate and IT governance; consequently, its content is discussed in a higher level of detail. *Framework* contains the executive summary as an abstract of its content. After the summary, the key concepts and meanings are defined to enable a common understanding of internal control issues.

COSO defines internal control as follows:

> *Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*
> - *Effectiveness and efficiency of operations*
> - *Reliability of financial reporting*
> - *Compliance with applicable laws and regulations*

Internal control is to be built into the entity's processes. Control is part of them and not an isolated activity, event or circumstance.

The guidance reports that there are five components that form internal control. The way they interrelate and interact and how they influence the objectives of the organisation constitute the system of internal control. The system of internal control is individual to an organisation; in other words, no two entities have the same system of internal control. It depends on the size of the organisation, the industry, and the culture and management philosophy.

The components of the system are:
- Control environment—The environment in which people operate. People are seen as the core of any business, and people have individual attributes as ethical values or competences.
- Risk assessment—The awareness of risk is a crucial factor for the organisation to set objectives. Risks are to be identified, analysed and managed in an appropriate manner.
- Control activities—Policies and procedures are to be established for sound management of risk and to achieve the objectives defined by the organisation. The policies and procedures define the activities that have to be executed.
- Information and communication—Information and communication systems are used to manage the process. Those systems enable people to carry out their responsibilities, including control activities.
- Monitoring—The process has to be monitored permanently. Possibilities for modifications are to be unveiled and implemented in a timely manner.

The objectives of an organisation can be divided into three categories:
- Operations
- Financial reporting
- Compliance

An effective internal control system helps an organisation:
- Achieve its objectives
- Publish reliable financial statements
- Comply with applicable laws and regulations

FURTHER REFERENCES

Internet	
COSO	*www.coso.org*
AICPA Store	*www.cpa2biz.com*

4. ITIL

DOCUMENT TAXONOMY

The IT Infrastructure Library (ITIL) is a series of eight books and is referred to as the only consistent and comprehensive best practice for IT service management to deliver high-quality IT services. Although produced and published by a single governmental body, ITIL is not a standard. The books are:

- *Software Asset Management*
- *Service Support*
- *Service Delivery*
- *Planning to Implement Service Management*
- *ICT Infrastructure Management*
- *Application Management*
- *Security Management*
- *Business Perspective, Volume II*

ISSUER

The ITIL collection was published by the Central Computer and Telecommunications Agency (CCTA) now the British Office of Government Commerce (OGC), which still holds the ITIL copyright and trademark. The OGC was commissioned to develop a methodology for efficient and effective use of IT resources within the British government.

GOAL OF THE PUBLICATION

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 high-quality IT services.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

ITIL is usually implemented subject to one or more of the following business cases:

- Defining of service processes within the IT organisation
- Defining and improving the quality of services
- Need to focus on the customer of the IT
- Implementation of a central help desk function

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing ITIL include:

- Error-prone support processes due to lack of attention

TARGET AUDIENCE

ITIL focuses on organisations of varying size. It targets those responsible for IT service management.

TIMELINESS

The publications state they will be updated in a frequent and ongoing manner. OGC released the eighth book *Business Perspective, Volume II*, in 2005. The entire set of ITIL is currently undergoing an update. Current guidance in the seven core books is being reviewed and updated. The update's intention is not to rewrite the books, but to clarify the guidance and improve its relevance to business needs today. This will be done in conjunction with changes to the syllabi of the ITIL qualification scheme, and in alignment with development work by BSI on ISO 20000. The writing process is underway, and the complete set of core guidance will be reissued by mid-2007.

CERTIFICATION OPPORTUNITIES

Certification of personnel is available already, but at present, organisations cannot be certified. British Standard (BS) 15000 presents a specification for IT management for which ITIL can be used as guidance documents. BS 15000 was developed with ITIL in mind, and it is foreseeable that it will be possible for certification bodies to be accredited to certify against this British Standard. Note that BS 7799 complies with the security requirements of BS 15000.

There are three levels of certifications for IT service management:

- Foundation certificate—After a three-day course, a short multiple-choice exam must be passed. The foundation certificate is the entry-level certificate.
- Practitioner's certificate—This requires passing of assessments within a course and a case study-based, multiple-choice exam. The practitioner's certificate is focused on a specific discipline.
- Manager's certificate—It is gained through attendance at an accredited, 10-day training programme and the subsequent passing of two written exam papers.

CIRCULATION

ITIL is used internationally; however, it is available in English only.

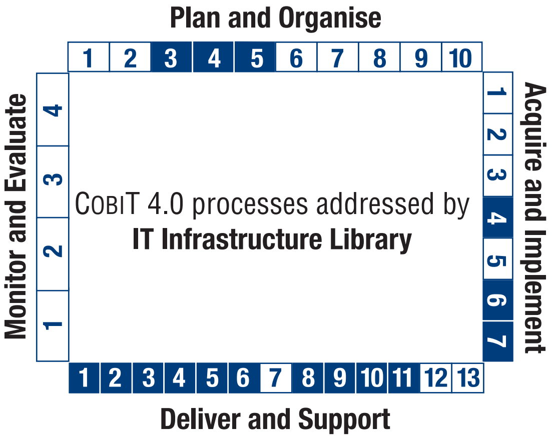
COMPLETENESS

The library has an adequate level of detail but does not cover the full breadth of IT management and IT governance as COBIT does. Processes of the COBIT DS domain are covered in a comprehensive manner; however, processes, tasks and duties of the PO, AI and ME domains are hardly treated.

AVAILABILITY

Most of ITIL is available for purchase as a paperback and a CD-ROM, with one exception: *Security Management* is available in print only.

COBIT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria	
+	Effectiveness
+	Efficiency
+	Confidentiality
+	Integrity
+	Availability
o	Compliance
-	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

IT Resources	
+	Applications
+	Information
+	Infrastructure
+	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

As mentioned previously, ITIL is a collection of books related to IT service management. ITIL, however, does not describe the *what*; it is focused on *how* and *who*.

Major tasks of an effective IT function are:
- Operation and maintenance of existing systems
- Development of new systems
- Adjustment of service delivery to the constantly evolving requirements of the core business

Two principal concepts characterise the basic thinking of ITIL:
- **Holistic service management**—IT service managers:
  - Assure the consideration of requirements for operations and maintenance
  - Develop test plans
  - Identify the effects on existing infrastructure caused by new or modified systems
  - Define future requirements
- **Customer orientation**—IT services are to be provided at a level of quality that allows permanent reliance on them. To assure this quality, responsibility is assigned to individuals who:
  - Consult the users and help them use the services in an optimal approach
  - Collect and forward opinions and recommendations of users
  - Track complaints
  - Monitor the users' appraisals of the services delivered
  - Support internal user groups

The core processes of IT service management are described within two ITIL documents: *Service Support* and *Service Delivery*. The description of the processes is not standardised and, thus, not consistent.

The processes of *Service Support* are:
- Incident management
- Problem management
- Configuration management
- Change management
- Release management

The key practices of *Service Delivery* are:

- Service level management
- Financial management for IT services
- Capacity management
- IT service continuity management
- Availability management

The volume *Planning to Implement Service Management* discusses the key issues of planning and implementing IT service management. It also explains the steps required for implementation or improvement of IT service delivery. The following volumes expand on specific aspects of IT service management:

- *ICT Infrastructure Management* guides through network service management, operations management, management of local processors, computer installation, and acceptance and systems management.
- *Application Management* discusses software development using a life cycle approach, as well as system design and change based on clear requirements, definition and users' needs.
- *Security Management* explains that the target of security management is to obtain the confidentiality, integrity and availability of information through risk assessment, security awareness, incident handling and service level management.
- *Software Asset Management* provides guidelines on what software asset management is and what is required to perform it effectively and efficiently.
- *Business Perspective*, not one of the original publications but a later addition, aims at helping business managers understand IT service delivery. It covers business relationship management, outsourcing, continuous improvement, and the contribution of information, communication and technology to achieve business advantages.

An overview of the processes within *Service Delivery* and *Service Support* is given in the following sections.

Incident Management

- **Description**—End users (the customers of the IT department) need a clearly defined point of contact, even though modern systems are becoming more user-oriented and user-friendly. Incident management's center of attention is the effective and efficient restoration/continuity of the operation or service affected to guarantee the compliance of the service level defined.
- **Goal**—The goal is swift restoration of normal service operation [as defined within service level agreement (SLA) limits] and minimal impact on business processes.
- **Major tasks:**
  – Identify and track incidents in a timely manner.
  – Classify the incident and provide initial support.
  – Localise potential causes of the incident.
  – Recover the services and manage closure.
  – Take ownership of the incident.
  – Monitor, track and communicate the execution.

Problem Management

- **Description**—A structured and systematic approach in problem management even before an incident occurs can minimise outages. Potential sources of error are to be identified and corrected in a timely manner. Hence, sound problem management is focused on preventive measures for the identification and solution of the root cause of incidents.
- **Goal**—An efficient and timely solution for problems is based on the definition of clear priorities. Critical problems are to be solved first. Moreover, a repeated occurrence of the problem is to be avoided, and the problem-solving capability of supporting staff is to be improved.
- **Major tasks:**
  – Identify and record problems.
  – Classify the problem, focused on the impact on the business.
  – Investigate the root cause of the problem.
  – Resolve the cause of the problem.
  – Close the problem.

Configuration Management

- **Description**—An application system's level of service is highly dependent on the knowledge of its inner structure. Thus, strict management of the configuration is essential to tap the full potential of an application system. Configuration management is responsible for providing the information necessary for planning and monitoring the resources.
- **Goal**—There is no single goal of the configuration management process. There are multiple goals:
  - Account for IT assets and configurations.
  - Verify the configuration records and correct exceptions.
  - Provide accurate information on configurations and the referring documentation as well as a sound basis for other processes (incident, problem, change and release management).
- **Major tasks:**
  - Identify the demand for relevant information (purpose, scope, objectives, policies and procedures for sound configuration).
  - With the owner, identify and label configuration items (CI), available documentation, versions and interrelationships.
  - Document CIs in a central configuration management database (CMDB).
  - Establish procedures and documentation standards to ensure that only authorised and identifiable CIs are recorded and historical, traceable information is available.
  - Ensure permanent accountability of data (status accounting).
  - Verify and audit the physical existence of CIs recorded in the CMDB.

Change Management

- **Description**—Even though services evolve constantly, the quality of services delivered to core business processes may not be disrupted. Reliable change management covers planning and supervising changes to the existing infrastructure, thus minimising the risk of damage to existing and new application systems, infrastructure and services.
- **Goal**—Changes are implemented within the agreed time and with minimal risk.
- **Major tasks:**
  - Record, log and filter requests for change (RFCs).
  - Prioritise and categorise the RFC.
  - Assess the impact of the RFC on the infrastructure and other services as well as on non-IT processes (e.g., information security) and effects of not implementing the RFC.
  - Identify required resources for implementing the RFC.
  - Obtain approval for the RFC.
  - Schedule the implementation.
  - Implement the RFC.
  - Review the implementation of the RFC.
  - Establish an entity in charge of the authorisation process of those RFCs identified with major impact; this entity is called the change advisory board (CAB).

Release Management

- **Description**—Assurance that only tested and approved applications are rolled out is becoming more and more important, as different operating systems, different locations and an increased frequency of patches complete the release management.
- **Goal**—Approved and accredited components (hardware, software, firmware and documents) are installed trouble-free and on schedule.
- **Major tasks:**
  - Plan the release.
  - Design the release and perform tests for accreditation.
  - Plan the rollout.
  - Inform and train prospective users.
  - Sign off on the release for implementation.
  - Audit the components before and after the implementation.
  - Install or roll out.

Service Level Management

- **Description**—With sound service level management, clear interfaces and specification of services are defined with customers (senior management). Users and internal and external suppliers are identified and managed. Internal operational level agreements and contracts with external suppliers facilitate adherence to negotiated service level agreements.
- **Goal**—The goal is to ensure the compliance of the services delivered with the level of services demanded and agreed upon.

- **Major tasks:**
  - Record the service level requirements (SLRs).
  - Ensure the delivery of the service level required by establishing or updating a service quality plan (SQP), contracts with third parties and operational level agreements (OLA).
  - Contract SLAs.
  - Monitor the level of services provided.
  - Improve service quality.
  - Establish and maintain the service catalogue.

Financial Management for IT Services

- **Description**—Management of expenses and accurate redistribution of costs improve the availability of financial resources.
- **Goal**—Finance-related information is provided to establish cost-oriented steering of the organisation.
- **Major tasks:**
  - Budgeting:
    - Define cost centres.
    - Calculate standard costs.
    - Compare target with actual values of costs, services and distribution of costs.
  - Accounting:
    - Define a costing sheet and procedures for recording accounting data.
    - Collect and assign actual costs.
    - Collect actual services and distribution of costs.
    - Monitor incoming and outgoing payments.
  - Distribution of costs:
    - Define procedures for the distribution of costs.
    - Establish a price list.
    - Prepare invoices.

Capacity Management

- **Description**—Proactive identification of performance requirements ensures a continuous level of service and proper management of resources. Sound management of capacity considers three levels:
  - Business capacity
  - Service capacity
  - Resource capacity
- **Goal**—Providing the appropriate capacity ensures the delivery of the service at an agreed-upon level.
- **Major tasks:**
  - Define, plan and manage the requirements.
  - Provide resources for the services.
  - Monitor the performance of resources and adjust if necessary.
  - Plan and implement improvements.
  - Establish and maintain a capacity plan.

IT Service Continuity Management

- **Description**—By minimising negative effects caused by disastrous and unpredictable events, disruption of the core business processes is minimised.
- **Goal**—The goal is to provide a predetermined and agreed-upon level of services in case of a disastrous event.
- **Major tasks:**
  - Define requirements and strategies for IT continuity, derived from the overall business continuity management process.
  - Define measures and continuity plans for IT services.
  - Manage continuity procedures (training, tests, reviews, change management and continuous improvement).
  - Manage continuity and recovery in an emergency.

Availability Management

- **Description**—Continuous monitoring and improvement of the availability of systems minimises outages and thus improves the availability of services.
- **Goal**—The goal is to ensure the consistent availability of IT services as required by the business processes.
- **Major tasks:**
  - – Define the requirements for availability.
  - – Set up availability forecasts.
  - – Define measures.
  - – Set up an availability plan.
  - – Determine actual availability.
  - – Improve the availability of IT services.

FURTHER REFERENCES

Internet	
OGC	*www.ogc.gov.uk*
ITIL Online	*www.itil.co.uk*
*it*SMF	*www.itsmf.com*

5. ISO/IEC 17799:2005

DOCUMENT TAXONOMY

ISO/IEC 17799:2005 *Code of Practice for Information Security Management* is an international standard.

