COBIT® MAPPING

Overview of International IT Guidance

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*

IT Governance Institute®

The IT Governance Institute (ITGI) strives to assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals. Its goals are to raise awareness and understanding among and provide guidance and tools to boards of directors, executive management and chief information officers (CIOs) such that they are able to ensure within their enterprises that IT meets and exceeds expectations, and its risks are mitigated.

Information Systems Audit and Control Association®

The Information Systems Audit and Control Association (ISACA®) is an international professional, technical and educational organization dedicated to being a recognized global leader in IT governance, security, control and assurance. With members in more than 100 countries, ISACA is uniquely positioned to fulfill the role of a central, harmonizing source of IT control practice standards the world over. Its strategic alliances with other organizations in the financial, accounting, auditing and IT professions ensure an unparalleled level of integration and commitment by business process owners.

Disclaimer

The IT Governance Institute, the Information Systems Audit and Control Association and the author of *COBIT Mapping* have designed the publication primarily as an educational resource for control professionals. The IT Governance Institute and the Information Systems Audit and Control Association make no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of any proper procedures and tests or exclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, controls professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or IT environment.

Disclosure

ISBN 1-893209-57-1
Printed in the United States of America

Acknowledgements

IT Governance Institute wishes to recognize:
The ISACA Austrian Chapter and Jimmy Heschl, CISA, CISM, for performing the research needed for this publication

The Board of Trustees, for its support
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young, LLP, USA, International President
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President
Ricardo J. Bria, CISA, Argentina, Vice President
Everett C. Johnson, CPA, Deloitte & Touche LLP, USA, Vice President
Dean R.E. Kingsley, CISA, CISM, CA, Deloitte Touche Tohmatsu, Australia, Vice President
Eddy Schuermans, CISA, PricewaterhouseCoopers LLP, Belgium, Vice President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Paul A. Williams, FCA, MBCS, Paul Williams Consulting, United Kingdom, Past International President
Emil G. D'Angelo, CISA, Bank of Tokyo-Mitsubishi, USA, Trustee
Ronald Saull, CSP, The Great-West Life Assurance Company, Canada, Trustee
Erik Guldentops, CISA, CISM, Belgium, Advisor IT Governance Institute

The ISACA Research Board, for managing the project
Chairperson, Lily M. Shue, CISA, CCP, CITC, LMS Associates, USA
Jayant Ahuja, CISA, CPA, CMA, PricewaterhouseCoopers LLP, USA
Candi Carrera, CF 6 Luxembourg, Luxembourg
John Ho Chi, CISA, CFE, Ernst & Young LLP, Singapore
Avinash W. Kadam, CISA, CISSP, CBCP, GSEC, CQA, MIEL E-Security Pvt. Ltd., India
Elsa K. Lee, CISA, MA, CSQA, Crowe Chisek LLP, USA
Robert G. Parker, CISA, CA, FCA, CMC, Deloitte & Touche LLP, Canada
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG, Austria
Johann Tello Mery k, CISA, CISM, Banco del Istmo, Panama
Frank van der Zwaag, CISA, CISSP, Air New Zealand, New Zealand
Paul A. Zonneveld CISA, CISSP, CA, Deloitte & Touche LLP, Canada

Expert Reviewers
Jayant Ahuja, CISA, CPA, CMA, PricewaterhouseCoopers LLP, USA
Sally Chan, MA, CMA, PAdm, ACIS, RBC Financial Group, Canada
Erik Guldentops, CISA, CISM, Belgium
Gary Hardy, ITWinners Ltd., United Kingdom
Avinash W. Kadam, CISA, CISSP, CBCP, GSEC, CQA, MIEL E-Security Pvt. Ltd., India
Kamal Khan, CISA, CISSP, Rabobank International, United Kingdom
Rodney Ian Marriner, CISA, IBM Global Services, New Zealand
Ernst J. Oud, CISA, Deloitte & Touche LLP, The Netherlands
Lily M. Shue, CISA, CCP, CITC, LMS Associates, USA

Table of Contents

1. Purpose and Scheme for Classification of the Guidance

Today several standards and collections of best practices are available, which prescribe how to best manage the information technology (IT) function of various organizations. In addition to the international standardization organizations, several private or partly private organizations have published suggested guidance. However, to date, no common framework is available for comparing them. With the availability of this research and such a framework, detailed comparisons and proper management of the IT function can be enhanced and consequently better decisions can be made.

In 1998, the IT Governance Institute was founded and began an initiative around the subject area of IT governance, which is focused on the COBIT framework, its processes, control objectives and maturity models. (Note: COBIT was initially created by the Information Systems Audit and Control Foundation® in 1996, and the IT Governance Institute updated in 2000 for the release of the 3rd Edition.) By using this framework, CIOs can provide their stakeholders the capacity to better understand IT processes and services. Too, stakeholders are provided with an instrument for governance of the information delivered by IT to the business processes.

With those points previously mentioned in mind, there is a need for information on implementing guidance supporting governance of IT, asking 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?

This is the first deliverable of the *COBIT Mapping* research project, which focuses on the business drivers for implementing the guidance, as well as the risks of noncompliance with the guidance. Furthermore, it contains a classification of the guidance publications, a short overview of their content, and how they align or map to COBIT.

Although most of these questions can be addressed using the openly available COBIT guidance, several have remained unresolved, until now. As a result, this project was initiated to map the most important and commonly used standards and guidance to the COBIT processes and control objectives. The term "standard" is used in this document to encompass guidance publications.

This document does not contain the result of detailed mappings; it merely gives an overview of the most popular guidance for managing IT, or at least parts of the tasks and duties of IT.

In 2004, the IT Governance Institute will publish the results of the second phase of the project, a detailed mapping of common guidance with the COBIT framework, beginning with ISO/IEC 17799:2000.

This research is limited to the publications in the following list, which is not exhaustive, as there are other documents and information sources available. The following is a brief overview of the guidance discussed in this research:
- **COBIT**—*Control Objectives for Information and related Technology* was 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. Beginning with the addition of *Management Guidelines* in 1998, COBIT is now being used more and more as a framework for IT governance, providing management tools such as metrics and maturity models to

complement the control framework.

- **ITIL**—The IT Infrastructure Library is a collection of best practices in IT service management. It is focused on the service processes of the IT and considers the central role of the user.
- **ISO/IEC 17799:2000**—The *Code of Practice for Information Security Management* is an international standard, based on BS 7799-1. It is presented as best practice for implementing information security management.
- **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**—*Security Techniques—Evaluation Criteria for IT Security* is used as a reference to evaluate and certify the security of IT products and services.
- **TickIT**—TickIT 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.
- **NIST 800-14**—The special publication *Generally Accepted Principles and Practices for Securing Information Technology Systems* contains information for establishing a comprehensive IT security program.
- **COSO**—*Integrated Framework* defines a framework that initiates an integrated process of internal control.

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
Is it an international or a national standard, a collection of best practices, etc.?

Issuer
This refers to the issuing body of the paper. Which organization is standing behind the definition and keeping the document up-to-date?

Goal(s) of the Standard or Guidance Publication
What are 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
What is the business case for implementing the guidance? What are the typical situations that indicate implementing the guidance?

Related Risks of Noncompliance
What are the business risks of not implementing the guidance?

Target Audience
Is there a special target audience and who is it? For example, are public organizations, assurance professionals, security management or general IT professionals the target audience?

Timeliness
Is the guidance up-to-date? How frequently is it revised and issued?

Certification Opportunities
Is there a certification path? What can be certified? Who may act as certification body?

Circulation
Is the guidance used internationally or is it limited to a certain region? Is information on the usage available?

Completeness
The completeness is classified using two dimensions:
- **Vertical—**How detailed are the guidelines in terms of technical or operational profundity?
- **Horizontal—**How complete is the guidance? How much of COBIT is addressed with the guidance? What is more comprehensively addressed than in COBIT? What is missing compared to COBIT?

Availability
How and where can the information be obtained?

COBIT Processes Addressed
Refers to a high-level mapping of which processes, as defined in COBIT, are addressed by the respective guidance. The COBIT processes are described in the section on COBIT in this publication.

Information Criteria Addressed
This section addresses which of the following COBIT information criteria are referenced. They are:
- Efficiency
- Effectiveness
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

IT Resources Concerned
This section focuses on the COBIT IT resources, and which are addressed by the respective guidance:
- People
- Applications
- Technology
- Facilities
- Data

Description of the Guidance and its Content
What fundamental concepts are covered by the guidance?