ISSUER

The international standard was published by the International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC), which established a joint technical committee, ISO/IEC JTC 1. The historic source for the standard was BS 7799-1, which contributed essential parts to ISO/IEC 17799:2005. It was developed and published by the British Standards Institution (BSI), labeled as BS 7799-1:1999. The original British Standard was issued in two parts:

- BS 7799 Part 1: *Information Technology—Code of Practice for Information Security Management*
- BS 7799 Part 2: *Information Security Management Systems—Specification with Guidance for Use* (now ISO/IEC 27001)

GOAL OF THE STANDARD

The goal of ISO/IEC 17799:2005 is to provide information to parties responsible for implementing information security within an organisation. It can be seen as a best practice for developing and maintaining security standards and management practices within an organisation to improve reliability on information security in interorganisational relationships. It defines 132 security controls strategies under 11 major headings. The standard stresses the importance of risk management and makes it clear that one does not have to implement every stated guideline, only those that are relevant.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

ISO/IEC 17799:2005 is usually implemented subject to one or more of the following business cases.

- Defining an information security management system and applying best practice in security management based on a systematic approach
- Identifying critical assets via the business risk assessment
- Enhancing the knowledge and importance of security-related issues at the management level
- Defining responsibility and organisational structures for information security
- Need for a basis for certification of the information security management system
- Need for contractual relationships

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing ISO/IEC 17799:2005 include:

- Risk of information disclosure, including related risks such as loss of confidence and trust
- Incomplete risk assessment, thus an inadequate level of risk management
- Inadequate business continuity management
- Lack of security awareness within the organisation
- Inadequate security requirements when interacting with third-party organisations
- Inadequate level of physical and logical security
- Flawed procedures due to the lack of incident management

TARGET AUDIENCE

The document targets those who are responsible for initiating, implementing and/or maintaining information security.

TIMELINESS

The first edition of the standard was published in 2000, and the second edition was released in 2005. Since the current version (ISO/IEC 17799:2005) is an official ISO standard, it will automatically be revised and updated as required every three to five years. ISO plans to include the standard in the ISO 2700x series, *Information Security Management System*, in April 2007 as 27002. The standard can be classified as current best practice in the subject area of information security management systems.

CERTIFICATION OPPORTUNITIES

A certification for ISO/IEC 17799:2005 is currently not available. However, a certificate on compliance with ISO/IEC 27001 (BS 7799-2) can be obtained, as ISO/IEC 27001 contains binding specifications for a certification of an information security management system, as well as normative controls.

ISO/IEC 27001:2005 was issued on 15 October 2005. A growing number of organizations have gone through or are in the process of obtaining certification.

CIRCULATION

The standard is used worldwide, and several countries have published local versions.

COMPLETENESS

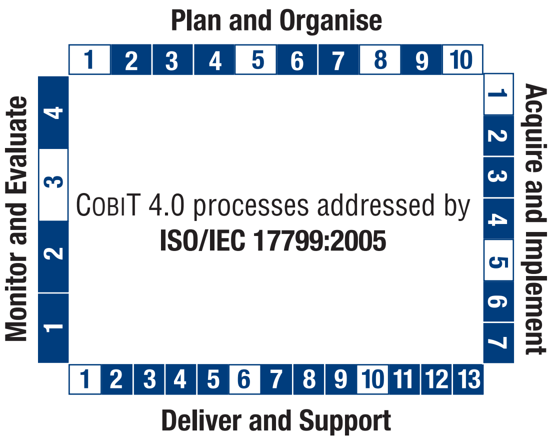
Generic measures for information security management are provided, as well as the imperative of compliance with laws and regulations.

The standard is focused on security issues and does not cover the full scope of IT management duties. The level of detail is comparable to CobiT. For a detailed comparison of the content, refer to the ITGI publication *CobiT® Mapping: Mapping of ISO/IEC 17799:2000 With CobiT.* ITGI anticipates releasing an update to this publication later in 2006 to be titled *CobiT Mapping: Mapping of ISO/IEC 17799:2005 With CobiT*.

AVAILABILITY

The standard can be purchased from ISO and from most local standardisation bodies.

CobiT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria	
-	Effectiveness
-	Efficiency
+	Confidentiality
+	Integrity
+	Availability
+	Compliance
o	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

IT Resources	
+	Applications
+	Information
o	Infrastructure
+	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

The need for information security is based on the fact that information and related systems are important assets for organisations. As organisations face information security threats, the protection of information is essential to maintain organisational stability.

Sources for the identification of security requirements are:
- Risks the organisation faces and the impact on business strategy and objectives
- Legal requirements
- Specific requirements, principles and objectives for information processing to support business operations

Controls should be selected and defined considering:
- Legal requirements
- Business requirements
- Cost of implementation
- Potential impact of a security breach

When implementing a system for information security management, several critical success factors should be considered to ensure:
- That the security policy, its objectives and its activities reflect the business objectives
- That the implementation considers cultural aspects of the organisation
- Open support and engagement of senior management
- Thorough knowledge of security requirements, risk assessment and risk management
- That effective marketing of security targets all personnel, including members of management
- That the security policy and security measures are communicated to contracted third parties
- That sufficient and adequate funding is available
- That users are well trained
- That a comprehensive information security incident management process is established
- That a comprehensive and balanced system for performance measurement is available that supports continuous improvement by giving feedback

After presenting introductory information (scope, terms and definitions), a chapter briefly describes methods for risk assessment and treatment wherein references to ISO/IEC TR 13335 are made. ISO/IEC 17799:2005 is structured into 11 sections (security control chapters), which contain 39 main security categories.

The main security categories consist of a control objective and one or more controls to achieve the control objective. Guidance is provided to implement controls, and references to further information are made.

Information security should—according to the standard—at least consider the following parts:

- **Security policy:**
  - An information security policy should define the direction and contain the commitment and support of management.
  - The policy should be reviewed periodically and communicated throughout the organisation.
- **Organisation of information security:**
  - Information security should be supported by management; therefore, a demonstrated commitment should be made.
  - Relevant activities should be co-ordinated throughout the organisation, and responsibilities for information security should be clearly defined.
  - Confidentiality agreements should be in place.
  - Appropriate contacts with authorities (e.g., fire department, law enforcement) and special interest groups (e.g., security forum) should be maintained.
  - Information security should be subject to independent review.
  - Controls should be implemented to manage identified risks related to external parties (including customers).
  - Outsourcing arrangements should address information security.
  - There should be an authorisation process for information processing facilities.
- **Asset management:**
  - An inventory of assets and assignment of the responsibility for their protection should be made as a prerequisite to sound accountability for assets.
  - All assets should have a nominated owner, and the use of assets should be based on defined rules.
  - Information should be classified and labeled following a generally accepted system, thus ensuring an appropriate level of protection.
- **Human resources security:**
  - Security requirements for employees should be identified throughout the life cycle: prior to employment, during employment, and upon termination or change of employment.
  - Security responsibilities, confidentiality agreements and the contract of employment should be part of the job responsibility and terms and conditions of employment.
  - Adequate controls for personnel screening should be in place.
  - Information security education and training should increase the security awareness of all employees.
  - A formal disciplinary process should be in place for individuals who breach security policies.
  - Rules for termination and change of employment should be defined and followed.
- **Physical and environmental security:**
  - Central equipment should be installed only within a secure area (including offices, rooms and facilities) where adequate access controls and damage prevention (against environmental factors and threats) are implemented.
  - Equipment should be protected against loss, damage or compromise by being sited and protected in an appropriate manner. Power supplies, an adequate level of cabling security and correct maintenance of the equipment should be in place.
  - Equipment installed off premises and the disposal or reuse of information should be considered; authorisation for taking equipment off site is recommended.
  - Special attention is needed at public access, delivery and loading areas where the central equipment is installed.
- **Communications and operations management:**
  - Operations should follow documented procedures.
  - All changes to facilities should be controlled.
  - Duties should be segregated, ensuring that no individual can both initiate and authorise an event.
  - Development and operational facilities should be separated.
  - Risks caused by contracted organisations should be covered, and third-party services should be controlled.
  - System planning and acceptance consider capacity management and the definition of acceptance criteria.
  - Damage caused by malicious software and mobile code should be prevented, using preventive and detective controls, formal policies, and defined recovery procedures.
  - Information should be backed up, and the backup files should be tested regularly.
  - Networks and network services should be set up and managed with a view to ensuring the necessary level of security and service levels.
  - Removable media should be handled with special care.
  - Media with sensitive information should be disposed of in a secure manner.

- Adequate controls in information handling procedures (e.g., labeling of media, ensuring completeness of inputs, storage of media) should be considered.
- System documentation is to be protected, as it may contain sensitive information.
- Agreements for the exchange of information and software should be established, including media in transit, e-commerce transactions, e-mail, electronic office systems, publicly available systems and other forms of information interchange.
- E-commerce services and their use should be controlled.
- Security-relevant activities should be logged and monitored, and the effectiveness of controls should be assessed.

- **Access control:**
  - Access to information should be granted in accordance with business and security requirements.
  - A formal access control policy should be in place.
  - Access control rules should be specified.
  - User access management (registration, privilege management, password management, review of user access rights) should follow a formal process.
  - User responsibilities concerning password use and protection of unattended equipment, as well as a ‘clear desk’ and ‘clear screen’ policy, should be clearly defined.
  - Networked services, operating systems and applications should be protected appropriately.
  - System access and use should be controlled efficiently, considering secure logon procedures, user identification and authentication, password management, usage of system utilities, and session time-out.
  - Software and information access should be restricted to authorised users.
  - Mobile computing and teleworking should be performed in a secure manner.
- **Information systems acquisition, development and maintenance:**
  - Security issues should be considered when acquiring or implementing information systems following defined requirements; security requirements should be specified.
  - Security in application systems should take into account the validation of input data, adequate controls of internal processing, message integrity and output data validation.
  - Use of cryptographic systems should follow a defined policy and consider best practices.
  - Security of and access to system files (including test data and program source code) should be controlled.
  - Project and support environments should allow for security by being rigorously controlled (e.g., change management procedures, arrangements for outsourced development, information leakage).
  - Damage through published vulnerabilities should be prevented.
- **Information security incident management:**
  - Security events and weaknesses should be reported.
  - Responsibilities and procedures for managing security incidents and improvements should be defined, and evidence for security incidents should be collected.
- **Business continuity management:**
  - A comprehensive business continuity management process should permit prevention of interruptions to business processes.
  - The business continuity management process should not be restricted to IT-related areas and activities.
  - An impact analysis should be executed that results in a strategy plan.
  - Business continuity plans should be developed following a single framework.
  - Business continuity plans should be tested, maintained and reassessed continuously.
- **Compliance:**
  - Relevant legal requirements should be identified and followed.
  - Any unlawful act (e.g., data protection acts) should be avoided.
  - Compliance with the security policy should be ensured by periodic reviews.

FURTHER REFERENCES

Internet	
ISO	*www.iso.org*
IEC	*www.iec.org*
BSI	*www.bsi-global.co.uk*

6. FIPS PUB 200

DOCUMENT TAXONOMY

The Federal Information Processing Standards (FIPS) Publication 200 *Minimum Security Requirements for Federal Information and Information Systems* is a US national standard. It was issued in March 2006.

ISSUER

The Computer Security Division of the National Institute of Standards and Technology (NIST), a department of the US Department of Commerce, published the standard. It is one of a series of security standards and guidelines developed by NIST in response to the Federal Information Security Management Act (FISMA) legislation.

GOAL OF THE STANDARD

The standard addresses the specification of minimum security requirements for US federal information and information systems. It promotes the development, implementation and operation of secure information systems by establishing minimum levels of due diligence for information security. It also provides an approach for selection and specification of security controls.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

FIPS PUB 200 is usually implemented subject to one or more of the following businesses cases:

- The need to comply with the principles and criteria for US federal organisations
- The need to implement a sound security baseline
- The need for a consistent, comparable and repeatable approach for information security
- Co-operation with federal organisations

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing FIPS PUB 200 include:

- Insecure systems due to insufficient information security
- Non-compliance with regulatory requirements

TARGET AUDIENCE

The standard is applicable to US federal government information systems and information systems designated as US national security systems. Individual groups within the organisations are not specified by the standard.

TIMELINESS

The FIPS PUB 200 was issued in March 2006 after an exposure and comment period.

CERTIFICATION OPPORTUNITIES

A certificate is not available.

CIRCULATION

The publication is from a US government department; thus, it is relevant for US government organisations. International usage of the standard is not expected.

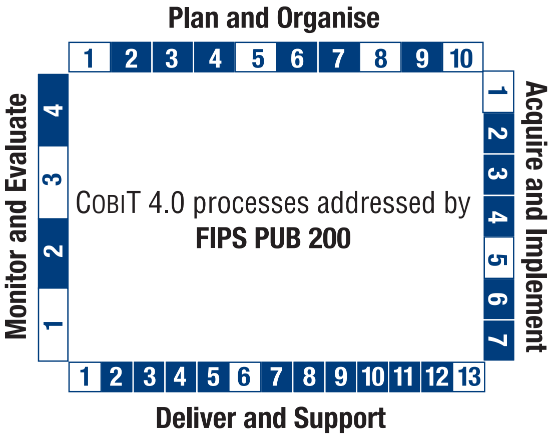
COMPLETENESS

The paper is focused on information security. Due to the focus on security, the information contained does not address the complete scope of IT management and governance issues and is classified as narrow. Its purpose is very specific, dealing with the security requirements for the US government; however, aspects can also be useful to the private sector. The paper is high-level and is not as deep as other guidance discussed within this research.

AVAILABILITY

The guidance is posted for complimentary download from the NIST Computer Security Division web site. Printed versions are not available from the publisher.

CobiT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria
- Effectiveness
- Efficiency
+ Confidentiality
+ Integrity
+ Availability
- Compliance
- Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

IT Resources
+ Applications
o Information
+ Infrastructure
+ People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

The standard was published to comply with the requirements of the FISMA legislation and should be used with the FIPS PUB 1999, which defines a security categorisation of information systems used by federal organisations. FIPS PUB 200 also provides security control selection and customises the control baseline. The security categories depend on the potential impact on confidentiality, integrity and availability of information and represent a high-watermark system. The potential is expressed as high, medium or low, and the highest impact on a security objective determines the security category.

Security-related areas are defined in the standard as follows:

- **Access control**—Access to information systems must be limited to authorised users.
- **Awareness and training**—Security awareness and knowledge of applicable regulations must be assured for users of information systems.
- **Audit and accountability**—Audit records must be retained, and the actions of users must be traceable.
- **Certification, accreditation and security assessments**—Security-related controls must be assessed periodically, deficiencies must be corrected to reduce vulnerabilities, information systems and system connections must be authorised, and security controls must be monitored.
- **Configuration management**—Baseline configurations and inventories of information systems must be maintained, considering security-related configuration settings, and changes must be controlled and monitored.
- **Contingency planning**—Plans for emergency response, continuous operations and disaster recovery must be defined for information systems.
- **Identification and authentication**—Users, processes or devices acting as users must be identified, and the authenticity must be verified.
- **Incident response**—Incident-handling procedures must be defined, and incident tracking, documentation and reporting must be ensured.
- **Maintenance**—Information systems must be subject to periodic maintenance. Tools, techniques, personnel, etc., used for maintenance must be controlled.
- **Media protection**—Information on media (printed or electronic) must be protected, access to media must be restricted to authorised users, and media must be destroyed before disposal.
- **Physical and environmental protection**—Physical access to systems must be restricted to authorised personnel, and systems must be protected against environmental hazards.
- **Planning**—Security plans must be developed and maintained for information systems.
- **Personnel security**—Personnel abilities and responsibilities must meet the requirements for the positions and the security level.
- **Risk assessment**—Risks to organisational operations must be assessed periodically.
- **System and services acquisition**—Appropriate resources for the acquisition and operation of information systems should be available.
- **System and communication protection**—Organisational communication must be protected within the organisation and at the external boundaries of information systems.
- **System and information integrity**—Information and information system flaws must be reported in a timely fashion, protection against malicious code must be in place, and alerts and advisories should be monitored and acted upon appropriately.

A set of security-related controls must be defined for the security requirements. The security control baseline must be tailored by considering:

- **Scoping guidance**—The guidance bears in mind considerations related to technology, common security controls, public access information systems, infrastructure, scalability and risks.
- **Compensating security controls**—Controls that provide equivalent (in scope and time) protection of the information systems. The design of compensating controls and residual risks is assessed and agreed.
- **Organisation-defined security control parameters**—The definition of controls depends on the requirements of the organisation but must comply with relevant regulation.
- **Supplementing the security control baselines**—As the baseline provides the minimum level for protection of information, the set of selected security controls must reflect the organisational risk assessment.

FURTHER REFERENCES

Internet	
NIST	*www.nist.org*
CSD	*http://csrc.nist.gov/publications*

7. ISO/IEC TR 13335

DOCUMENT TAXONOMY

ISO/IEC TR 13335 *Information Technology—Guidelines for the Management of IT Security* is a technical report divided into five parts.

ISSUER

The report was published by ISO and IEC, which established the joint technical committee, ISO/IEC JTC 1, Subcommittee SC 27 (IT security techniques), which is tasked to publish international standards (e.g., ISO/IEC 17799:2005).

GOAL OF THE STANDARD

The goal of the report is to provide guidance on aspects of IT security management. It is divided into five parts:

1. The management tasks of IT security are outlined, providing an introduction to security concepts and models for information and communication technology.
2. The implementation and management of IT security are discussed in a comprehensive manner.
3. Techniques for the management of IT security are provided.
4. Guidance is provided on the selection of safeguards, considering the type of IT systems as well as security concerns and threats.
5. Information is offered on identifying and analysing communication-related factors that should be taken into account when introducing network security.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

ISO/IEC TR 13335 is usually implemented subject to one or more of the following businesses cases:

- Guidance for security management
- The need for a structured approach

RELATED RISKS OF NON-COMPLIANCE

There is no direct risk from not complying unless the organisation has an inherent need to comply with this standard.

TARGET AUDIENCE

The report is applicable to all types of organisations. The first part explicitly addresses senior management and information security managers, whereas the other parts target individuals, such as IT managers and IT security staff, who are responsible for the implementation of security measures.

TIMELINESS

Dates of publication range from 1997 (part 2) to 2004 (update of part 1). None of the parts has a defined update frequency, as each was published as a technical report. ISO/IEC TR 13335 Part 1:2004 has superseded ISO/IEC TR 13335 Part 1:1996 and ISO/IEC TR 13335 Part 2:1997. ISO/IEC 13335-2, when published, will cancel and replace ISO/IEC TR 13335-3:1998 and ISO/IEC TR 13335-4:2000. Additionally, all or some of 13335 may make it into the 2700x series on Information Security Management being developed by ISO.

CERTIFICATION OPPORTUNITIES

There is no specific certification available.

CIRCULATION

The technical reports are recognised globally.

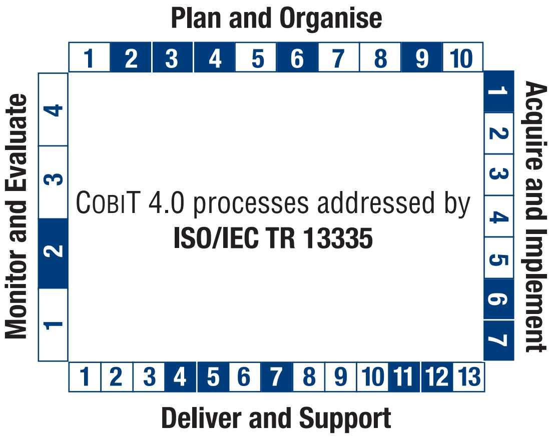
COMPLETENESS

The standard contains comprehensive guidance on managing information security. Since it is focused on security issues, it does not address the complete scope of IT management duties.

AVAILABILITY

The documents can be acquired from ISO.

COBIT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria

o Effectiveness
- Efficiency
+ Confidentiality
+ Integrity
+ Availability
+ Compliance
+ Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

IT Resources

+ Applications
+ Information
+ Infrastructure
+ People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

As mentioned previously, the current version of the report consists of five parts.

Part 1—Concepts and Models for Information and Communications Technology Security Management

The first part discusses basic management concepts and models of IT security. It can be used as an introduction to the management of IT security, as it does not provide detailed information on IT security.

The major elements involved in the security management process are as follows:

- Security principles [risk management, commitment, defined roles and responsibilities, objectives, strategies and policies, and life cycle management of organisational information and communication technology (ICT) assets]
- Assets (physical assets, information, software, people and intangibles)
- Threats (human and environmental)
- Vulnerabilities
- Impact
- Risk
- Safeguards
- Constraints
- Security element relationships

The objectives, strategies and policies section describes the approach to establishing the required basis for an effective ICT security in an organisation. A clear policy hierarchy (corporate security policy, information security policy, corporate ICT security policy and ICT system security policy) is provided, as well as recommended elements of those policies.

The organisational aspects of IT security are explained, including requirements of roles and responsibilities and assigning accountability. The roles of the security forum, a corporate ICT security officer, ICT users and the ICT security management function are discussed, as well as organisational principles (commitment to the goals of ICT security, a consistent approach and integration of ICT security).

Part 2—Managing and Planning IT Security

Part 2 contains guidelines that address essential topics on the management of IT security.

Establishing and maintaining an IT security programme is the main task of IT security management. It consists of a planning and management process, risk management, implementation, follow-up (maintenance and monitoring), and integration throughout the organisation.

A sound corporate IT security policy should address the following questions:

- **Objectives**—What is to be achieved, how are the objectives to be achieved, and what are the rules for achieving the objectives?
- **Management commitment**—What level of commitment and support is provided by senior management?
- **Policy relationships**—What are the relationships amongst corporate strategy, marketing policy, security policy, IT policy, IT security policy and system-specific policies?
- **Policy elements**—Is there a comprehensive list of topics that are to be covered?

Organisational aspects of IT security, such as roles and responsibilities, the initiation of a security forum, and the nomination of security, project and system security officers, are discussed. The need for support by all levels of management is outlined, as is the importance of following a consistent approach throughout the organisation and all systems.

Strategic options for a risk management strategy are presented thereafter. The specific advantages and disadvantages are addressed. The approaches are:

- **Baseline approach**—By selecting a set of safeguards to all systems, a baseline protection level is achieved.
- **Informal approach**—A pragmatic risk analysis for all systems, it requires experience of individuals and seems to be suitable for small organisations.
- **Detailed risk analysis**—A detailed analysis begins with the identification and valuation of assets, the threats to those assets, a selection of appropriate safeguards and the identification of an acceptable level of residual risk.
- **Combined approach**—Using the detailed approach at a high level identifies systems with a high risk, which are analysed in a more comprehensive manner. The other systems are appropriate for a baseline protection approach.

The security recommendations section addresses different types of safeguards, their interdependency and recommendations for selecting and maintaining them, as well as the need for acceptance of residual risk and its classification as 'acceptable' or 'unacceptable'.

Following the discussion of risk management, other issues briefly mentioned are:

- **IT system security policy**—Contents and endorsement
- **IT security plan**—Documentation of actions to be taken for implementing the IT security policy
- **Implementation of safeguards**—Implementing safeguards as defined in the plan, including security training
- **Security awareness**—Passing the knowledge from the security officer to all levels of the organisation
- **Follow-up**—Activities such as maintenance of safeguards and policies, security compliance checking, monitoring and incident handling

Part 3—Techniques for the Management of IT Security

Management techniques are described and recommended in Part 3 of the report.

In addition to general information, an overview of the IT security management process is provided. Its major activities are:

- **Analysis of security requirements**—The definition of security objectives, strategy and the development of a corporate IT security policy
- **Selection of a corporate risk analysis strategy**—Identification and assessment of risks and their reduction to an acceptable level based on security requirements of different systems
- **Implementation of the IT security plan**—Implementation of safeguards, including security awareness and security training
- **Follow-up**—Checking compliance, monitoring, change management practices and incident handling

The importance of a corporate IT security policy is discussed, and recommended policy components are listed. A detailed table of contents is provided in the annex of the report.

The implementation of safeguards and a security awareness programme follow the methodology-based identification of security needs. During the implementation phase, a security awareness programme is used to increase the level of awareness within the organisation. A sound awareness programme consists of the following components:

- **Needs analysis**—Existing and targeted level of awareness within different target groups and identification of necessary methods
- **Programme delivery**—Interactive and promotional techniques
- **Monitoring**—Periodic performance evaluation to determine the level of awareness and comprehensive change management to ensure that skills and awareness reflect modifications to systems

Either internal or external experts ensure the achievement of the objectives by closing the implementation phase with an approval of the systems implemented. Part 3 concludes with a discussion of follow-up activities such as maintenance, compliance checking, change management, monitoring and incident handling. A comprehensive list of possible threat types and vulnerabilities and a description of a risk analysis method are provided in the annex, after the aforementioned table of contents of a security policy.

Part 4—Selection of Safeguards

The selection of safeguards should be based on a high-level risk analysis. The high-level result is the identification of systems requiring a detailed risk analysis and the need for baseline protection. The method for detailed risk analysis is discussed in Part 3. Baseline protection can come in two flavours: selection of safeguards according to the type of IT system or according to security concerns and threats.

The basic assessments of the safeguard selection process are:

- **Identification of the type of system**—IT systems can be stand-alone workstations, workstations connected to a network or servers/workstations sharing resources via a network.
- **Identification of physical/environmental conditions**—In addition to general considerations concerning the environment of the organisation, more specific concerns are to be taken into account, such as perimeter and building (physical situation, single or multioccupied, information about other occupants, identification of sensitive/critical areas), access control (access to the building, physical access controls, robustness and structure of the building, protection level of doors, windows, etc.) or the protection in place (protection of rooms, fire detection/suppression facilities, water leakage detection, uninterruptible power supply (UPS), temperature and humidity controls, etc.).
- **Assessment of existing/planned safeguards**—By identifying existing safeguards, reselection of safeguards should be prevented. The identification is done by a review of documentation, a check with responsible personnel, or a walk-through of the building. Existing safeguards may exceed the current needs.

Safeguards can be classified into organisational/physical and system-specific safeguards:

- **Organisational and physical safeguards:**
  - IT security management and policies
  - Security compliance checking
  - Incident handling
  - Personnel
  - Operational issues
  - Business continuity planning
  - Physical security
- **IT system-specific safeguards:**
  - Identification and authentication
  - Logical access control and audit
  - Protection against malicious code
  - Network management
  - Cryptography

The organisational safeguard categories are applicable to all IT systems. Thus, all safeguards from this category should be considered first when following the baseline approach. IT system-specific safeguards require an in-depth consideration of the needs of the type and characteristics of the system.

When selecting safeguards, the security concerns—the loss of confidentiality, integrity, availability, accountability, authenticity or reliability—should be considered. Each of these categories faces several threats:

- **Confidentiality:**
  - Eavesdropping
  - Electromagnetic radiation
  - Malicious code
  - Masquerading of user identity
  - Misrouting/rerouting of messages
  - Software failure
  - Theft
  - Unauthorised access to computers, data, services and applications
  - Unauthorised access to storage media
- **Integrity:**
  - Deterioration of storage media
  - Maintenance error
  - Malicious code
  - Masquerading of user identity
  - Misrouting/rerouting of messages
  - Non-repudiation
  - Software failure
  - Supply failure (power, air conditioning)
  - Technical failure
  - Transmission errors
  - Unauthorised access to computers, data, services and applications
  - Use of unauthorised programs and data
  - Unauthorised access to storage media
  - User error
- **Availability:**
  - Destructive attack
  - Deterioration of storage media
  - Failure of communication equipment and services
  - Fire, water
  - Maintenance error
  - Malicious code
  - Masquerading of user identity
  - Misrouting/rerouting of messages
  - Misuse of resources
  - Natural disasters
  - Software failures
  - Supply failure (power, air conditioning)

- Technical failures
- Theft
- Traffic overloading
- Transmission errors
- Unauthorised access to computers, data, services and application
- Use of unauthorised programs and data
- Unauthorised access to storage media
- User error

- **Accountability, authenticity and reliability:**
  - No specific threats are listed in the report—only exemplary threats, such as account sharing, lack of traceability, masquerading of user identity, software failure, a weak authentication of identity or unauthorised access to computers, data and applications.

Examples of countermeasures to the previously mentioned threats are provided in the report. The selection of a specific safeguard should include consideration of and decision on the basic aspect that is to be addressed by the safeguard. These aspects are:

- **Threat**—Reduction of the likelihood
- **Vulnerability**—Removal of the vulnerability or making it less serious
- **Impact**—Reduction or avoidance of the impact

During the implementation of an organisationwide baseline, it must be decided whether the organisation can be protected by the same baseline or if different levels have to be identified.

The annexes contain a short description of several sources of information concerning baseline protection and IT security.

Part 5—Management Guidance on Network Security

Part 5 deals with network security and provides guidance for the identification and analysis of communication and networks. It also provides an introduction to safeguard areas.