2. COBIT

The first guidance publication explained is COBIT. COBIT is an abbreviation of *Control Objectives for Information and related Technology*.

Document Taxonomy
COBIT represents a collection of documents which 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 currently available was issued by the IT Governance Institute in 2000, and added the *Management Guidelines*, as well as several other detailed control objectives.

Goal(s) of the Standard or Guidance 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."

Business Drivers for Implementing the Guidance, Including Typical Situations
COBIT is usually implemented subject to 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 standardized/automated.
- A framework for overall IT processes is needed.
- Processes are to be unified.
- There is a need of 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 (e.g., regulators, organizations or third-party) requirements is of concern.

Related Risks of Noncompliance
- 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 management's expectations
- Know-how tied to key individuals, not to the organization
- Excessive IT cost and overheads
- Erroneous investment decisions and projections

Target Audience
Various organizations, public and private companies and external assurance professionals form the relevant target group. Within organizations, three levels are addressed: management, IT users and professionals and assurance professionals.

Timeliness
Although the latest version was issued in 2000, it is still up-to-date. The latest enhancements to COBIT at the time of this publication in 2003-04 include:

- *COBIT Quickstart*
- *COBIT Online*
- *IT Governance Implementation Guide*
- *IT Control Practices*

Certification Opportunities
COBIT's audit guidelines contain information for auditing and self-assessment against the control-objectives, however there is no certificate available for any part of COBIT. Furthermore, the COBIT framework is used frequently by certified public accountants (CPAs) and chartered accountants (CAs), for instance, when performing an SAS 70 review.

Non-COBIT certification is available through ISACA, the originator of COBIT, 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 version of the publications, it has been translated into Spanish, German, French, as well as several other languages.

Completeness
As mentioned, COBIT addresses a broad spectrum of duties in IT management. COBIT includes all 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 Online can be purchased by going to, *www.isaca.org/cobitonline*. COBIT Online allows users to customize a version of COBIT just right for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys and benchmarking. Most parts of COBIT are open and readily accessible for complimentary electronic download on the ITGI or ISACA web sites, *www.itgi.org* or *www.isaca.org*. The audit guidelines are posted for complimentary download for ISACA members. Alternatively, a printed set and fully searchable CD-ROM can be purchased from the ISACA bookstore, *bookstore@isaca.org*.

COBIT Processes Addressed*

COBIT Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	+	+	+	+	+	+	+	+	+	+	+	\	\
AI	+	+	+	+	+	+	\	\	\	\	\	\	\
DS	+	+	+	+	+	+	+	+	+	+	+	+	+
M	+	+	+	+	\	\	\	\	\	\	\	\	\

(+) Addressed
(-) Not or rarely 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	
+	People
+	Applications
+	Technology
+	Facilities
+	Data

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

*Note: these three charts are not a comparison, this is COBIT itself.

Description of the Guidance and its Content

Enterprise governance (the system by which organizations are governed and controlled) and IT governance (the system by which the organization'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 organization, 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 subject matter 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 the IT Governance Institute:

> "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 organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."

COBIT Framework

Organizations must satisfy the quality, fiduciary and security requirements for their information, as they do for all assets. Management also must optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to

achieve their objectives, management must understand the status of their own IT systems and decide what security and control they should provide.

The COBIT framework helps to meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's good practices reflect consensus of the experts, help optimise information investments, and provide a measure to be judged against if 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: planning and organization, acquisition and implementation, delivery and support, and monitoring. 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.

Management Guidelines

The COBIT management guidelines provide a link between IT control and IT governance. They are action-oriented and generic, and provide management specific guidance and direction for getting the enterprise's information and related processes under control, monitoring achievement of organizational goals, monitoring and improving performance within each IT process and benchmarking organizational 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 key performance indicators?
- What are the critical success factors?
- What are the risks of not achieving our objectives?
- What do others do?
- How do we measure and compare the organization's maturity to the current status of (best-in-class in) the industry and the current status of international standards?
- What is the organization's strategy for improvement?

Control Practices

IT 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 IT 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

Analyze, assess, interpret, react and implement. To achieve the desired goals and objectives, the enterprise must constantly and consistently audit its procedures. *Audit Guidelines* outlines and suggests actual activities to be performed, corresponding to each of the 34 high-level IT control objectives, while substantiating the risk of control objectives not being met.

COBIT Quickstart

This special version is a baseline for many small to medium 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 towards 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 has been developed and exceptions are reviewed. Those enterprises for whom the strategic nature of IT is relatively low, who fall

within certain ranges on the self-assessment and who do not have any of the exceptions that might indicate a higher level of dependence on IT are considered SMEs.

This project is being 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 being included, so that implementation of COBIT's fundamental principles can take place easily, effectively and relatively quickly.

COBIT Online

An online version of COBIT allows users to customize a version of COBIT just right for 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 is planned for the second release in 2004.

IT Governance Implementation Guide

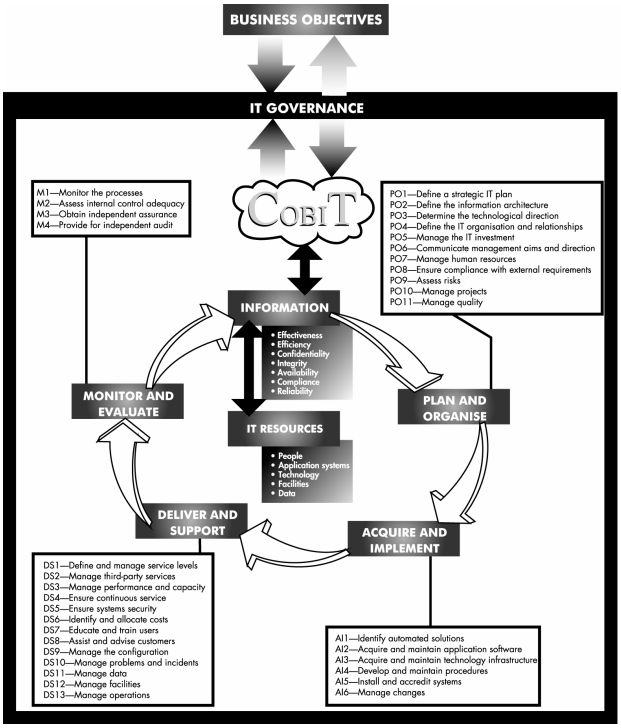
The objective of the *IT Governance Implementation Guide* is to provide readers with a methodology for implementing and improving IT governance, using COBIT. The guide is focused on a generic methodology for implementing IT governance, covering the following subjects:

- Why IT governance is important and why organizations 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

The COBIT IT Process

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

Figure 1—COBIT IT Processes Defined Within the Four Domains

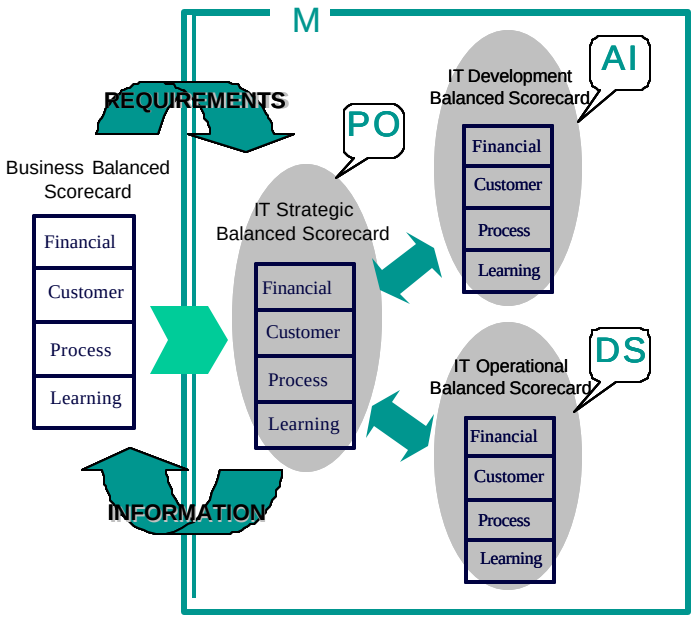


Any service delivered by IT, as well as all services as a whole provided to the core processes, have to be planned and integrated into existing plans, as indicated in **figure 1**. Alternatively, existing plans and organizational structures could be adopted, depending on the significance of each service. Services subsequently are 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. Thus, another chart, **figure 2** illustrates the superordinate role of monitoring, which could be seen as a concept for a balanced scorecard.