The following series of activities is recommended for the process of identification and analysis of communication-related factors:

- **Review corporate IT security requirements**—The IT security policy states the requirements for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information.
- **Review network architectures and applications**—Depending on the types of networks, protocols used, applications installed, and other considerations, such as trust relationships, different safeguard areas may be identified.
- **Identify types of network connection**—Networks are usually connected in different topologies and at different organisational levels:
  - A single controlled location within an organisation
  - Connection amongst different geographical locations within an organisation
  - Connection between an organisation site and personnel working in locations away from the organisation
  - Connection amongst different organisations with a closed community
  - Connections with other organisations
  - Connections with the Internet
- **Review networking characteristics and related trust relationships**—The characteristics can be classified into public or private networks and data and/or voice networks. Another distinction can be made between packet (using hubs) or switched networks. The trust relationship is—depending on its environment—classified into low, medium or high. The combination of the characteristics of the network connection (private or public) and trust environment (low, medium or high) provides basic information for identification of safeguards.
- **Determine the types of security risks**—Depending on the type of security risk (loss of confidentiality, loss of integrity, etc.) and the previous combination of characteristic and trust, appropriate safeguards can be nominated.
- **Identify appropriate potential safeguard area**s—On the basis of the security risks, several safeguards can be identified. They are grouped into disciplines such as:
  - Secure service management
  - Identification and authentication
  - Audit trails
  - Intrusion detection
  - Protection against malicious code
  - Network security management
  - Security gateways

  - Data confidentiality over networks
  - Data integrity over networks
  - Non-repudiation
  - Virtual private networks
  - Business continuity and disaster recovery
- **Document and review security options**—The documentation of the intended architecture allows a final analysis of its design.
- **Prepare for the allocation of safeguard selection, design, implementation and maintenance**—Set up an organisation and define specific tasks for selection, implementation and maintenance of the safeguard.

FURTHER REFERENCES

Internet	
ISO	*www.iso.org*

8. ISO/IEC 15408:2005/COMMON CRITERIA/ITSEC

The international standard ISO/IEC 15408:2005 *Security Techniques—Evaluation Criteria for IT Security* is based on the *Common Criteria for Information Technology Security Evaluation 2.0*; thus, they are treated in one chapter. *Common Criteria* (CC) succeeds *Information Technology Security Evaluation Criteria* (ITSEC), published by the European Commission in 1991. The naming of those documents is synonymous.

DOCUMENT TAXONOMY

ISO/IEC 15408:2005 is an international standard. CC is labelled as a multipart standard.

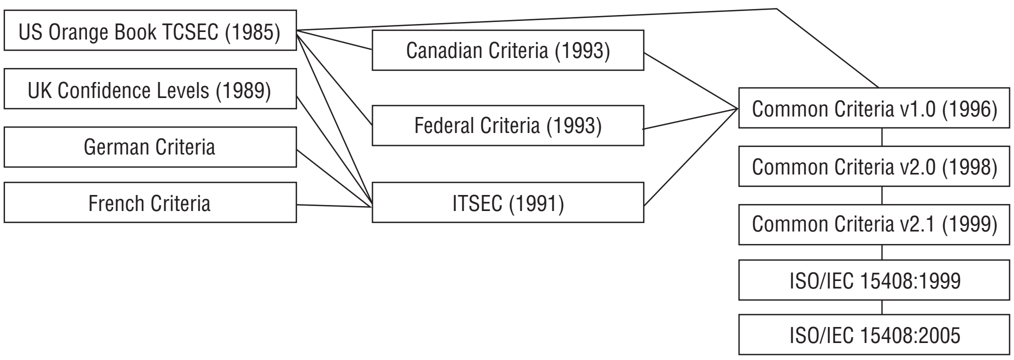
ISSUER

ISO/IEC 15408:2005 was published by the ISO/IEC JTC 1 working group in collaboration with the Common Criteria Project Sponsoring Organisation, which published CC. Members of this organisation include the following countries, which are represented by the corresponding agency/department:

- **Canada**—Communications Security Establishment
- **France**—Central Service of the Information System Security
- **Germany**—Federal Office for Security in Information Technology
- **The Netherlands**—The Netherlands National Communications Security Agency
- **United Kingdom**—Communications-Electronics Security Group
- **United States**—National Institute of Standards and Technology and National Security Agency

From an historic point of view, the various standards/guidance issued by some of the member bodies were influenced by other standards/guidance, as shown in **figure 5**.

Figure 5—Standards Influences


US Orange Book TCSEC (1985)
UK Confidence Levels (1989)
German Criteria
French Criteria
Canadian Criteria (1993)
Federal Criteria (1993)
ITSEC (1991)
Common Criteria v1.0 (1996)
Common Criteria v2.0 (1998)
Common Criteria v2.1 (1999)
ISO/IEC 15408:1999
ISO/IEC 15408:2005

GOAL OF THE STANDARD

The standard was issued to define criteria as the basis for a common and comparable evaluation of IT security, focusing on the security of systems and products.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

ISO/IEC 15408:2005/*Common Criteria*/ITSEC is usually implemented subject to one or more of the following business cases:

- Implementation of products or services that shall be certified
- Security imperative to the development of semi-finished products (e.g., control systems)

RELATED RISKS OF NON-COMPLIANCE

There is no direct risk for not complying unless the organisation has an inherent need to comply with this standard.

TARGET AUDIENCE

There are three specific target audiences mentioned:

- **Consumers**—The needs of consumers are considered throughout the evaluation process. The level of security provided by an evaluated product is comprehensible for consumers.
- **Developers**—Developers have a guideline to prepare the evaluation of their systems. On the other hand, CC helps in identifying security requirements and can be useful as a source of security functions that may be implemented into a system.
- **Evaluators**—Evaluators have clear and agreed-upon criteria to assess the security of a system. Steps necessary for an evaluation are included, but the standard does not stipulate procedures to be followed.

CC may be seen as a useful source of information by others, such as security and assurance professionals

TIMELINESS

CC was originally published in 1999 and updated in 2004. The currently valid version 2.2 (updated in 2004) differs only in formatting and minor changes to comply with ISO/IEC 15408:2005. *Common Criteria* 3.0 has been released for public comment, and the final version is scheduled to be issued in 2006.

CERTIFICATION OPPORTUNITIES

The purpose of the document is to provide common criteria for the certification of IT products and services, not individuals.

CIRCULATION

By being published as an international standard, CC has gained worldwide acceptance.

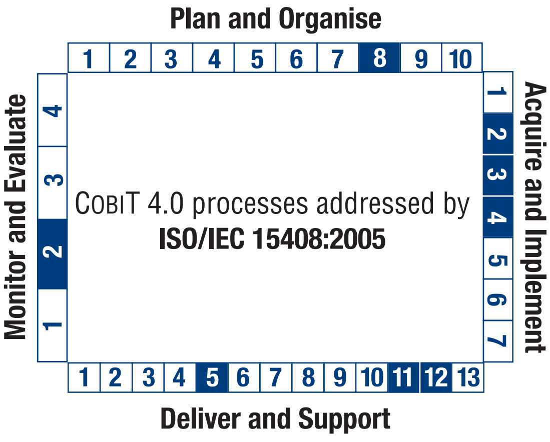
COMPLETENESS

From an IT governance point of view, the standard is not complete, as it does not address the full scope of IT management duties. Its focus is on IT products and services, not on IT management issues. However, it is very detailed.

AVAILABILITY

The international standard can be acquired from ISO. CC is freely available for public use.

CobiT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

	Information Criteria
-	Effectiveness
-	Efficiency
+	Confidentiality
+	Integrity
+	Availability
o	Compliance
+	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

	IT Resources
+	Applications
+	Information
+	Infrastructure
+	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

The *Common Criteria* and the internal standards consist of the following three parts.

Part 1—Introduction and General Model

Part 1 explains the general model, general concepts and principles to be considered when evaluating IT security. Constructs for expressing security objectives and for selecting and defining security requirements are provided. Instructions for writing high-level specifications for products and systems are given.

Part 2—Security Functional Requirements

Part 2 contains functional components that are used for expressing the security requirements of targets of evaluation (TOEs) in a standardised manner. It is structured into sets of functional components, families and classes.

The security classes—the highest level in the catalogue structure—are as follows:
- FAU—Security audit
- FCO—Communication
- FCS—Cryptographic support
- FDP—User data protection
- FIA—Identification and authentication
- FMT—Security management
- FPR—Privacy
- FPT—Protection of the TOE security function
- FRU—Resource utilisation
- FTA—TOE access
- FTP—Trusted path/channels

Part 3—Security Assurance Requirements

A set of assurance components is included in Part 3, enabling a standardised approach to defining assurance requirements for IT products and services. The structure of the catalogue is similar to the one in Part 2 in that it is subdivided into components, families and classes. Evaluation criteria for protection profiles (PPs) and security targets (STs) are also included in Part 3. The evaluation of the PP and the ST is to be performed before evaluating the TOE.

The evaluation criteria tasks for PPs are as follows:
- APE_DES—Description of the TOE
- APE_ENV—Security environment
- APE_INT—PP introduction
- APE_OBJ—Security objectives
- APE_REQ—IT security requirements
- APE_SRE—Explicitly stated IT security requirements (applicable only for an extended evaluation)

The ST evaluation tasks are as follows:
- ASE_DES—TOE description
- ASE_ENV—Security environment
- ASE_INT—ST introduction
- ASE_OBJ—Security objectives
- ASE_PPC—PP claims
- ASE_REQ—IT security requirements
- ASE_SRE—Explicitly stated IT security requirements (applicable only when evaluating extended requirements)
- ASE_TSS—TOE summary specification

Seven evaluation assurance levels (EALs) are presented, representing packages of assurance components. These EALs allow the IT security rating of products and services. For each EAL, a description of its objectives and minimal assurance components is provided.

The EALs identified within CC are as follows:
- EAL1—Functionally tested
- EAL2—Structurally tested
- EAL3—Methodically tested and checked
- EAL4—Methodically designed, tested and reviewed
- EAL5—Semi-formally designed and tested
- EAL6—Semi-formally verified design and tested
- EAL7—Formally verified design and tested

FURTHER REFERENCES

Internet	
ISO	*www.iso.org*
IEC	*www.iec.org*
NIST (CC)	*www.nist.gov*

9. PRINCE2

DOCUMENT TAXONOMY

Projects in Controlled Environments (PRINCE) provides a structured method for effective project management, published in a single document, *Managing Successful Projects With PRINCE2*. Although produced and published by a single governmental body, PRINCE2 is not a standard.

ISSUER

PRINCE2 was launched in 1996 in response to user requirements for improved guidance on project management on all projects, not just information systems. The PRINCE method was first established in 1989 by the Central Computer and Telecommunications Agency (CCTA), now the British Office of Government Commerce (OGC). OGC continues to develop the method.

GOAL OF THE PUBLICATION

The goal of PRINCE2 is to define a project management method to provide a framework covering the wide variety of disciplines and activities required within a project. The focus throughout PRINCE2 is on the business case, which describes the rationale and business justification for the project. The business case drives all the project management processes, from initial project setup to successful finish.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

PRINCE2 is usually implemented subject to one or more of the following business cases:

- Establishing a common understanding of the processes, responsibilities and accountabilities for project management
- Providing for a consistent approach to project management, no matter the type of project
- Ensuring the active involvement of users and stakeholders
- Ensuring that there is a focus on business outcomes during project decision making
- Adopting proven best practice for project management

RELATED RISKS OF NON-COMPLIANCE

Project failure through a lack of consistency in the organisation approach is a risk of non-compliance.

TARGET AUDIENCE

PRINCE2 focuses on organisations of varying size.

TIMELINESS

OGC continues to update PRINCE2. The latest release was in 2005.

CERTIFICATION OPPORTUNITIES

There are two levels of certification of personnel:

- Foundation Certificate—The examination is a one-hour, 75-question, multiple-choice test.
- Registered Practitioner—This is a three-hour examination with three case-scenario-based questions. There are a total of 150 marks offered, and a score of 75 is passing. This examination is open book, which means examinees are allowed to bring into the examination room any notes or reference material they wish. PRINCE2 Registered Practitioners must take the re-registration examination every three to five years to maintain their certification. This is a similar examination to the original practitioner examination, except it is only a one-hour exam with one scenario-based question.

The APM Group Limited (APMG) is the certification body for PRINCE2, accredited by United Kingdom Accreditation Service (UKAS). APMG has been working as a strategic partner of OGC since 1996 on the development and promotion of professional standards associated with the use and implementation of PRINCE2. The group's activities extend beyond the UK.

CIRCULATION

PRINCE2 is used internationally; however, it is available only in English.

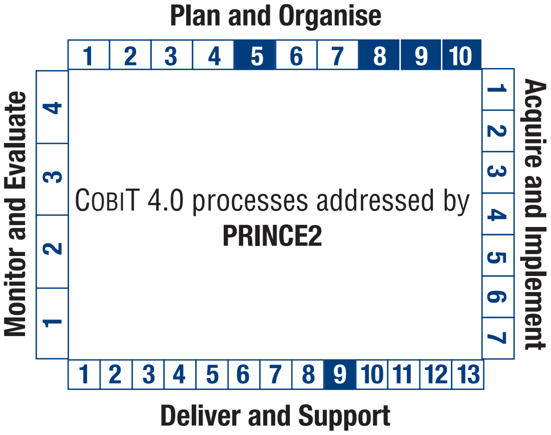
COMPLETENESS

PRINCE2 provides a project management methodology and does not address IT management and IT governance issues specifically.

AVAILABILITY

PRINCE2 is available for purchase as a paperback and a CD-ROM.

COBIT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

	Information Criteria
+	Effectiveness
+	Efficiency
-	Confidentiality
-	Integrity
-	Availability
-	Compliance
-	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

	IT Resources
-	Applications
-	Information
-	Infrastructure
+	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

PRINCE2 is a process-based project management methodology that is scalable to meet organisations' requirements, depending on project complexity and risk.

A core concept within the PRINCE2 methodology is that projects are segmented into manageable stages, enabling efficient control of resources and regular progress monitoring throughout the project. The project manager has control of a project on a day-to-day basis within a stage, as long as the projects stay within tolerances defined by the project board.

Project planning using PRINCE2 is product-based, which means the project plans are focused on delivering results and are not simply about planning when the various activities of the project will be done.

The PRINCE2 process model consists of eight distinct management processes, from setting the project off on the right track, through controlling and managing the project's progress, to the completion of the project. The common planning (PL) process is used by four of the other processes. The eight processes of the PRINCE2 process model are:

1. Starting up a project (SU) is the first process in PRINCE2. It is a pre-project process, designed to ensure that the prerequisites for initiating the project are in place. The process expects the existence of a project mandate that defines in high-level terms the reason for the project and what product is required. The process should be very short.
2. Directing a project (DP) is aimed at the project board, a group of managerial decision makers representing business, users and suppliers. The project board manages by exception, monitors via reports and controls through a number of decision points.
3. Initiating a project (IP) is aimed at planning and costing the projects, reviewing and confirming the business cases, and providing the baseline for decision making once approved by the project board. The key product of this process is the project initiation document, which defines the what, why, who, when and how of the project.
4. Managing stage boundaries (SB) produces the information on which the project board will take key decisions on whether to continue with the project or not. Activities in this process should verify that all products planned in the current stage plan have been completed as required, provide the project board with any other information needed to approve the current stage's completion, authorise the start of the next stage, and record any measurements or lessons that can help later stages of this and/or other projects. The key product of this process is an end stage report, given by the project manager to the project board, containing information on the stage achievements, a revised project plan and a plan for the next stage.
5. Controlling a stage (CS) is the activities that should be undertaken by a project manager to control work, react to events and report to the project board.
6. Managing product delivery (MP) consists of those processes relating to the creation and delivery of products. This involves the specification and acceptance of work packages as well as team management activities in defining, delivering and accepting work packages.
7. Closing a project (CP) is the processes required from the project manager's work to wrap up the project either at its end or at a premature close. Most of the work is to prepare input to the project board to obtain its confirmation that the project may close.
8. Planning (PL) is the processes required for development plans at various stages in the project life cycle.