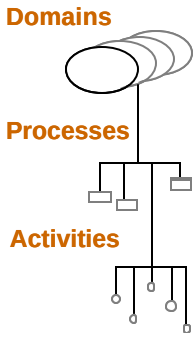
The main domains are:
- **PO**¾ Plan and Organize
- **AI**¾ Acquire and Implement
- **DS**¾ Deliver and Support
- **M**¾ Monitor and Evaluate

Figure 2—Balanced Scorecard



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

Figure 3—Top-down Approach



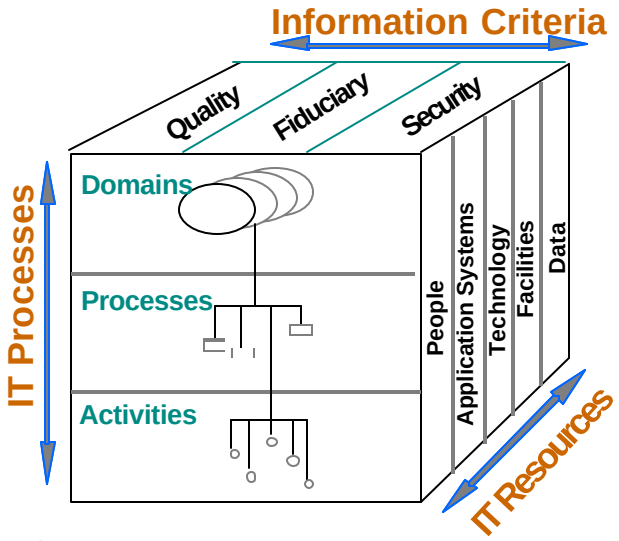
Each process is described by using the following information:
- High-level control objectives
- Detailed control objectives
- Information criteria affected by the process
- IT resources used by the process
- Typical characteristics depending on the maturity level
- Critical success factors
- Key performance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

Information Criteria
Information delivered to the core business processes has to fulfil certain criteria, which are summarily characterized 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 unauthorized 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
  - **Reliability**—Relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities

IT Resources
Following the COBIT definition, the resources used by the IT are identified as follows:
- **Data**—Objects in their widest sense (i.e., external and internal), structured and nonstructured, graphics, sound, etc.
- **Application systems**—Understood to be the sum of manual and programmed procedures
- **Technology**—Covers hardware, operating systems, database management systems, networking, multimedia, etc.
- **Facilities**—All the resources to house and support information systems
- **People**—Includes staff skills, awareness and productivity to plan, organize, acquire, deliver, support, monitor and evaluate information systems and services

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 on deviations compared 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 CSFs that usually apply to all processes as they deal with what is the standard, who sets it, and who controls or needs to act.

Further References

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

3. ITIL

Document Taxonomy
The IT Infrastructure Library (ITIL) is a series of seven books which is referred to as the only consistent and comprehensive best practice for IT service management. Although published by a governmental body, ITIL is not a standard.

Issuer
The first versions of the ITIL collection were published by the British Office of Government Commerce (OCG), which still holds the ITIL trademark. The OCG was commissioned to develop a methodology for efficient and effective use of IT resources within the British government.

Goal(s) of the Standard or Guidance 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
- Defining of service processes within the IT organization
- Definition and improvement of the quality of services
- Need to focus on the customer of the IT
- Implementation of a central help desk function

Related Risks of Noncompliance
- Error-prone support processes due to lack of attention

Target Audience
ITIL focuses on organizations 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; however, not all updated books announced are available yet. The *Business Perspective* volume is still being developed.

Certification Opportunities
Certification of personnel is available already, but at present organizations cannot be certified. British Standard 15000 (BS15000) presents a specification for IT management for which ITIL can be used as guidance documents. BS15000 was developed with ITIL in mind and it is foreseeable that it will be possible that certification bodies will be accredited to certify against this British Standard.

There are three levels of certifications:
- 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 ten-day training program 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 scale of IT management and IT governance as COBIT does. Processes of the DS domain are covered in a comprehensive manner; however, processes, tasks and duties of the domains PO, AI and M are hardly treated.

Availability
ITIL is available in paperback and a CD-ROM version. The printed version of *Security Management* is not available in electronic format.

COBIT Processes Addressed

COBIT Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	-	+	+	+	-	-	-	-	+	-		
AI	+	+	+	+	+	+							
DS	+	+	+	+	+	+	-	+	+	+	+	+	+
M	-	-	-	-									

(+) Addressed
(-) Not or rarely 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
+	People
+	Applications
+	Technology
+	Facilities
+	Data

(+) 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 process 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 management are described within the two ITIL documents *Service Support* and *Service Delivery*. The description of the processes is not standardised and thus not consistent. Not all processes contain metrics or key performance indicators, a description of the roles and activities or guidelines for implementing the process.

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

The key practices of *Service Delivery* are as follows:
- 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.

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.

ITIL Security Management explains the necessary measures of security, focused on IT infrastructure.

At the time of this research, ITIL had not yet released a document entitled *Business Perspective*, aimed at helping business managers understand IT service delivery. It will cover 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 list.

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 and more user-oriented and user-friendly. Incident management's center of attention is the restoration of the agreed service level in a speedy and uniform manner.
- **Goal**—Swift restoration of normal service operation (normal, as defined within 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.
  - Localize potential causes of the incident.
  - Recover the services and manage closure.
  - Take ownership over the incident.
  - Monitor, track and communicate the execution.

Problem Management

- **Description**—A structured and systematic approach in problem management can minimize outages, even before an incident occurs. Potential sources of error are to be identified and corrected in a timely manner. Hence, sound problem management is focused on preventive measures and the identification 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 of the resources.
- **Goal**—There is no single goal of the configuration management process, rather 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).
  - Identify and label configuration items (CI) with their owner, available documentation, versions and interrelationships.
  - Document CIs in a central configuration management database (CMDB).
  - Establish procedures and documentation standards to ensure that only authorized 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 treats planning and supervising of changes to the existing infrastructure thus minimizes the risk of damage to existing and new application systems, infrastructure and services.
- **Goal**—Changes are implemented within the agreed time and minimal risk.
- **Major Tasks**
  - Record, log and filter requests for changes (RfC).
  - Priorities and categories the RfC.
  - Assess the impact of the RfC on the infrastructure and other services as well 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.

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 as well as 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 a sound service level management, clear interfaces and specification of services are defined with customers (senior management). Users and internal as well as external suppliers are defined 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 (SLR).
  - 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 catalog.

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 organization.
- **Major Tasks**
  - Budgeting
    - Define cost centers.
    - 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 a proper management of resources. A 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 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 minimizing negative effects caused by disastrous and unpredictable events, disruption of the core business processes is to be minimized.
- **Goal**—The goal is to provide a predetermined and agreed 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 minimizes 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	
ITIL Online	*www.itil.co.uk*
itSMF	*www.itsmf.com*

4. ISO/IEC 17799:2000

Document Taxonomy
ISO/IEC 17799:2000 is an international standard.

Issuer
The international standard was published by ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission), which have established a joint technical committee, ISO/IEC JTC 1, addressing the components of BS7799-1 only. Essential parts of the international standards labeled as *Information Technology—Code of Practice For Information Security Management* were developed and published by the British Standards Institution, 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

Goal(s) of the Standard or Guidance Publication
ISO/IEC 17799:2000 provides information to parties responsible for implementing information security within an organization. It can be seen as a basis for developing security standards and management practices within an organization to improve reliability on information security in interorganizational relationships.

Business Drivers for Implementing the Guidance
- Definition of an information security management system, applying best practice in security management based on a systematic approach
- Identification of critical assets via the business risk assessment
- Enhancement of the knowledge and importance of security-related issues at the management level
- Definition of responsibility and organizational structures for information security
- Need for a basis for certification of the information security management system
- Need for contractual relationships

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

Target Audience
The document targets people responsible for information security within various organizations willing to initiate, implement or maintain information security.

Timeliness
The standard was published in 2000 in its first edition, which still is valid, and it is updated at infrequent intervals. Since this is an official ISO standard it will automatically be revised and updated when required every three to five years. It can be classified as current best practice in the subject area of information security management systems. The originating BS 7799 was revised and reissued in September 2002.

Certification Opportunities
A certification of ISO/IEC 17799:2000 is not available. However, a certificate on compliance with the British Standard 7799 Part 2 can be obtained, as BS7799 Part 2 contains binding specifications for a certification of an information security management system, as well as normative controls.