All projects need to address each of these processes in some form. However, the key to successful use of the process model is in tailoring it to the needs of the individual project. Each process should be approached with this question: How extensively should this process be applied to this project?

In addition, PRINCE2 describes a number of components that are applied within the appropriate activities. PRINCE2 provides guidance as to how each affects project management and provides guidance on when and how to address the issues as part of the various processes. The components include a business case, organisation (project team, responsibilities and relationships), plans (project plan, stage plan, team plan, quality plans, exception plan) and controls (e.g., monitor progress, detect problems), management of risk, quality in project management, configuration management, and change control.

FURTHER REFERENCES

Internet	
OGC	*www.ogc.gov.uk*
APM	*www.apmgroup.co.uk*

10. PMBOK

DOCUMENT TAXONOMY

A Guide to the Project Management Body of Knowledge (PMBOK) is described as ‘the sum of knowledge within the profession of project management’. PMBOK is an American National Standard, ANSI/PMI 99-001-2004.

ISSUER

PMBOK is published by the Project Management Institute (PMI).

GOAL OF THE PUBLICATION

The primary purpose of PMBOK is to ‘identify that subset of *The Project Management Body of Knowledge* that is generally recognised as good practice’. The PMBOK guide ‘provides and promotes a common lexicon for discussing, writing and applying project management’.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

PMBOK is usually implemented subject to one or more of the following business cases:

- To establish a common lexicon of the processes for project management
- To gain knowledge of proven best practice for project management

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing PMBOK include:

- Inconsistent project management practices
- Increased risk of project failure

TARGET AUDIENCE

PMBOK is aimed at providing a foundational reference for anyone interested in the profession of project management.

TIMELINESS

PMBOK has been subject to periodic review and update since it was initially published in 1983. The most recent update was in 2004.

CERTIFICATION OPPORTUNITIES

PMI offers the Project Management Professional (PMP) certification programme for project managers. This is based on a Project Management Professional Examination Specification for the examination, describing the tasks (competencies) that PMPs perform, and the project management knowledge and skill PMPs use to complete each task.

CIRCULATION

PMBOK Guide is used internationally and is available in Arabic, Chinese, English, French, German, Italian, Japanese, Korean, Portuguese, Russian and Spanish

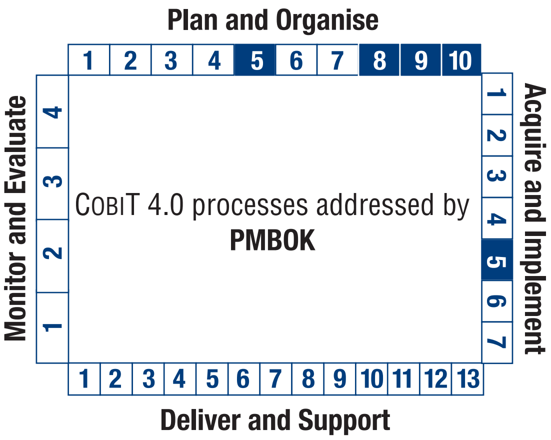
COMPLETENESS

PMBOK provides great detail on the practices and techniques required to achieve sound project management. However, while the processes and techniques described in PMBOK are applicable to projects involving IT, they do not cover IT management and IT governance issues specifically.

AVAILABILITY

PMBOK is available for purchase as a paperback and a CD-ROM.

COBIT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria	
+	Effectiveness
+	Efficiency
-	Confidentiality
-	Integrity
-	Availability
-	Compliance
-	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

IT Resources	
-	Applications
-	Information
-	Infrastructure
+	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

PMBOK presents project management practices in two groups or dimensions. One presents project management processes segmented into five process groups. The other is knowledge areas for project management.

The five process groups are:
1. Initiating—Defines and authorises the project or a project phase
2. Planning—Defines and refines objectives, and plans the course of action required to attain the objectives and scope that the project was undertaken to address
3. Executing—Integrates people and other resources to carry out the project management plan for the project
4. Controlling—Regularly measures and monitors progress to identify variances from the project management plan so corrective action can be taken when necessary to meet project objectives
5. Closing—Formalises acceptance of the product, service or result and brings the project or project phase to an orderly end

Each PMBOK knowledge area describes project management knowledge and practice in terms of one or more processes. Each process is further described in terms of its inputs, outputs, tools and techniques.

The knowledge areas are:
1. Project integration management—The processes and activities that integrate the various elements of project management, which are identified, defined, combined, unified and co-ordinated within the project management process groups. It consists of the project charter development, preliminary project scope statement development, project management plan development, project execution direction and management, project work monitoring and control, change control integration, and closure of project management processes.
2. Project scope management—The processes involved in ascertaining that the project includes all the work required, and only the work required, to complete the project successfully. It consists of the scope planning, scope definition, work breakdown structure (WBS) creation, scope verification and scope control of project management processes.
3. Project time management—The processes concerning the timely completion of the project. It consists of the activity definition, activity sequencing, activity resource estimating, activity duration estimating, schedule development and schedule control of project management processes.
4. Project cost management—The processes involved in planning, estimating, budgeting and controlling costs, so the project is completed within the approved budget. It consists of the cost estimating, cost budgeting and cost control of project management processes.
5. Project quality management—The processes involved in assuring that the project will satisfy the objectives for which it was undertaken. It consists of the quality planning, quality assurance performance and quality control performance of project management processes.
6. Project human resource management—The processes that organise and manage the project team. It consists of the human resource planning, project team acquisition, project team development and project team management of project management processes.
7. Project communications management—The processes concerning the timely and appropriate generation, collection, dissemination, storage and ultimate disposition of project information. It consists of the communications planning, information distribution, performance reporting and stakeholders management of project management processes.
8. Project risk management—The processes concerned with conducting risk management on a project. It consists of the risk management planning, risk identification, qualitative risk analysis, quantitative risk analysis, risk response planning, and risk monitoring and control of project management processes.
9. Project procurement management—The processes concerned with purchasing or acquiring products, services or results, as well as contracting management processes. It consists of the purchases and acquisitions planning, contracting planning, seller responses request, sellers selection, contract administration and contract closure of project management processes.

The relationship between the processes and knowledge area is shown in **figure 6**.

Figure 6—Relationship of Processes Within Knowledge Areas to Project Management Phases

Project Management Phases	Project Management Process Groups				
	Initiating Process Group	Planning Process Group	Executing Process Group	Monitoring and Controlling Process Group	Closing Process Group
Project integration management	• Project charter development • Preliminary project scope statement development	• Project management plan development	• Project execution direction and management	• Project work monitoring and control • Integrated change control	• Project closure
Project scope management		• Scope planning • Scope definition • WBS creation		• Scope verification • Scope change control	
Project time management		• Activity definition • Activity sequencing • Activity resource estimating • Activity duration estimating • Development scheduling		• Schedule control	
Project cost management		• Cost estimating • Cost budgeting		• Cost control	
Project quality management		• Quality planning	• Quality assurance performance	• Quality control performance	
Project human resources management		• Human resource planning	• Project team acquisition • Team development	• Project team management	
Project communication management		• Communication planning	• Information distribution	• Performance reporting • Stakeholders management	
Project risk management		• Risk management planning • Risk identification • Qualitative risk analysis • Quantitative risk analysis • Risk response planning		• Risk monitoring and control	
Project procurement management		• Procurement and acquisitions planning • Contract planning	• Seller responses request • Seller selection	• Contract administration	• Contract close-out

Source: Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 3rd Edition*, 2004, figure 3-45

FURTHER REFERENCES

Internet	
PMI	*www.pmi.org*

11. TickIT

DOCUMENT TAXONOMY

TickIT is a scheme for assessment and certification of an organisation's software quality management system.

ISSUER

TickIT is published and maintained by TickIT Office, which is a business unit within the British Standards Institution.

GOAL OF THE PUBLICATION

Software developers are encouraged to think about:
- The quality that is intrinsic to the process of software development
- Achieving the quality objectives
- Continuous improvement of the quality management system

The objective is the development of a framework for the management of software development that enables efficient certification of quality management systems. To reach this objective, the following steps have been taken:
- Creation of a guide that facilitates interpretation of the ISO 9001:2000 requirements
- Improvement of auditors' knowledge and provision of information on registered auditors with expertise and competence
- Creation of rules to accredit prospective certification bodies for the software sector

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

TickIT is usually implemented subject to one or more of the following business cases:
- The requirement of a certification of the quality management system
- The need for guidance on the specification of requirements
- Software as an integrated part of the product (e.g., in embedded systems)
- Subcontracting of third parties and dependence of the organisation on the quality of the software delivered

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing TickIT include:
- Inadequate or ineffective control of the complex area of software development
- Incomplete specification of requirements

TARGET AUDIENCE

TickIT is for organisations in which software development adds significant value to the organisation's products or services. Thus, it is relevant for senior managers, operational bodies and accreditation authorities. TickIT is focused on three audiences:
- **Customers**—How the customer can influence the quality of the product
- **Suppliers**—Including in-house developers, who intend to improve the effectiveness of their quality management system
- **Auditors**—How to assess the procedures defined within TickIT

TIMELINESS

The current version was published in 2001 and considers the modifications of the framework of ISO 9000.

CERTIFICATION OPPORTUNITIES

A certification of an organisation's quality management system is available, indicating the adoption of the TickIT scheme for quality management. Moreover, TickIT is used to accredit certification bodies. The ISO 9001:2000 standard is an internationally recognised quality management system standard developed by ISO. ISO 9001:2000 certification is the same as the TickIT certification. TickIT certification is available for auditors.

CIRCULATION

TickIT is of British origin, but it is used in several European countries. Information provided on the TickIT web site reports that there were 1,093 TickIT active certificates as of June 2004.

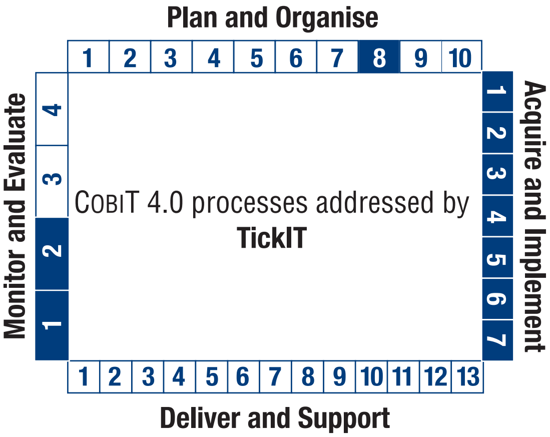
COMPLETENESS

TickIT has a clear focus on software development and related quality management systems; thus, it is classified as narrow and does not address many areas of IT governance. In addition, TickIT is not very detailed.

AVAILABILITY

A printed version can be acquired from the TickIT web site, and a CD-ROM is also available

COBIT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria
+ Effectiveness
+ Efficiency
+ Confidentiality
+ Integrity
+ Availability
+ Compliance
+ Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

It should be noted that TickIT is focused on a quality management system; consequently, the information criteria and IT resources addressed are also concerned with software development and the related quality management system.

IT RESOURCES ADDRESSED

IT Resources
+ Applications
+ Information
+ Infrastructure
+ People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

TickIT can be used to support the development of all types of software, including operating systems, embedded systems or software for office use. It is based on ISO 9000-3 (*Quality Management and Quality Assurance Standards—Part Three: Guidelines for the Application of ISO 9001:1994 to the Development, Supply, Installation and Maintenance of Computer Software*) and adds information to the guidelines by providing additional guidance for customers, suppliers and auditors. It also contains clear requirements for auditors that must be met when accredited by certification bodies, including:

- **Guidance for customers**—Part B (succeeding the introductory part A) contains issues relating to the certification of a quality management system for software from the customer's point of view. The role of the customer is to initiate a development project; thus, the customer is informed on how he/she can contribute to the quality of the product and services.
- **Guidance for suppliers**—Part C describes information and guidance for the quality management system of suppliers using the TickIT procedures. Suppliers can be organisations providing software services as well as in-house developers. Assessing and improving the effectiveness of the organisation's quality management system is also part of this chapter.
- **Guidance for auditors**—Part D contains guidance for auditors on how to perform an assessment using the procedures provided by TickIT.
- **Software quality management system requirements (standards perspective)**—This part follows the sequence of ISO 9001. It presents information and guidance on how to interpret the requirements of ISO 9001, focusing on organisations producing software products.
- **Software quality management system requirements (process perspective)**—Effective and continuous control of a software quality management system is essential for the quality of the product. Good practice is provided, assisting organisations with improvement of their quality management system. It follows the basic processes and structure of ISO/IEC 12207 (*Information Technology—Software Life Cycle Processes*).

FURTHER REFERENCES

Internet	
TickIT	*www.tickit.org*
ISO	*www.iso.org*

12. CMMI

DOCUMENT TAXONOMY

The publication *Capability Maturity Model Integration*® (CMMI) is a best practice document used as guidance for improving processes. It provides models for system engineering, integrated product and process development, and supplier sourcing.

ISSUER

CMMI is published by the Software Engineering Institute (SEI) of Carnegie Mellon University, Pittsburgh, Pennsylvania, USA. CMMI is based on the more generic Capability Maturity Model (CMM).

GOAL OF THE PUBLICATION

The goal mentioned on the cover of the publication is 'improving processes for better products', which widens the basic intention of providing guidance to use when developing processes.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

CMMI is usually implemented subject to one of more of the following business cases:

- Assessing the current maturity of processes
- Improving processes and organisational structures, following an accepted best practice approach
- Requirement for benchmarking processes with other organisations
- Improving productivity and lowering project risks
- Reducing software defects
- Improving customer satisfaction

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing CMMI include:

- Ineffective approach for process improvement
- Inefficient approach for process improvement
- Inability to benchmark process maturity
- Low project and product quality due to undefined processes
- Ineligibility for government contracts

TARGET AUDIENCE

The guideline targets systems and software developers; systems, program and software managers; practitioners of disciplines that support systems and software; and government and industry acquirers of software-intensive systems.

TIMELINESS

Version 1.1 was published in 2002 and is still up to date.

CERTIFICATION OPPORTUNITIES

A number of organisations offer assessments of process maturity. Process maturity appraisals are performed using SEI's Standard CMMI Appraisal Method for Process Improvement (SCAMPI) or ISO/IEC 15504. Individuals can be certified as SEI CMMI assessors.