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.

Being focused on security issues, it does not cover the full scope of IT management duties, while the level of detail is comparable to COBIT. Phase two of this research will provide a detailed mapping of ISO 17799 to COBIT.

Availability
The standard can be purchased from ISO.

COBIT Processes Addressed

COBIT Processes and Domains	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	+	+	+	-	+	+	+	+	-	-		
AI	-	+	+	+	+	+							
DS	-	+	+	+	+	-	+	+	+	+	+	+	+
M	+	+	-	-									

(+) Addressed
(-) Not or rarely 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
+	People
+	Applications
+	Technology
+	Facilities
o	Data

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

Description of the Guidance and Its Content

The guiding principles are the initial point when implementing information security. They rely on either legal requirements or generally accepted best practices.

Measures based on legal requirements are (among others):

- Protection and nondisclosure of personal data
- Protection of internal information
- Protection of intellectual property rights

Best practices mentioned are:

- Information security policy
- Assignment of responsibility for information security
- Problem escalation
- Business continuity management

When implementing a system for information security management several critical success factors should be considered:

- The security policy, its objectives and its activities reflect the business objectives.
- The implementation considers cultural aspects of the organization.
- Open support and engagement of senior management are required.
- Thorough knowledge of security requirements, risk assessment and risk management is required.
- Effective marketing of security targets all personnel, including members of the management.
- The security policy and security measures are communicated to contracted third parties.
- Users are trained in an adequate manner.
- A comprehensive and balanced system for performance measurement is available, which supports continuous improvement by giving feedback.

After presenting introductory information (scope, terms and definitions), guidance is presented for initiating, implementing and maintaining information security. This guidance is structured into 10 sections, which contain 36 objectives and 127 controls.

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

- **Security policy**
  - An information security policy should define the direction and contain the commitment and the support of the management.
  - The policy should be communicated throughout the organization.
- **Organizational security**
  - The definition of adequate organization structures for the management of information security within the organization should include:
    - An information security management forum
    - A forum for co-ordination
    - Assignment of responsibility for information security to individuals
    - Definition of responsibility areas for managers
    - Definition of an authorization process for IT facilities
    - Definition of responsibility for investigation of security-relevant know-how
    - Defined range for co-operation with third parties as well as independent security reviews
  - Comprehensive measures should exist for management of third-party services (definition or risks and security requirements).
  - Risks caused by outsourcing contracts should be managed.

- **Asset classification and control**
  - The inventory of assets and the assignment of the responsibility should be seen as a prerequisite to sound accountability for assets.
  - Information should be classified following a generally accepted system, thus ensuring an appropriate level of protection.
- **Personnel security**
  - Security responsibilities, confidentiality agreements and the contract of employment should be part of the job responsibility.
  - Adequate controls for personnel screening should be in place.
  - Information security education and training should increase users' security awareness.
  - The process of reporting security incidents, weaknesses and software malfunctions should be defined. This should include the assessment of the adequacy of the controls implemented by a permanent process of learning from incidents.
- **Physical and environmental security**
  - Central equipment should be installed only within a secure area, where adequate access controls and damage prevention are implemented. These areas include offices, rooms and facilities. There is also a need for a special attention to delivery and loading areas.
  - 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 disposal or reuse of information should be considered.
  - General controls (such as a clear desk and clear screen policy) to protect information processing facilities or to prevent damage caused by unauthorized offsite usage of equipment should be in place.
- **Communications and operations management**
  - Operations should follow documented procedures.
  - All changes to equipment should be documented.
  - Procedures for sound incident management should be defined.
  - Duties should be segregated, ensuring no individual can both initiate and authorize an event.
  - Development and operational facilities are to be separated.
  - Risks caused by contracted external facilities organizations should be covered.
  - Capacity demands should be observed and future demands should be projected.
  - Acceptance criteria for new systems should be defined.
  - Damage caused by malicious software should be prevented, using preventive and detective controls, formal policies and defined recovery procedures.
  - Information should be backed up and the backup files tested regularly.
  - Activities performed by operational staff and errors should be logged.
  - Networks should be set up and managed with a view to ensuring the necessary level of security.
  - 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, electronic commerce transactions, electronic mail, electronic office systems, publicly available systems and other forms of information interchange.
- **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.
  - Responsibilities of users should be clearly defined.
  - Networked services, operating systems and applications should be protected appropriately.
  - System access and use should be monitored constantly.
  - Mobile computing and teleworking should be performed in a secure manner.
- **Systems development and maintenance**
  - Security issues should be considered when implementing systems following defined requirements.
  - Security in application systems should take into account the validation of input data, adequate controls of internal processing, message authentication and output data validation.
  - Use of cryptographic systems should follow a defined policy.
  - Access to system files (including test data and source libraries) should be controlled.
  - Project and support environments should allow for security by being rigorously controlled (e.g., change management procedures, arrangements for outsourced development).
- **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 which 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**
  - Any unlawful act (e.g., data protection acts) should be avoided.
  - Compliance with the security policy should be ensured by periodical reviews.

Further References

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

5. ISO/IEC TR 13335

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

Issuer
The report was published by ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission), which have established a joint technical committee, the ISO/IEC JTC 1, Subcommittee SC 27 (IT security techniques), which is tasked to publish international standards (e.g., ISO/IEC 17799:2000).

Goal(s) of the Standard or Guidance Publication
The report provides guidance on aspects of IT security management, and is divided into five parts:
1. The management tasks of IT security are outlined, providing an introduction to security concepts and models.
2. & 3. Discuss implementation and management of IT security in a comprehensive manner.
4. Provides guidance on the selection of safeguards considering the type of IT systems as well as security concerns and threats.
5. Contains information on identifying and analysing communication-related factors that should be taken into account when introducing network security.

Business Drivers for Implementing the Guidance
- Guidance for security management
- The need for a structured approach

Related Risks of Noncompliance
- There is no direct risk from not complying unless the organization has an inherent need to comply with this standard.

Target Audience
The report is applicable to all kinds of organizations. Part one explicitly addresses senior management and information security managers, whereas the other parts target individuals responsible for the implementation of security measures, for instance, IT managers and IT security staff.

Timeliness
Dates of publication range from 1996 (part one) to 2001 (part five). No part has a defined update frequency, as they were published as technical reports. Parts 1, 2 and 3 are currently under revision (parts 1 and 2 will be combined into a new part 1); the revision of Part 4 is planned.

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 come close to addressing the complete scope of IT management duties.

Availability
The documents can be acquired from ISO.

COBIT Processes Addressed

COBIT Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	+	+	+	-	+	-	-	+	-	-		
AI	+	-	-	-	-	+							
DS	-	-	-	+	+	-	+	-	-	-	+	+	-
M	-	+	+	-									

(+) Addressed
(-) Not or rarely 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	
+	People
+	Applications
+	Technology
+	Facilities
+	Data

(+) 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 One—Concepts and Models for IT Security
The first part discusses basic management concepts and models of IT security. It could be used as an introduction to the management of IT security, as it does not provide detailed information on IT security.

A systematic approach considers the definition of a policy, the identification of roles and responsibilities, a systematic risk management, configuration and change management, contingency/disaster recovery planning, selecting and implementing safeguards and follow-up activities.

Corporate objectives, strategies and policies influence the organization's general security objectives, strategies and policies, which in themselves form the basis for the narrower set of IT security objectives, strategies and policies. IT system security objectives, strategies and policies are derived from the more general level of overall IT security.

The major elements involved in the security management process are as follows:
- Assets (physical assets, information, software, people and intangibles)
- Threats (human and environmental)
- Vulnerabilities
- Impact
- Risk
- Safeguards
- Residual risk
- Constraints

The ongoing process of IT security management consists of the subprocesses:
- **Configuration management**—Changes in the configuration may not lead to a reduction of the security level. Furthermore, tracking of changes is available, and changes to the systems are reflected in various documentation (e.g., disaster recovery plan).
- **Change management**—This is the process of identifying security requirements when systems change.
- **Risk management**—Risk management is to be performed throughout the system's life cycle. A risk management process compares risks with benefits and costs of different types of safeguards.
- **Risk analysis**—Risks are identified by the analysis of asset values, threats and vulnerabilities, resulting in a statement of the likelihood of risks to previously mentioned assets.
- **Accountability**—Responsibility for security is to be assigned explicitly. Ownership is assigned to assets.
- **Security awareness**—This explains the security objectives, strategies and policies and the need to comply with them.
- **Monitoring**—A periodic review of the safeguards is needed to assure their effectiveness.
- **Contingency plans and disaster recovery**— Contingency plans describe how to maintain core business processes in the case of system outages. Disaster recovery contains information on restoration of systems affected by an unintended outage.

Part Two—Managing and Planning IT Security

Part two contains guidelines that address essential topics on the management of IT security. They are useful for identifying and managing IT security.

Establishing and maintaining an IT security program 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 organization.

A sound corporate IT security policy should address the following questions:
- **Objectives**—What is to be achieved, how are these objectives achieved, and what are the rules for achieving these objectives?
- **Management commitment**—What is the commitment and support of senior management?
- **Policy relationships**—What are the relationships among 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?

Organizational 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 organization and to all systems.

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

- **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 organizations.
- **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 analyzed 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 into "acceptable" and "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 the safeguards as defined in the plan, including security training
- **Security awareness**—To pass the knowledge from the security officer to all levels of the organization
- **Follow-up**—Activities such as maintenance of safeguards and policies, security compliance checking, monitoring and incident handling

Part Three¾Techniques for the Management of IT Security

Management techniques are described and recommended in part three 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 of compliance, monitoring, change management practices and incident handling

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

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

- **Needs analysis**—Existing and targeted level of awareness within different target groups and identification of necessary methods

- **Program 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 three concludes with a discussion of follow-up activities such as maintenance, compliance checking, change management, monitoring and incident handling. In the annex, after the aforementioned table of contents of a security policy, a comprehensive list of possible threat types and vulnerabilities and a description of a risk analysis method are provided.

Part Four—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 three. Baseline protection can come in two flavours: selection of safeguards according to the type of IT system and safeguards according to security concern and threats.

The basic assessments of the safeguard selection process are:

- **Identification of the type of system**—IT systems can be a standalone workstation, a workstation connected to a network or a server/workstation sharing resources via a network.
- **Identification of physical/environmental conditions**—In addition to general considerations concerning the environment of the organization, 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, 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 the building. It has to be borne in mind that existing safeguards may exceed the current needs.

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

- **Organizational 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 organizational 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
  - Unauthorized access to computers, data, services and applications
  - Unauthorized access to storage media
- **Integrity**
  - Deterioration of storage media
  - Maintenance error
  - Malicious code
  - Masquerading of user identity
  - Misrouting/rerouting of messages
  - Nonrepudiation
  - Software failure
  - Supply failure (power, air conditioning)
  - Technical failure
  - Transmission errors
  - Unauthorized access to computers, data, services and applications
  - Use of unauthorized programs and data
  - Unauthorized 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
  - Unauthorized access to computers, data, services and application
  - Use of unauthorized programs and data

  - Unauthorized access to storage media
  - User error
- **Accountability, authenticity and reliability**
  - No specific threats are listed in the report, only such exemplary threats as account sharing; lack of traceability; masquerading user identity; software failure; unauthorized access to computers, data and applications; or a weak authentication of identity.

Examples of countermeasures to the previously mentioned threats are provided in the report. During the selection of a specific safeguard, it has to be decided which basic aspect should 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 organizationwide baseline, it must be decided whether the organization 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 Five—Management Guidance on Network Security

Part five deals with network security and provides guidance for 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 communications-related factors:

- **Review corporate IT security requirements**—The IT security policy states the requirements for confidentiality, integrity, availability, nonrepudiation, accountability, authenticity and reliability of information.
- **Review network architectures and applications**—Depending on the types of networks, the protocols used, the 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 organizational levels:
  - A single controlled location within an organization
  - Connection among different geographical parts but within an organization
  - Connection between an organization site and personnel working in locations away from the organization
  - Connection among different organizations with a closed community
  - Connections with other organizations
  - 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 network. The trust relationship is—depending on its environment—classified into low, medium and high. The combination of the two classes of publicity 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, characteristic safeguards are nominated.

- **Identify appropriate potential safeguard areas**—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
  - Nonrepudiation
  - 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 organization and define specific tasks for selection, implementation and maintenance of the safeguard.

Further References

Internet	
ISO	*www.iso.org*

6. ISO/IEC 15408:1999/Common Criteria/ITSEC

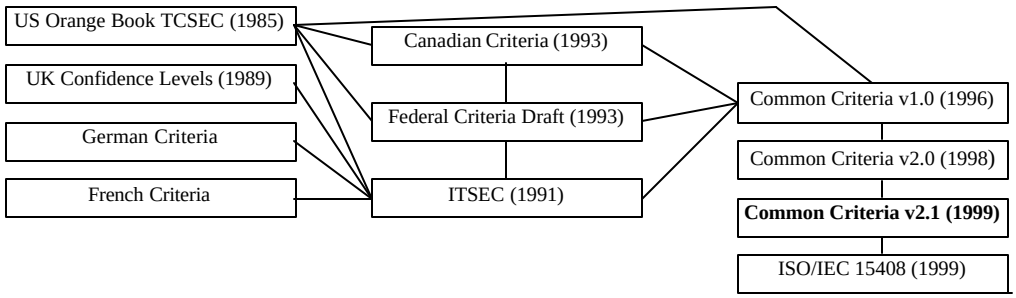
The international standard ISO/IEC 15408:1999 *Security Techniques—Evaluation Criteria for IT Security* is based on the *Common Criteria (CC) for Information Technology Security Evaluation 2.0*, thus they are treated in one chapter. *Common Criteria* succeeds *Information Technology Security Evaluation Criteria (ITSEC)*, published by the European Commission in 1991. The naming of those documents is synonymous.

Document Taxonomy
ISO/IEC 15408:1999 is an international standard. *Common Criteria* is labelled as a multipart standard.

Issuer
ISO/IEC 15408:1999 was published by the ISO/IEC JTC 1 working group in collaboration with the Common Criteria Project Sponsoring Organization, which published *Common Criteria*. Members of this organization are:
- **Canada**—Communications Security Establishment
- **France**—Service Central de la Sécurité des Systèmes d'Information
- **Germany**—Bundesamt für Sicherheit in der Informationstechnik
- **Netherlands**—Netherlands National Communications Security Agency
- **United Kingdom**—Communications-Electronics Security Group
- **United States**—National Institute of Standards and Technology and National Security Agency

From a historical 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 5¾ Standards Influences



Goal(s) of the Standard or Guidance Publication
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
- Implementation of products or services that shall be certified
- Security imperative to the development of semifinished products (e.g., control systems)

Related Risks of Noncompliance
- There is no direct risk for not complying unless the organization 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. The CC can be useful as a source of security functions that may be implemented into a system.
- **Evaluators**—Evaluators have clear and agreed 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.
- **Others**—CC may be seen as a useful source of information by others, such as security and assurance professionals

Timeliness
Although published in 1999, *Common Criteria* is still up-to-date. The criteria mentioned are very stable. The currently valid version 2.1 of *Common Criteria* differs only in formatting and minor changes to comply with the ISO standard.

Certification Opportunities
The purpose of the document is to provide common criteria for the certification of IT products and services.

Circulation
By being published as an international standard, *Common Criteria* 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. *Common Criteria* is freely available for public use.

COBIT Processes Addressed

COBIT Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	-	-	-	-	-	-	-	-	-	+		
AI	-	+	+	+	+	-							
DS	-	-	-	-	+	-	-	-	-	-	+	+	-
M	-	+	+	-									

(+) Addressed
(-) Not or rarely 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	
+	People
+	Applications
+	Technology
o	Facilities
+	Data

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

Part One ¾ Introduction and General Model

Part one explains the general model, the general concepts and the 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 Two ¾ Security Functional Requirements

Part two 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 catalog 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 Utilization
- FTA—TOE access
- FTP—Trusted path/channels

Part Three ¾ Security Assurance Requirements

A set of assurance components is included in part three, enabling a standardised approach of defining

assurance requirements for IT products and services. The structure of the catalog is similar to the one in part two 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 three. The evaluation of PP and 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 *Common Criteria* are as follows:
- EAL1—Functionally tested
- EAL2—Structurally tested
- EAL3—Methodically tested and checked
- EAL4—Methodically designed, tested and reviewed
- EAL5—Semiformally designed and tested
- EAL6—Semiformally 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*

7. TickIT

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

Issuer
TickIT is published and maintained by TickIT Office, which is a business unit within the British Standards Institute (BSI).