CIRCULATION

The publication is used internationally by many organisations. The documents are in English; however, Japanese and traditional Chinese versions are also available.

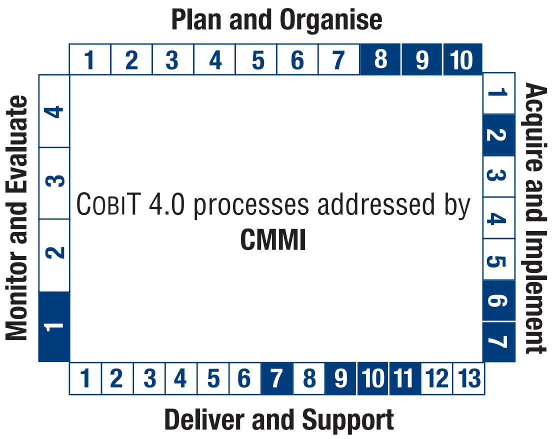
COMPLETENESS

The models are focused on system development and, therefore, cover only a limited range of IT governance and management issues. However, the details provided are comprehensive.

AVAILABILITY

The guidance is posted for complimentary download from the CMMI web site. Printed versions are not available from the publisher.

CobiT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria	
+	Effectiveness
+	Efficiency
o	Confidentiality
o	Integrity
o	Availability
o	Compliance
+	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES ADDRESSED

IT Resources	
+	Applications
-	Information
+	Infrastructure
+	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

CMM provides a model for developing processes and identifying the key practices required to increase the maturity of the software improvement process, but CMM does not provide the processes themselves or process descriptions. The model can be used to define process improvement objectives and priorities, improve processes, and provide guidance for ensuring stable, capable and mature processes.

The CMMI project is based upon various capability maturity models.[4] CMMI currently provides four bodies of knowledge, also referred to as disciplines.

Disciplines

CMMI accommodates multiple disciplines and supports two different representations, namely the staged representation and the continuous representation. Currently, an organisation can select from the following four disciplines (models) integrated into the CMMI project:

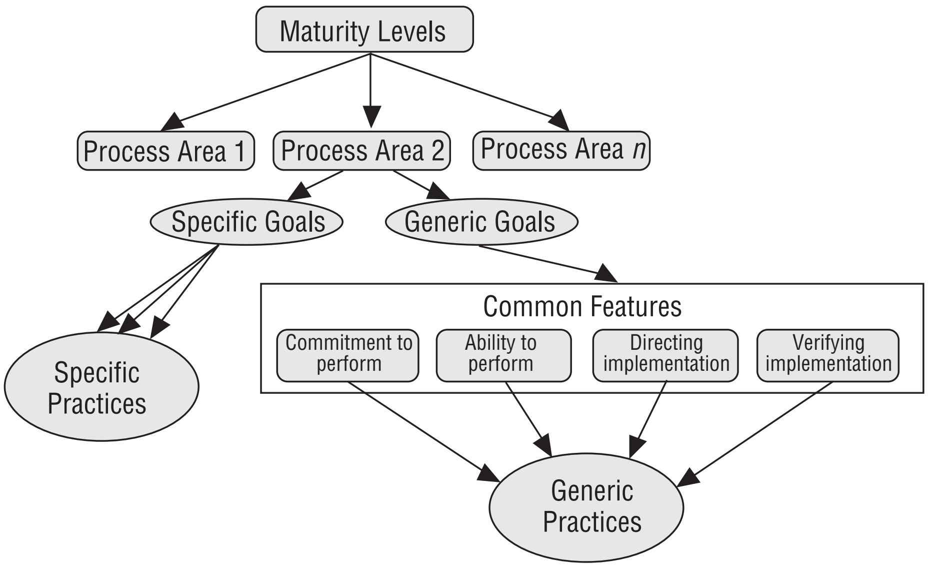
- **Systems engineering**—This discipline covers the development of systems, which may or may not include software. The focus is on transforming customer needs, expectations and constraints into product solutions, and supporting these product solutions throughout the life of the product.
- **Software engineering**—This discipline covers the development of software. The content is directed at applying systematic, disciplined and quantifiable approaches to the development, operation and maintenance of software.
- **Integrated product and process development (IPPD)**—IPPD defines a systematic approach that achieves a timely collaboration of relevant stakeholders throughout the life of the product. This aims at a higher satisfaction of customer needs, expectations and requirements. The need for integration with other processes throughout the organisation is stated.
- **Supplier sourcing**—This discipline covers acquiring products from suppliers. Acquisition may be required if suppliers are used to perform functions or add modifications to products. As projects may benefit (or risks may be lowered) from enhanced source analysis and monitoring supplier activities, supplier sourcing should be performed in a defined manner.

It is recommended to choose the systems engineering discipline together with the software engineering discipline, rather than choosing either one of them alone.

Model Components

The model components of CMMI are depicted in **figure 7**.

Figure 7—CMMI Model Components



[4] Since 1991, Carnegie Mellon University has developed capability maturity models (CMMs) for a wide range of disciplines.

Process Area Categories

The process areas of CMMI are structured in the following four categories:

- **Process management**—Cross-project activities related to defining, planning, resourcing, deploying, implementing, monitoring, controlling, appraising, measuring and improving processes. The process areas in this category are organisational process focus, organisational process definition, organisational training, organisational process performance, and organisational innovation and deployment.
- **Project management**—Activities related to planning, monitoring and controlling a project. The area consists of project planning, project monitoring and control, supplier agreement management, integrated project management for IPPD (or integrated project management), risk management, integrated teaming, integrated supplier management, and quantitative project management.
- **Engineering**—The development and maintenance activities that are shared across engineering disciplines (e.g., systems engineering and software engineering). The engineering process area contains six interrelated areas: project planning, project monitoring and control, supplier agreement management, integrated project management for IPPD (or integrated project, management), risk management, integrated teaming, integrated supplier management, and quantitative project management.
- **Support**—Activities that support product development, maintenance and processes that are used in the context of performing other processes within this category, which encompasses the following areas: configuration management, process and product quality assurance, measurement and analysis, organisational environment for integration, decision analysis and resolution, and causal analysis and resolution.

Capability Levels

Capability levels apply to an organisation's process improvement achievement for each process area. A generic goal and a set of generic and specific practices are provided. The capability levels are:

- **0**—Incomplete
- **1**—Performed
- **2**—Managed
- **3**—Defined
- **4**—Quantitatively managed
- **5**—Optimising

Maturity Levels

The overall maturity of an organisation is defined by its maturity level. The maturity levels belong to the staged representation of the model. A predefined set of process areas are presented and discussed in detail in the standard.

- **1**—Initial
- **2**—Managed
- **3**—Defined
- **4**—Quantitatively managed
- **5**—Optimising

An organisation is not advised to skip levels when advancing through them. This is considered counterproductive because each level is based on the ones below it.

The objective of the CMMI project effort is to reduce the cost of establishing and maintaining process improvement efforts across an enterprise using multiple disciplines to produce products or services. The standard also describes how organisations can use CMMI models for process improvement and benchmarking. The last chapter, the most comprehensive part of the standard, contains detailed descriptions for each process area.

FURTHER REFERENCES

Internet	
CMMI	*www.sei.cmu.edu/cmmi*
ISO	*www.iso.org*

13. TOGAF 8.1

DOCUMENT TAXONOMY

The Open Group Architecture Framework (TOGAF) is a detailed method and set of supporting tools for developing an enterprise architecture.

ISSUER

Members of The Open Group, working within the Architecture Forum, developed TOGAF. TOGAF has been in existence since 1995 when the newly created Architecture Forum developed the first version based on the US Department of Defense (DoD) Technical Architecture Framework for Information Management (TAFIM). The DoD gave The Open Group explicit permission and encouragement to create TOGAF by building on TAFIM. The members of The Open Group Architecture Forum have developed successive versions of TOGAF that are published on The Open Group public web site.

GOAL OF THE PUBLICATION

The Open Group operates as a not-for-profit consortium committed to delivering greater business efficiency by bringing together buyers and suppliers of information systems to lower the barriers of integrating new technology across the enterprise. Its goal is to realise the vision of Boundaryless Information Flow™.

TOGAF is a key part of its strategy for achieving this goal, and The Open Group wants TOGAF to be taken up and used in practical architecture projects, and the experience from its use fed back to help improve it.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

TOGAF 8.1 is usually implemented subject to one or more of the following business cases:

- Facilitating business and IT alignment by providing the fundamental technology and process structure for an IT and/or business strategy
- Managing intellectual capital by formalising models across architecture domains
- Improving business/IT effectiveness and efficiency
- Reducing risk for future investment and deriving better return on existing investment
- Managing complexity and change

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing TOGAF 8.1 include:

- Increased complexity and cost of ownership
- Fragmentation of information resources
- Reduced organisational agility
- Reduced innovation capability

TARGET AUDIENCE

TOGAF focuses on organisations of varying size. It targets those responsible for enterprise architecture management, strategic planning, the acquisition and implementation of business systems, risk management, and organisational development.

TIMELINESS

The publications state they will be updated in a frequent and ongoing manner. Two versions of TOGAF are available:

- TOGAF Version 8 (Enterprise Edition), first published in December 2002 and republished in updated form as TOGAF Version 8.1 in December 2003
- TOGAF Version 7 (Technical Edition), published in December 2001

TOGAF Version 8 focuses particular attention on technical architectures, but uses the same underlying architecture development method evolved from the earlier versions. It applies that architecture development method to all the domains of an overall enterprise architecture, including business, data (information) and application architecture, as well as technical architecture.

TOGAF Version 9 is due for release in late 2006 and will provide additional focus on the following themes:

- The enterprise, culture and stakeholders
- Enterprise architecture creation
- Enterprise architecture-based transformation
- Enterprise architecture deployment
- Enterprise architecture realisation
- Enterprise architecture management and governance

CERTIFICATION OPPORTUNITIES

TOGAF certification is for individuals and organisations. Individuals can become certified by demonstrating their knowledge of TOGAF by attending a training course or passing an examination. Organisations can have their products (TOGAF tools or training courses) and services certified.

CIRCULATION

TOGAF is used internationally; however, it is available only in English. A Japanese version has recently been produced, but is not yet publicly available.

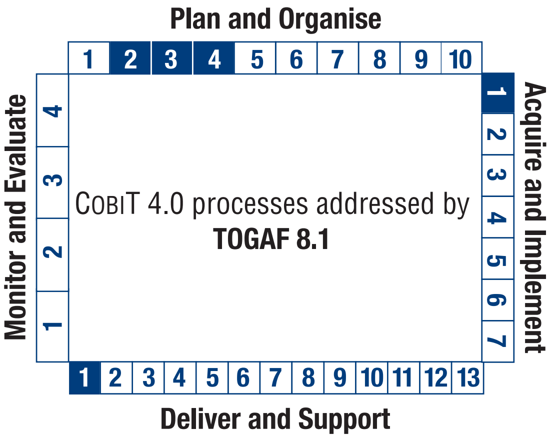
COMPLETENESS

TOGAF provides a common-sense, practical and effective method of developing enterprise architecture.

AVAILABILITY

TOGAF is published by The Open Group on its public web server. In addition, TOGAF 8.1 (Enterprise Edition) is published in book format.

COBIT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria	
+	Effectiveness
+	Efficiency
o	Confidentiality
o	Integrity
o	Availability
-	Compliance
o	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES CONCERNED

IT Resources	
+	Applications
+	Information
+	Infrastructure
-	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

TOGAF consists of three parts:

1. The TOGAF Architecture Development Method (ADM) explains how to derive an organisation-specific enterprise architecture that addresses business requirements. The ADM provides:
   - A reliable, proven way of developing the architecture
   - Architecture views that enable the architect to ensure that a complex set of requirements is adequately addressed
   - Linkages to practical case studies
   - Guidelines on tools for architecture development
2. The Enterprise Continuum is a virtual repository of all the architecture assets—models, patterns, architecture descriptions, etc.—that exist both within the enterprise and in the IT industry at large, which the enterprise considers itself to have available for the development of architectures. At relevant places throughout the TOGAF ADM, there are reminders to consider which architecture assets from the Enterprise Continuum the architect should use, if any. TOGAF itself provides two reference models for consideration for inclusion in an enterprise's own Enterprise Continuum:
   - The TOGAF Foundation Architecture, an architecture of generic services and functions that provides a foundation on which specific architectures and architectural building blocks can be constructed. The Foundation Architecture in turn includes:
     - The TOGAF Technical Reference Model (TRM), which provides a model and taxonomy of generic platform services
     - The TOGAF Standards Information Base (SIB), a database of open industry standards that can be used to define the particular services and other components of an enterprise-specific architecture
   - The Integrated Information Infrastructure Reference Model, which is based on the TOGAF Foundation Architecture and is specifically aimed at helping the design of architectures that enable and support the vision of Boundaryless Information Flow
3. The TOGAF Resource Base, which is a set of resources, including guidelines, templates and background information, to help the architect in the use of the ADM

FURTHER REFERENCES

Internet	
The Open Group	*www.opengroup.org*
Architecture Forum	*www.opengroup.org/architecture/*
TOGAF 8.1	*www.opengroup.org/architecture/togaf8-doc/arch*

14. IT Baseline Protection Manual

DOCUMENT TAXONOMY

The *IT Baseline Protection Manual* (BPM) is a handbook recommending standard security safeguards for typical IT systems.

ISSUER

The manual was published by the German BSI (Bundesamt für Sicherheit in der Informationstechnik—Federal Office for Information Security).

GOAL OF THE PUBLICATION

The purpose of the recommendations in this manual is to define and achieve a security level for IT systems that is adequate and sufficient to satisfy the requirements for protecting information and assets. The IT BPM can be used as a basis for highly sensitive IT systems and applications. The information security baseline is accomplished by implementing suitable organisational, personal, infrastructural and technical standard security measures.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

IT BPM is usually implemented subject to one or more of the following business cases:

- Need to define a security baseline
- Requirement for information security best practice information on a technical level
- Improvement of information system security
- Need for certification

RELATED RISKS OF NON-COMPLIANCE

Risk of not implementing IT BPM include:

- Insecure systems
- No ability to audit information systems against an agreed baseline
- Inefficient methodology to ensure information systems security

TARGET AUDIENCE

The manual is intended primarily for public authorities and companies aiming to implement IT security concepts. Due to its technical bias, the manual is also useable by producers of hardware and/or software. Moreover, certification service providers can be seen as a target audience since certifications are possible regarding compliance with the IT BPM. It is to be noted that the catalogue of safeguards defines responsibilities for initiation and realisation.

TIMELINESS

According to the publication, the manual is updated every six months. The topics being updated are prioritised based upon a poll.

CERTIFICATION OPPORTUNITIES

The German BSI provides criteria for certifying public authorities or companies concerning their compliance with the recommendations in the baseline protection manual. A list of certification service providers is available on the German BSI's web site.