Goal(s) of the Standard or Guidance 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

A further objective was the development of a framework for the management of software development that enables efficient certification of quality management systems. To reach those objectives, the following steps were taken:
- Creation of a guide that facilitates interpretation of the ISO 9001 requirements
- Improvement of knowledge of auditors 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
- 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 organization on the quality of the software delivered

Related Risks of Noncompliance
- The complex area of software development is controlled inadequately or the control is performed in an ineffective manner.
- Specification of requirements is incomplete.

Target Audience
TickIT is for organizations whose software development adds significant value to the organization'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. The latest revision considers the modifications of the framework of ISO 9000.

Certification Opportunities
A certification of an organization's quality management system is available, indicating the adoption of the TickIT scheme for quality management. Moreover, TickIT is used to accredit certification bodies.

Circulation
TickIT is of British origin, but it is used in several European countries. Information provided on the TickIT web site reports that 1,157 TickIT active certificates have been issued as at July 2003.

Completeness
TickIT has a clear focus on software development and related quality management systems, thus it is classified as narrow and not addressing 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 also is available

COBIT Processes Addressed

COBIT Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	-	-	-	-	-	-	-	-	-	+		
AI	+	+	+	+	+	+							
DS	-	-	-	-	-	-	-	-	-	-	-	-	-
M	+	+	+	-									

(+) Addressed
(-) Not or rarely 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 information criteria addressed and IT resources are also concerned with software development and the related quality management system.

IT Resources Addressed

	IT Resources
+	People
+	Applications
+	Technology
+	Facilities
+	Data

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

Description of the Guidance and Its Content

TickIT can be used to support development of all types of software, such as 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 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 organizations providing software services as well as in-house developers. Assessing and improving the effectiveness of the organization's quality management system is also part of this chapter.
- **Guidance for auditors**—Part D contains guidance to 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 organizations 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 organizations 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*

8. 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(s) of the Standard or Guidance Publication
The publisher intends to provide a baseline for establishing or reviewing IT security programs. It should help in gaining an understanding of basic security requirements of IT systems. It not only focuses on security practices, it also describes the intrinsic expectations of security provisions from a high viewpoint in the form of the principles.

Business Drivers for Implementing the Guidance
- The need to comply with the principles and criteria for US government organizations
- Arguably the need to implement a sound security baseline

Related Risks of Noncompliance
- 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 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 organizations. 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 the questions: Why is security important? How can an adequate level of security 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 electronically from the CSRC web site. Printed versions are not available from the publisher.

COBIT Processes Addressed

COBIT Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	-	+	+	+	-	+	+	+	+	-	-		
AI	+	+	+	+	+	+							
DS	-	+	+	+	+	-	+	+	+	+	+	+	+
M	+	+	-	-									

(+) Addressed
(-) Not or rarely 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	
+	People
o	Applications
o	Technology
+	Facilities
o	Data

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

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

- **Computer security supports the mission of the organization**—Even though the protection of assets (information, hardware and software) is essential to achieve the goals of the organization, security frequently is seen as inconsistent with the business objectives. Thus management needs to understand the mission of the organization 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 nonmonetary terms. Direct and indirect costs should be considered when analyzing the costs.
- **System owners have security responsibilities outside their own organizations**—System owners have to inform external users of the security measures of the systems and they are responsible for incidence 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 reevaluation of security measures is obvious in the wake of permanent changes to organizations, 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 among 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 analyzed.
- **Acquisition**—During the acquisition (or development) phase, requirements for the 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 systems, 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 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	*csrc.nist.gov*

9. COSO

Document Taxonomy
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 Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is a voluntary private sector organization. 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. Sponsoring organizations are: American Accounting Association, American Institute of Certified Public Accountants, Financial Executives Institute, Institute of Internal Auditors and Institute of Management Accountants.

Goal(s) of the Standard or Guidance 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 to manage risks. It is the most comprehensive study on internal control.

Business Drivers for Implementing the Guidance
- 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

Related Risks of Noncompliance
- Nonsystematic approach for controls
- Incomplete controls
- Weak control environment
- Inefficient controls
- Inadequate processes due to a lack of controls

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

Timeliness
COSO published *Internal Control—Integrated Framework* in 1992. At the time of this publication, a new version was out for exposure.

Certification Opportunities
There is no opportunity for a certification.

Circulation
The report is referenced to 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 online from AICPA, *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 with other guidance with this document.

COBIT Processes and Domains	1	2	3	4	5	6	7	8	9	10	11	12	13
PO	+	+	+	+	+	+	+	+	+	-	-		
AI	+	+	+	+	+	+							
DS	+	-	+	+	+	-	+	-	+	-	+	+	-
M	-	-	-	-									

(+) Addressed
(-) Not or rarely 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	
+	People
+	Applications
+	Technology
+	Facilities
+	Data

(+) 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. *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 organization.
- *Reporting to External Parties* provides guidance to establish reports in a properly controlled manner. It is addressed to organizations 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.

The definition of internal control reads 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 there are five components that form internal control. The way they interrelate and interact and how they influence the objectives of the organization is the system of internal control. The system of internal control is individual to an organization; in other words, no two entities have the same system of internal controls. It depends on the size of the organization, the industry and also on 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 organization to set objectives. Risks are to be identified, analyzed and managed in an appropriate manner.
- Control activities—Policies and procedures are to be established for a sound management of risk and to achieve the objectives defined by the organization. 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 organization can be divided into three categories:
- Operations
- Financial reporting
- Compliance

The effectiveness of the internal control system depends on:
- Management knowledge on the level of the achievement of the organization's objectives
- The reliability of financial statements published by the organization
- Compliance with applicable laws and regulations

Further References

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

10. Conclusion

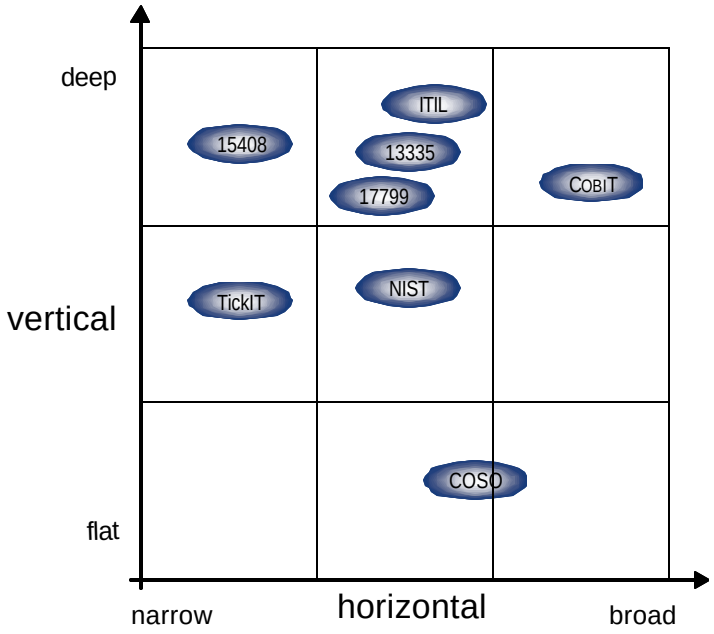
The various worldwide guidance publications reviewed in this research document does focus on specific issues of IT governance. However, only COBIT addresses the full spectrum of IT governance duties. However, several standards publications describe the duties in a more comprehensive manner than COBIT. Thus, when implementing sound IT governance, those standards publications have to be considered and the guidelines, models and processes should be used to facilitate the implementation of COBIT.

The completeness is classified using two dimensions:

- **Vertical—**How detailed are the guidelines in terms of technical or operational profundity?
- **Horizontal—**How complete is the guidance? How much of COBIT is addressed with the guidance? What is more comprehensively addressed than in COBIT? What is missing compared to COBIT?

The horizontal and vertical classification of different guidance is depicted in **figure 6**.

Figure 6¾ Classification of Guidance



A high-level mapping of the guidance to the COBIT domains is provided in **figure 7**.

Figure 7—High-level Mapping of Guidance to COBIT Domains

	PO	AI	DS	M
ITIL	o	+	+	-
ISO/IEC 17799	o	+	+	o
ISO/IEC 13335	o	-	o	o
ISO/IEC 15408	-	o	-	o
TickIT	-	+	-	+
NIST	o	+	+	o
COSO	+	+	o	-

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

11. References

COBIT 3rd Edition: *Framework*, IT Governance Institute, Rolling Meadows, IL, USA, 2000
COBIT 3rd Edition: *Management Guidelines*, IT Governance Institute, Rolling Meadows, IL, USA, 2000
Common Criteria and Methodology for Information Technology Security Evaluation, CSE (Canada), SCSSI (France), BSII (Germany), NLNCSA (Netherlands), CESG (United Kingdom), NIST (USA) and NSA (USA), 1999
Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, USA, *www.coso.org*
ISO TR 13334, International Organization for Standardization (ISO), *Information Technology—Guidelines for the Management of IT Security*, Switzerland, 1996 - 2001
ISO IEC 15408, International Organization for Standardization (ISO), *Evaluation Criteria for Information Technology Security*, Switzerland, 1999
ISO IEC 17799, International Organization for Standardization (ISO), *Code of Practice for Information Security Management*, Switzerland, 2000
ISO 9000-3, International Organization for Standardization, *Quality Management and Quality Assurance Standards—Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software*, Switzerland, 1991
ISO 9001, International Organization for Standardization (ISO), *Quality Management Standard*, Switzerland, 2000
National Institute of Standards and Technology (NIST), *An Introduction to Computer Security: The NIST Handbook*, *Special Publication 800-12*, USA, 1996
IT Infrastructure Library (ITIL), British Office of Government Commerce (OCG), Central Computer and Telecommunications Agency (CCTA), London, 1989
Paulk, M.C., et al: Capability Maturity Model℠ for Software, CMU/SEI-93-TR-24, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, USA, 1993
TickIT: *Guide to Software Quality Management System Construction and Certification*, British Department of Trade and Industry (DTI), London, 1994

Other IT Governance Institute Publications

To order these and other ITGI publications, or for further information, please visit *www.isaca.org/bookstore* or e-mail *bookstore@isaca.org*.

COBIT Quickstart
This special version is a baseline for many small to medium 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 towards 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 has been developed and exceptions are reviewed. Those enterprises for whom the strategic nature of IT is relatively low, who fall within certain ranges on the self-assessment and who do not have any of the exceptions that might indicate a higher level of dependence on IT are considered SMEs.

This project is being 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 being included, so that implementation of COBIT's fundamental principles can take place easily, effectively and relatively quickly.

COBIT Online
An online version of COBIT allows users to customize a version of COBIT just right for 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 is planned for the second release in early 2004. See *www.isaca.org/cobitonline*

IT Governance Implementation Guide
The *IT Governance Implementation Guide* provides 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 organizations should implement it
- The IT governance life cycle
- The COBIT framework
- How COBIT is linked to governance and how COBIT enables the implementation of IT governance
- The stakeholders who have an interest in IT governance
- Using COBIT as a road map for implementing IT governance

IT Control Objectives for Sarbanes-Oxley
A step-by-step, road map approach explains the current focus on enhancing corporate accountability, the audit committees responsibility, the need to adopt and use an internal control framework (COSO), the need to consider fraud in an audit or review of internal control, the necessary but unique challenge of focusing on IT controls and using a compatible IT governance framework (COBIT), and how to seize the opportunity of turning compliance into a competitive challenge. The document provides IT professionals and organizations with assessment ideas and approaches, IT control objectives mapped into COSO for disclosure and financial reporting purposes, and a clear road map to deal with the murkiness of these regulatory times.

IT Strategy Committee
This document describes the purpose, mission, reasons and possible structure for an IT strategy committee of the board of directors. Also compares and contrasts the IT strategy committee to IT steering committees. Complimentary download is provided at *www.itgi.org.*

IT Governance Executive Summary
Couched in high-level, nontechnical, business-oriented language, this document discusses why IT governance is important to the enterprise, reasons for focusing on IT governance, and what boards and management should do to address IT governance in their enterprises. Complimentary download is provided at *www.itgi.org.*

Board Briefing on IT Governance
This booklet describes IT governance, outlines why it is important, defines the role of boards and executive management in it and offers tool kits and maturity models for implementing and measuring IT governance enterprise-wide. Complimentary download is provided at *wwwitgi.org.*

Information Security Governance: Guidance for Boards of Directors and Executive Management
This book discusses why information security governance is increasingly important and outlines questions to ask and steps to take to ensure an effective information security governance program within an enterprise. Complimentary download is provided at *www.itgi.org.*

COBIT Training Course
A new COBIT implementation course has been added to the Professional Seminar Series available through ISACA chapters. This course is intended for individuals responsible for, or involved in, IT governance, and it covers:
- The principles and objectives of COBIT
- The various components of COBIT
- How COBIT supports IT governance
- Planning IT management/governance initiatives with COBIT
- Assessing IT management capability using COBIT maturity models and control objectives
- Planning control improvements using COBIT control objectives and control practices
- Creating a performance measurement framework using COBIT metrics and scorecards
- Implementation factors, issues and support

COBIT 3rd Edition
COBIT incorporates generally applicable and accepted international standards for good practice of IT management and control. It applies to enterprisewide information systems, including personal computers, minicomputers, mainframes and client/server environments. COBIT is based on the philosophy that IT resources need to be managed by a set of naturally grouped processes in order to provide the information an organization needs to achieve its objectives. To ensure the delivery of pertinent and reliable data, COBIT provides a framework of IT control objectives that can be implemented and monitored within enterprises.

The third edition of COBIT enhances the existing framework by including management guidelines, which provide additional concepts and tools for managing IT processes. Key goal indicators, critical success factors, and key performance indicators are provided for all of COBIT's high-level control objectives. In addition, maturity models have been developed to support the planning and monitoring of the evolving IT capabilities. The third edition also expands concepts of IT governance and has been updated to reflect new and revised international references.

Control Objectives for Net Centric Technology (CONCT)
While advances in network computing technology have given users greater access to information resources, they have also created the need for global best practices in the cyberspace environment. This four-volume set contains a framework and volumes on intranet/extranet/Internet, online transaction processing and the data warehouse, each containing audit steps, control guidelines and suggestions. The publication offers global guidelines for the net centric technologies that reflect not only the management perspective of the issue, but the architectural, security and integrity perspectives as well. The ability to communicate immediately and concisely in a global environment using net centric technology, utilizing generally accepted and comprehensive control objectives, has become essential to enterprise governance.

Peer-to-peer Networking Security and Control
Peer-to-peer (P2P) is not a particular technology, industry, communications protocol or single network structure, but rather it is a mindset of decentralized and distributed uses of information resources. The purpose of this paper is to outline the reasons an enterprise might consider implementing P2P, describe the basics of P2P technology, and examine some of the potential issues and risks and how they might be addressed. The business drivers of decentralization, excess capacity and performance are examined. The technology and examples are explained and security and control issues explored. An appendix of some P2P vendors with a brief description of their products is included. This white paper is posted to the ISACA web site at *www.isaca.org/research.*

Security, Audit and Control Features SAP® R/3®: A Technical and Risk Management Reference Guide
Current best practices and future trends in ERP issues are documented in a practical how-to guide to enable auditors and risk professionals (both IT and non-IT) to evaluate risks and controls in existing ERP implementations and to facilitate the design and building of better practice controls into system upgrades and enhancements. The guide presents:
- ERP Audit impacts from implementation are detailed and frameworks and methodologies for auditing and testing in an SAP R/3 environment are provided. A technique to assist in identifying the cause of issues using the ISACA COBIT™ framework is also described.
- Auditing SAP R/3—Core Business Cycles: Revenue, Inventory and Expenditure and Basis Technical Infrastructure.

This is the first in a series of technical and risk management reference guides dealing with the world's three major ERP systems: SAP R/3, Oracle Applications and PeopleSoft.

Security, Audit and Control Features—Oracle® Applications A Technical and Risk Management Reference Guide
Current best practices and future trends in ERP issues are documented in a practical how-to guide to enable risk professionals and auditors (both IT and non-IT) to evaluate risks and controls in existing ERP implementations and to facilitate the design and building of better practice controls in system upgrades and enhancements. This is the second in a series of technical and risk management reference guides dealing with the world's three major ERP systems: SAP R/3 Audit, Oracle Financials and PeopleSoft. The guides concentrate on three very different software programs but do contain common chapters on ERP risk management and audit approach. This guide uses Release 11*i* and provides frameworks and methodologies for auditing and testing in an Oracle environment, including a recommended Oracle audit framework, how to adopt a risk-based audit approach to

ERP, an overview of the Oracle authorisation concept, how to test Oracle security, configurable controls and segregation of duties/excessive access. The need to identify the causes of issues arising from audit or control testing and a technique to assist in identifying the cause of issues using the COBIT framework also are described.