CIRCULATION

As a publication of a German federal agency, the manual originally had only regional importance; however, as the standard is also available in English, it is used internationally.

COMPLETENESS

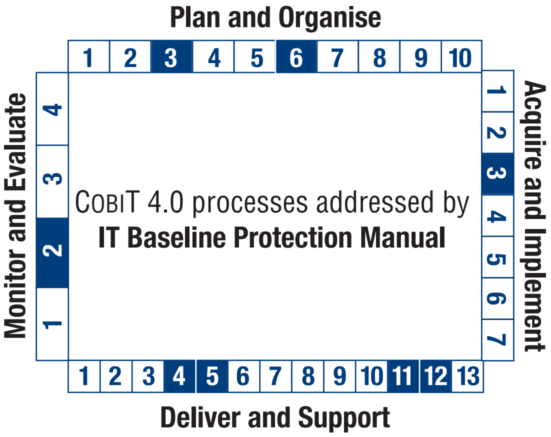
In the current version, the IT BPM consists of more than 2,300 pages with a strong technical bias and detailed technical instructions.

Consequently, the manual—as technical guidance—can be seen as very extensive and detailed. The manual explicitly does not deal with the software development process, particularly with application controls addressing the development and changes of software, which is crucial in the scope of IT governance. Thus, the IT BPM can be considered deep, but not broad and sufficient.

AVAILABILITY

The IT BPM is available as a loose-leaf collection (with update sheets) in electronic form and can be downloaded from the German BSI's web site.

COBIT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria

- - Effectiveness
- - Efficiency
- + Confidentiality
- + Integrity
- + Availability
- - Compliance
- - Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES ADDRESSED

IT Resources

- o Applications
- o Information
- + Infrastructure
- + People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

The manual is suitable for:

- IT security process and IT security management
- IT structure analysis
- Assessment of protection requirements
- IT baseline protection modelling
- Basic security check
- Supplementary security analysis
- Implementation of IT security safeguards
- IT baseline protection certificate

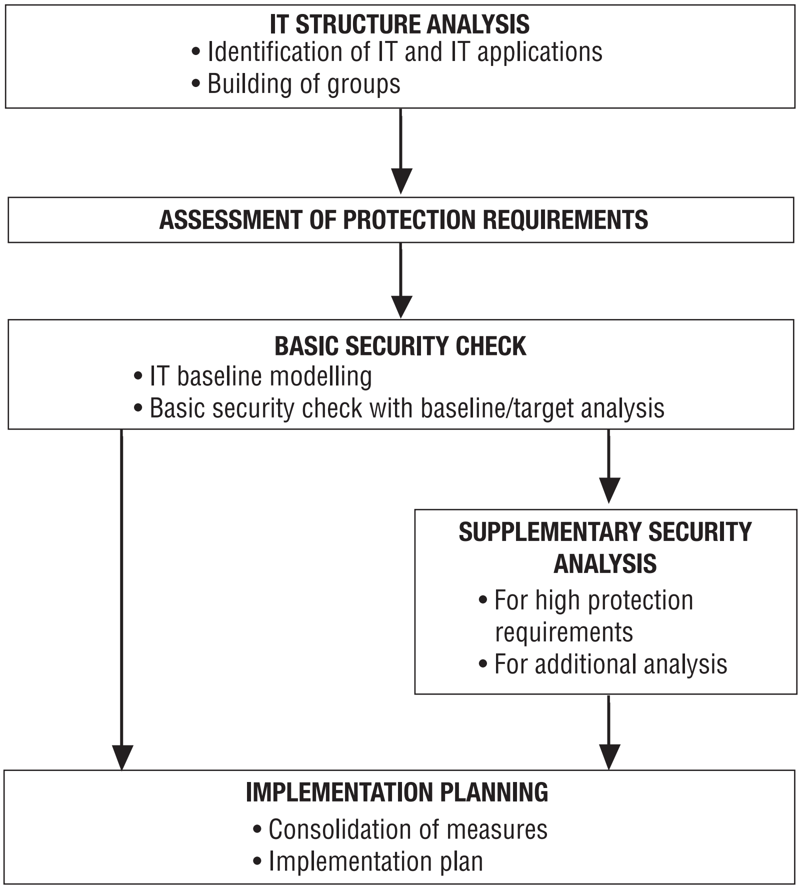
After an introduction, the manual includes instruction on how to implement an adequate security level, followed by a description of the modules and a catalogue of threats and safeguards.

The IT baseline protection modelling (and the corresponding identification of whether the security level is appropriate) is displayed in **figure 8.**

The assessment of protection requirements addresses the point in time at which the control system requirements are defined; its required functionality can be seen in the implementation planning phase.

The chapter about the assessment of protection requirements defines categories for protection requirements (low to middle, high and very high), to which IT structural elements (as result of the IT structure analysis) can be mapped. Additionally, follow-up damages have to be assessed, and elements have to be moved to a higher category if dependent elements are part of such a higher-ranked category. The results have to be documented and processed, as shown **figure 7**.

Figure 8—Modelling an IT Security Concept


IT STRUCTURE ANALYSIS
• Identification of IT and IT applications
• Building of groups
ASSESSMENT OF PROTECTION REQUIREMENTS
BASIC SECURITY CHECK
• IT baseline modelling
• Basic security check with baseline/target analysis
SUPPLEMENTARY SECURITY ANALYSIS
• For high protection requirements
• For additional analysis
IMPLEMENTATION PLANNING
• Consolidation of measures
• Implementation plan

Source: *www.bsi.de*

The modules are structured as follows:

- **IT baseline protection of generic components:**
  - **IT security management**—A useful implementation of IT security measures is based upon an elaborate IT security process. The corresponding planning and controlling tasks are called IT security management.
  - **Organisation**—Collection of organisational measures to reach a minimum protection level
  - **Personnel**—Standard baseline protection measures in human resources, e.g., introductory courses for new employees
  - **Contingency planning concept**—Recovery measures in case of failure of an IT system (in four stages: contingency planning, implementing the contingency measures accompanying IT operation, emergency preparedness exercises, and implementing planned measures after an emergency situation arises)
  - **Data backup policy**—Preparation of a data backup policy for IT systems in case of technical failure, inadvertent deletion or manipulation
  - **Data protection**—Protecting individuals from impairment of personal data
  - **Computer virus protection concept**—Suitable safeguards to prevent or detect as early as possible computer viruses in the organisation's IT systems
  - **Crypto-concept**—Cryptographic procedures and techniques for a heterogeneous environment to protect effectively the data stored locally and the data to be transmitted
  - **Handling of security incidents**—To maintain IT security in ongoing operations, it is necessary to have developed and practise a policy for the handling of security incidents.
  - **Hardware and software management**—Procedures and processes that affect IT systems in such a way that the targeted IT security level can be achieved and maintained
  - **Outsourcing**—The use of external service providers for all or part of the work or business processes
- **Infrastructure:**
  - Buildings
  - Cabling
  - Rooms (office, server room, data media archives, technical infrastructure room)
  - Protective cabinets
  - Working place at home (telecommuting)
  - Computer centre
- **Non-networked systems:**
  - DOS PC (single user)
  - UNIX system
  - Laptop
  - PC with a non-constant user population
  - PC under Windows NT
  - PC with Windows 95
  - Windows 2000 Client
  - Internet PC
  - Stand-alone IT systems
- **Networked systems:**
  - Server-supported network
  - UNIX servers
  - Peer-to-peer services
  - Windows NT network
  - Novell Netware 3.x
  - Novell Netware 4.x
  - Heterogeneous networks
  - Network and system management
  - Windows 2000 server
- **Data transmission systems:**
  - Exchange of data media
  - Modem
  - Firewall
  - E-mail
  - Web servers
  - Remote access
  - Lotus Notes
  - Internet information server
  - Apache web server
  - Exchange/Outlook 2000

- **Telecommunication:**
  - Telecommunications systems (private branch exchange)
  - Fax machines
  - Answering machines
  - LAN connection of an IT system via the Integrated Services Digital Network (ISDN)
  - Fax servers
  - Mobile telephones
- **Other IT components:**
  - Standard software
  - Databases
  - Telecommuting
  - Novell eDirectory 8.6
  - Archiving

There are a list of threats and a comprehensive catalogue of safeguards covering measures, responsibilities and controls. However, there is no mapping of threats and measures available centrally—these mappings are merely defined via modules that have threat levels and appropriate measures assigned.

The catalogue of threats has a very broad scope and is divided into several categories. The number of threats explained and listed in each category is listed in parentheses.

- *Force majeure* (15)
- Organisational shortcomings (101)
- Human error (76)
- Technical failure (52, including two deleted threats)
- Deliberate acts (126)

The very detailed catalogue of 857 safeguards is structured as follows:

- Infrastructure (60)
- Organisation (306)
- Personnel (43)
- Hardware and software (232)
- Communication (121)
- Contingency planning (95)

The IT BPM does not mention which safeguard should be implemented to abandon a given threat—there is only a mapping via the modules, which is not precise either. The GSTOOL (an application for modelling and management of IT security concepts) of the publishing German Federal Office based on these modules also lacks a direct combination of threats and safeguards.

REFERENCES

Internet	
BSI	*www.bsi.de*
IT BPM	*www.bsi.bund.de/gshb*

15. NIST 800-14

DOCUMENT TAXONOMY

The publication *Generally Accepted Principles and Practices for Securing Information Technology Systems* is a collection of principles and practices to establish and maintain system security. It is labelled as a special publication.

ISSUER

The Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST), a department of the US Department of Commerce, published the document. It is part of NIST's 800 series (computer security).

GOAL OF THE PUBLICATION

The publisher intends to provide a baseline for establishing or reviewing IT security programmes. It should help in gaining an understanding of basic security requirements of IT systems. It focuses not only on security practices, but also the intrinsic expectations of security provisions from a high viewpoint through its principles.

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE

NIST 800-14 is usually implemented subject to one or more of the following business cases:

- The need to comply with the principles and criteria for US government organisations
- The need to implement a sound security baseline

RELATED RISKS OF NON-COMPLIANCE

Risks of not implementing NIST 800-14 include insecure systems due to insufficient security management and awareness.

TARGET AUDIENCE

The guideline targets management, internal auditors, users, system developers and security practitioners. Thus, it explicitly addresses all parties responsible for IT security. Following the document, the security principle and practices are to be applied for governmental IT systems, particularly for systems of e-governance.

TIMELINESS

The paper was published in 1996, and no subsequent revision of the document is available. However, the documents that NIST 800-14 was based on have been updated recently.

CERTIFICATION OPPORTUNITIES

A certificate is not available.

CIRCULATION

The publication is from a US government department; thus, it is relevant for US government organisations. International usage of the document is not comparable with the other documents discussed in this research.

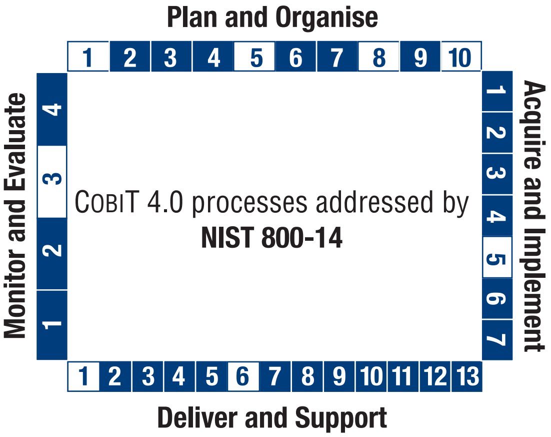
COMPLETENESS

The paper focuses on information security and provides thorough information on why security is important and how an adequate level of security can be achieved. Due to the focus on security, the information provided by this document does not address the complete scope of IT management issues and is classified as narrow. The paper is high-level; it is not as deep as other guidance discussed within this research.

AVAILABILITY

The guidance is posted for complimentary download from the CSRC web site. Printed versions are not available from the publisher.

COBIT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria	
-	Effectiveness
-	Efficiency
+	Confidentiality
+	Integrity
+	Availability
-	Compliance
-	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

IT RESOURCES ADDRESSED

IT Resources	
o	Applications
o	Information
+	Infrastructure
+	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

The principles of NIST 800-14 are listed below, and they are based on those published by the Organisation for Economic Co-operation and Development (OECD). NIST 800-14's principles imply the premise of being generally accepted and applied when developing or maintaining IT systems. The principles provided by the OECD guideline are accountability, awareness, ethics, multidisciplinary, proportionality, timeliness, reassessment and democracy. The principles of NIST 800-14 are:

- **Computer security supports the mission of the organisation.** Even though the protection of assets (information, hardware and software) is essential to achieve the goals of the organisation, security frequently is seen as inconsistent with the business objectives. Thus, management needs to understand the mission of the organisation and how this mission is supported by IT systems.
- **Computer security is an integral element of sound management.** Management must accept the fact that harm to assets can be caused, even though security provisions are in place. Management has to commit to the level of risk it is willing to accept.
- **Computer security should be cost-effective.** The cost for securing systems has to be aligned with the security need. This requires that the cost and benefits of security be examined in monetary and non-monetary terms. Direct and indirect costs should be considered when analysing the costs.
- **System owners have security responsibilities outside their own organisations.** System owners have to inform external users of the security measures of the systems, and they are responsible for incident response in a timely and co-ordinated manner.
- **Computer security requires a comprehensive and integrated approach.** Computer security and areas outside computer security should be considered. The interdependence of security controls and other controls must be understood, and a mix of managerial, operational and technical controls must be applied to enable an adequate and stable level of security.
- **Computer security should be periodically reassessed.** The need for re-evaluation of security measures is obvious in the wake of permanent changes to organisations, business environments, legal issues, threats or technologies.
- **Computer security is constrained by societal factors.** Security measures may come into conflict with other limitations, such as workplace privacy. Those conflicts must be solved.

Additionally, the guidance provides information on the common practices in IT security. There is no distinction amongst technical, operational and management controls—all practices are provided in the same structure. Explanatory subsections with practices and additional information are provided if needed.

Most of the practices provided in the guideline are quite common and the style is similar to the international standard ISO/IEC 17799. In fact, this was used as a reference during the development of the practices in NIST 800-14.

The document discusses security from a life cycle point of view. As this is unique to the documents discussed in this paper, the following enumeration summarises the relevant issues:

- **Initiation**—When defining the scope of the system, the sensitivity of information processed by the system and the system itself is analysed.
- **Acquisition**—During the acquisition (or development) phase, requirements for system security are defined. The requirements are worked into specifications; thereafter, security activities are considered when building the system.
- **Implementation**—During the installation/activation of the system, security features are to be used where appropriate. Testing the security of the system consists of testing particular parts and the whole system. After positive tests, a formal accreditation expresses the acceptance of the system as well as the remaining risk.
- **Operation/maintenance**—Security measures such as operations (backup, administration of user accounts, managing software updates, etc.) and audits are to be performed throughout the productive phase of the system.
- **Disposal**—At the end of the life cycle of a system, the information has to be moved to other systems (e.g., to comply with legal requirement for record retention) and the media have to be disposed of in a secure manner.