Risks of Customer Relationship Management (CRM)—A Security, Control and Audit Approach
The book emphasizes the strategic value and business impact of customer relationship management initiatives to enterprises, their processes, the technology involved and how they help achieve business objectives. The publication also outlines the impacts that risk management and assurance professionals can have by addressing the tactical issues during the transformation process. To view the detailed table of contents and foreword of this book, visit the ISACA Bookstore online at *www.isaca.org/bookstore.* A white paper on CRM can be found on the ISACA site as well.

Security Provisioning: Managing Access in Extended Enterprises
Preautomated business processes rely on informal circuit breakers to moderate the impact or pace of change across the enterprise. If change is not effectively addressed as processes move online or onto the Internet, their velocity and scope of effect can disrupt and overwhelm normal processing. This book provides senior corporate management and IT administrators with a clear vision of the advantages, criteria and implementation considerations of using policy-based provisioning to manage security access rights across the enterprise and beyond. It provides an overview of the virtualised and extended enterprise to illustrate how provisioning is central for ensuring the integrity of corporate policies, individual privacy and overall system security. The book also includes several self-evaluation questionnaires and checklists.

Virtual Private Network—New Issues for Network Security
VPNs have proven popular due to their operational efficiencies and savings while retaining the baseline security associated with a private network. They allow a trusted network to communicate with another trusted network, over untrusted/public networks like the Internet. Unlike other VPN books, this research was conducted and written solely from the perspective of the security, control and assurance professional. The deliverable focuses on functionality rather than just on technology. The control objectives section in the publication is aligned with the previously released research, *Control Objectives for Net Centric Technology* (CONCT), and adapted specifically to the VPN environment. The book also contains control guidelines, and a sample audit program for the pre-implementation through post-implementation of a VPN.

Digital Signatures—Security and Controls
In the electronic communications environment it is essential to be able to establish that the signatory of a message is indeed its originator. This detailed publication on the security and control issues of digital signatures addresses all of the vital components that are relevant to the IT audit and control community. Written by experts in cryptography, it explains what digital signatures are, how they work and unresolved issues in their use. It includes audit programs, questionnaires and suggestions for the assurance professional.

Electronic and Digital Signatures: A Global Status Report
The objective of this research is to provide CIOs, CEOs, CTOs and control professionals an overview of the UNCITRAL Model Law and the EU Directive, and to determine if various country legislation adequately addresses either electronic signatures or digital signatures as a baseline of their laws. Since it would be close to impossible to provide coverage for all countries, for the purpose of this project a sample of countries was selected to take part in the research and to answer a survey.

The focus of this survey includes:
- Providing a reference point on the status of electronic signatures legislation implementation in the selected countries and where one can obtain additional information regarding specific country legislation on electronic signatures
- Determining if the specific country legislation:
  - Defines the requirements for electronic signatures the same as the legal requirements for handwritten signatures
  - Recognises foreign certificates and electronic signatures, and determines if any geographic or procedural limitations exist to prevent cross-border recognition of electronic signatures
  - Defines or limits the liability of the sender, receiver or the certification service provider

IT Governance Institute E-commerce Security Series in Partnership with Deloitte & Touche

Securing the Network Perimeter
This document deals with security practices in the environment surrounding network applications of an e-commerce infrastructure. It details the security vulnerabilities, issues and controls involving network applications residing on commerce servers, web browsers, firewalls, proxies and other network devices. The auditor and security professional can expect to find security risks and best practices to access control, identification and authorization, auditing, content filtering and intrusion detection at the network application level.

Business Continuity Planning
This publication deals with security controls that help ensure that e-commerce applications are uninterrupted in the event of an incident, such as a natural disaster, or a breach of security, such as a break-in to the e-commerce server. It also provides procedures to respond to an incident in addition to normal activities involving the backup and retention of systems, applications and data. The assurance professional will be particularly interested in the discussion of the difference between e-commerce continuity compared to traditional business continuity plans, specifically in relation to the continued availability of e-commerce infrastructure (e.g., public key infrastructure, certificate authorities, Internet service providers). Included in the publication are FAQs, audit considerations, ICQs and audit programs.

Trading Partner Authentication, Registration and Enrollment
This publication documents the process of recognizing and establishing the authenticity of a new trading partner and deciding whether to do business. Its focus is the establishment of the relationship. That is, it focuses on "new account" time. The auditor will find it useful when deciding whether to audit an e-commerce application and when planning or conducting such an audit. He or she may also find it useful when examining or making judgments about any new account process, whether, or to what extent, such a process is automated. Included in the publication are FAQs, audit considerations, ICQs and audit programs.

Public Key Infrastructure
In addition to describing the technology and the related infrastructure issues, this guide highlights risks, management issues, controls and audit concerns. The research centers on the application or enterprise PKI and details the creation, distribution, validation and management of cryptographic keys. It also discusses the use of digital signatures, certificates and certificate authorities as part of the cryptographic infrastructure and it describes their characteristics in terms of security. Furthermore, the document examines the PKI marketplace and compares cryptographic technologies offered by major technology companies. Included in the publication are FAQs, audit considerations, ICQs and audit programs.

A Global Status Report
E-commerce is changing the way organizations conduct business with each other and their customers. As organizations facilitate the evolution of existing business processes, to take advantage of the benefits of the Internet, are they effectively managing their risks? In this initial phase of the research, over 150 business executives were interviewed, and a portion of the ISACA membership was surveyed.

Enterprise Best Practices
The second deliverable of the project is a framework for business managers to understand the principles of e-commerce security and how best to control and implement it within their organizations. The book offers valuable insights and best practices involving e-commerce issues such as protecting data, maintaining confidentiality, confirming identities, controlling system changes, detecting unauthorized intrusions and handling denial of service attacks.

Future IT Governance Institute Publications

Security, Audit and Control Features PeopleSoft® A Technical and Risk Management Reference Guide
This technical reference guide covers application security risk, audit and technical infrastructure considerations of PeopleSoft. The purpose of this research is to document current best practices in PeopleSoft risk and control issues and to provide a comprehensive reference guide for assurance and control professionals. It will include self-assessment questions and audit programs.

Identity Management
Identity management and user provisioning solutions of today can help improve cost efficiencies, enable effective processes and promote user satisfaction while providing a high degree of security. Tools and methodologies are available to centralize the management of users and their access to resources, delegating administration to different business units or groups, and bringing users, systems and applications online quickly. This has a direct impact on an organization's bottom line as a properly implemented identity management solution helps reduce the cost of managing user information, increase user and administrator productivity, and reduce the time-to-market for new initiatives. Deliverables of this project include a short focused paper outlining the business issues, technology drivers, risks involved, and necessary controls for the environment. The research will include a self-assessment questionnaire and assurance program for assistance to the control professional.

Biometrics
This project will address business drivers associated with biometrics, the current and future demand for biometric technology, the role and components of a biometric system and the processes involved in using a biometric system for security. Furthermore, the project will address risks associated with biometrics including a general discussion of reliability, probability and recovery approaches, risks associated with several specific types of biometric technology, security and audit considerations for protecting biometric systems. The research will include a self-assessment questionnaire and a PowerPoint presentation summarising the findings.

Wireless Communication
Because wireless communications transcend traditional and regulatory boundaries, they pose significant technical challenges, as well as greater challenges in the areas of control, security and audit. This project will provide a technical and functional assessment and will be written from a business and risk management perspective. A white paper on wireless security can be found on the ISACA web site.

Oracle Database Security, Audit and Control Features
Work has begun on an update to the very popular *Security and Controls in an Oracle Environment*, a part of the ISACA Monograph Series. The revised edition will include the issues that have changed in subsequent Oracle environments, from Oracle 6 through Oracle 9*i*, as well as a comprehensive focus on architecture, security, controls and risk, and operating systems approach of version 9*i*.

OS/390—z/OS Security, Audit and Control Features
This research will include updates to the recent revisions of the legacy functions of the operating system and outline the system components and their interaction. The project's focus will include: system initialisation; security functions; audit tools and methods; detailed descriptions of new components and functions in the above areas; recently added functions, mainly those that permit the use of the Internet; and UNIX functions in the OS/390 environment.

Information Integrity
In an increasingly dynamic global environment, IT organizations must address complex solutions and operating environments to provide assurance of the dependability and trustworthiness of information across the enterprise. The purpose of this project is to define the key elements of enterprise information integrity, address information as a resource as well as an object, to define the benefits criteria associated with them, and to present a framework and process for management. The Centre for IS Assurance is conducting this project for the IT Governance Institute.