FURTHER REFERENCES

Internet	
NIST	*www.nist.gov*
CSRC	*http://csrc.nist.gov*

16. CONCLUSION

The purpose of this paper is to compare various worldwide guidance publications focused on specific issues of IT governance. Only COBIT addresses the full spectrum of IT governance duties; however, several standards publications describe the duties in a more comprehensive manner than COBIT. Thus, when implementing sound IT governance, those standards publications have to be considered, and the guidelines, models and processes should be used to facilitate it, but the framework to integrate the standards should be COBIT. Please note that all documents discussed in this paper and the information therein are subject to change, and implementation of those standards requires thorough planning and knowledge of the guidance.

In summary, three figures provide a high-level view of how the guidance documents discussed in this paper link to COBIT and relate to each other:

- **Figure 9** shows the horizonal and vertical classification of completeness of the guidance documents. Vertical refers to how detailed the guidance is in terms of technical or operational profundity. Horizontal refers to the completeness of the guidance: How much of COBIT is addressed within it? What is more comprehensively addressed in another standard than in COBIT? What is missing compared to COBIT?
- **Figure 10** displays a high-level mapping of the guidance documents covered in this publication to the COBIT domains.
- **Figure 11** shows a high-level mapping of the guidance to the COBIT processes.

Figure 9—Classification of Guidance

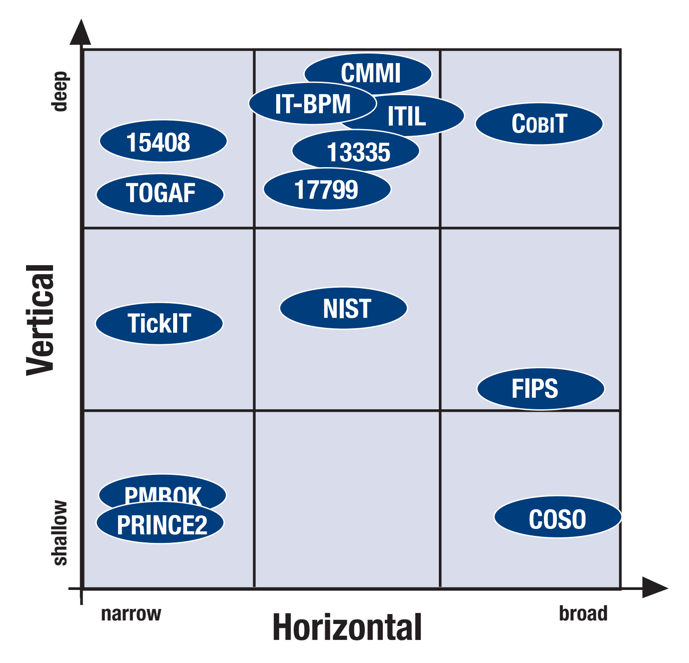


Figure 10—High-level Mapping of Guidance to COBIT Domains

	PO	AI	DS	ME
COSO	+	+	0	0
ITIL	0	0	+	-
ISO/IEC 17799	0	+	+	0
FIPS PUB 200	0	+	+	0
ISO/IEC 13335	0	0	0	-
ISO/IEC 15408	-	0	-	-
PRINCE2	0	-	-	-
PMBOK	0	-	-	-
TickIT	-	+	-	0
CMMI	-	+	-	0
TOGAF 8.1	0	-	-	-
IT BPM	0	-	0	-
NIST 800-14	0	+	+	0

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

Figure 11—High-level Mapping of Guidance to CobiT Processes

CobiT Process	COSO	ITIL	ISO/IEC 17799	FIPS PUB 200	ISO/IEC TR 13335	ISO/IEC 15408	PRINCE2	PMBOK	TickIT	CMMI	TOGAF 8.1	IT BPM	NIST 800-14
PO 1	+	-	-	-	-	-	-	-	-	-	-	-	-
PO 2	+	-	+	+	+	-	-	-	-	-	+	-	+
PO 3	+	+	+	+	+	-	-	-	-	-	+	+	+
PO 4	+	+	+	+	+	-	-	-	-	-	+	-	+
PO 5	+	+	-	-	-	-	+	+	-	-	-	-	-
PO 6	+	-	+	+	+	-	-	-	-	-	-	+	+
PO 7	+	-	+	+	-	-	-	-	-	-	-	-	+
PO 8	-	-	-	-	-	+	+	+	+	+	-	-	-
PO 9	+	-	+	+	+	-	+	+	-	+	-	-	+
PO 10	-	-	-	-	-	-	+	+	-	+	-	-	-
AI 1	+	-	-	-	+	-	-	-	+	-	+	-	+
AI 2	+	-	+	+	-	+	-	-	+	+	-	-	+
AI 3	+	-	+	+	-	+	-	-	+	-	-	+	+
AI 4	+	+	+	+	-	+	-	-	+	-	-	-	+
AI 5	-	-	-	-	-	-	-	+	+	-	-	-	-
AI 6	+	+	+	+	+	-	-	-	+	+	-	-	+
AI 7	+	+	+	+	+	-	-	-	+	+	-	-	+
DS 1	+	+	-	-	-	-	-	-	-	-	+	-	-
DS 2	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 3	+	+	+	+	-	-	-	-	-	-	-	-	+
DS 4	+	+	+	+	+	-	-	-	-	-	-	+	+
DS 5	+	+	+	+	+	+	-	-	-	-	-	+	+
DS 6	-	+	-	-	-	-	-	-	-	-	-	-	-
DS 7	+	-	+	+	+	-	-	-	-	+	-	-	+
DS 8	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 9	+	+	+	+	-	-	+	-	-	+	-	-	+
DS 10	-	+	-	+	-	-	-	-	-	+	-	-	+
DS 11	+	+	+	+	+	+	-	-	-	+	-	+	+
DS 12	+	-	+	+	+	+	-	-	-	-	-	+	+
DS 13	-	-	+	-	-	-	-	-	-	-	-	-	+
ME 1	-	-	+	-	-	-	-	-	+	+	-	-	+
ME 2	-	-	+	+	+	+	-	-	+	-	-	+	+
ME 3	+	-	-	-	-	-	-	-	-	-	-	-	-
ME 4	+	-	+	+	-	-	-	-	-	-	-	-	+

(+) Frequently addressed
(-) Not or rarely addressed

17. References

British Department of Trade and Industry (DTI), *TickIT: Guide to Software Quality Management System Construction and Certification*, UK, 1994

British Office of Government Commerce (OCG), [formerly the Central Computer and Telecommunications Agency (CCTA)], IT Infrastructure Library (ITIL), UK, 1989

British Office of Government Commerce, *Managing Successful Projects with PRINCE2*, UK, 2002, 2005

British Standards Institution, *TickIT Guide Issue 5 Using IS0 9001:2000 for Software Quality Management Systems—Construction, Certification and Continued Improvement*, UK, 2001

Committee of Sponsoring Organisations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, USA, 1992

Computer Security Division of the National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems* (FIPS PUB 200), Department of Commerce, USA, March 2006, *http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-March.pdf*

Computer Security Resource Center of the National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12, Department of Commerce, USA, 1995

Computer Security Resource Center of the National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, Special Publication 800-14, Department of Commerce, USA, 1996

Common Criteria Project Sponsoring Organisation, *Common Criteria for Information Technology Security Evaluation 2.0*, 1999

Federal Office for Information Security (BSI), *IT Baseline Protection Manual (IT BPM)*, Germany

International Organisation for Standardisation, *Code of Practice for Information Security Management*, ISO/IEC 17799, Switzerland, 2005

International Organisation for Standardisation, *Information Technology—Guidelines for the Management of IT Security*, ISO/IEC TR 13335, Switzerland, 1998, 2000, 2001, 2004

International Organisation for Standardisation, *Quality Management and Quality Assurance Standards—Part 3: Guidelines for the Application of ISO 9001:1994 to the Development*, *Supply, Installation and Maintenance of Computer Software,* ISO 9000-3, Switzerland, 1991

International Organisation for Standardisation, *Quality Management Systems*, ISO 9001, Switzerland, 2000

International Organisation for Standardisation, *Security Techniques—Evaluation Criteria for IT Security*, ISO/IEC 15408, Switzerland, 2005

IT Governance Institute, COBIT 3rd Edition *Framework*, USA, 2000

IT Governance Institute, COBIT 3rd Edition *Management Guidelines*, USA, 2000

IT Governance Institute, COBIT 4.0, USA, 2005

Paulk, M.C., *et al; Capability Maturity Models for Software*, CMU/SEI-93-TR-24, Carnegie Mellon University, Software Engineering Institute, USA, 1993

Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK), 3rd Edition*, 2004

Software Engineering Institute of Carnegie Mellon University, *Capability Maturity Model Integration* (CMMI), USA, 2002

The Open Group, *The Open Group Architecture Framework* (TOGAF) 8.1, 2003

OTHER PUBLICATIONS

All publications come with detailed assessment questionnaires and work programmes. For further information, please visit *www.isaca.org/bookstore* or e-mail *bookstore@isaca.org*.

Enterprise Value: Governance of IT Investments

Enterprise Value: Governance of IT Investments is a series of three books, the first publications of the Val IT™ body of work, a governance framework that includes generally accepted guiding principles and supporting processes related to the evaluation and selection of IT-enabled business investments, and benefit realisation and value delivery from those investments. The Val IT framework is based on the COBIT framework. To obtain a return on investment, the Val IT principles are applied to management processes, including value governance, portfolio management and investment management. The Val IT framework will be supported by publications and operational tools and provides guidance to:

- Define the relationship amongst IT and the business and those functions in the organisation with governance responsibilities
- Manage an organisation's portfolio of IT-enabled business investments
- Maximise the quality of business cases for IT-enabled business investments, with particular emphasis on the definition of key financial indicators, the quantification of 'soft' benefits and the comprehensive appraisal of the downside risk

Val IT addresses assumptions, costs, risks and outcomes related to a balanced portfolio of IT-enabled business investments.

The initial series contains:

- *Enterprise Value: Governance of IT Investments, The Val IT Framework*
- *Enterprise Value: Governance of IT Investments, The Business Case*
- *Enterprise Value: Governance of IT Investments, The ING Case Study*

2006

Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition

The second edition streamlines the information and provides a one-page laminate card summary. With increased networking and a growing realisation of how valuable information assets are, information security is recognised as one of the most important issues to address for all IT users. However, the subject of IT security is often presented in high-tech terms, and managers find it difficult to understand the issues and feel confident about how their organisations are managing security-related risks. *Information Security Governance, 2nd Edition,* helps overcome these barriers by explaining information security in business terms and comes complete with tools and techniques to help managers uncover security-related problems. **2006**

A second publication, *Information Security Governance: Implementation Guide*, will provide a useful tool for practitioners, and will be available in late 2006.

COBIT 4.0

Control Objectives for Information and related Technology (COBIT) is an IT governance framework and supporting toolset that allows managers to bridge the gap amongst control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organisations. COBIT 4.0 emphasises regulatory compliance, helps organisations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework. It does not invalidate work done based on earlier versions of COBIT but instead can be used to enhance work already done based upon those earlier versions. When major activities are planned for IT governance initiatives or when an overhaul of the enterprise control framework is anticipated, it is recommended to start fresh with COBIT 4.0. COBIT 4.0 presents activities in a more streamlined and practical manner so continuous improvement in IT governance is easier than ever to achieve. **2005**

COBIT Online

COBIT Online provides easy and rapid access to all COBIT resources, such as browsing and searching the best practices, downloading customised guidance, benchmarking, and more. Designed as a web-based service and available to anyone with an Internet connection, COBIT Online makes COBIT more accessible and user-friendly than any other IT best practices. Furthermore, by using MyCOBIT, users can construct and download their own version of COBIT for use on the desktop in MS Word or Access formats as assessment forms, rich text Word documents or as a database. A variety of subscription levels are available, each providing different levels of access and functionality. **2005**

Aligning CobiT, ITIL and ISO 17799 for Business Benefit
This management briefing is the result of a joint study, initiated by the IT Governance Institute and the British Office of Government Commerce, in response to the growing significance of best practices to the IT industry and the need for senior business and IT managers to better understand the value of IT best practices and how to implement them.

The briefing suggests how implementation should be tailored, prioritised and planned to achieve effective use. To achieve alignment of best practice to business requirements, it is recommended that CobiT be used at the highest level, providing an overall control framework based on an IT process model that should generically suit every organisation. Specific practices and standards, such as ITIL and ISO 17799, cover discrete areas and can be mapped up to the CobiT framework, thus providing a hierarchy of guidance materials. **2005**

IT Governance Domain Practices and Competencies Series:
The series includes the following five publications:
- *Information Risks: Whose Business Are They?,* **2005**
- *Optimising Value Creation From IT Investments,* **2005**
- *Measuring and Demonstrating the Value of IT,* **2005**
- *Governance of Outsourcing,* **2005**
- *IT Alignment: Who Is in Charge?,* **2005**

Security Awareness: Best Practices to Serve Your Enterprise
This document provides the critical steps needed to implement an enterprisewide security awareness effort, build concurrence amongst departments, and provide baselines, maturity levels and control objectives. The guidance provided includes:
- A discussion of security awareness foundations and an outline of steps to design a security awareness programme
- A maturity model for best practice, security awareness self-assessment programme and case study

2005

Information Security Harmonisation—Classification of Global Guidance
The role of the information security manager has evolved from being IT-focused to that of a strategic business/IT hybrid. At the same time, numerous security standards, codes of practices, methodologies, etc., have been developed and published, all with the purpose of providing some level of direction or support for security objectives. This technical study provides the Certified Information Security Manager® (CISM®) with a guide to the better-known and more widely available information security documents. In all, 17 standards/guidance were evaluated across a number of criteria, enabling information security managers to identify those that may be most appropriate for improving their skills and knowledge or be of use within their organisation. The study includes insights learned from a global survey of CISMs. **2005**

CobiT *Mapping: Mapping ISO/IEC 17799:2000 With CobiT,* 2004
CobiT® *Security Baseline*, 2004
Control Practices*, 2004*
***IT Control Objectives for Sarbanes-Oxley*, 2004**
***IT Governance Implementation Guide*, 2003**
CobiT® *Quickstart*, 2003

IT
GOVERNANCE
INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

3701 ALGONQUIN ROAD, SUITE 1010
ROLLING MEADOWS, IL 60008 USA
PHONE: +1.847.590.7491
FAX: +1.847.253.1443
E-MAIL: *info@itgi.org*
WEB SITE: *www.itgi.org*

COBIT®
GOVERNANCE, CONTROL *and*
ASSURANCE *for* INFORMATION
and RELATED TECHNOLOGY