SANDIA REPORT

SAND2005-3455
Unlimited Release
Printed June 2005

A COBIT® Primer

Philip L. Campbell

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2005-3455
Unlimited Release
Printed June 2005

A COBIT® Primer

Philip L. Campbell
Networked Systems Survivability and Assurance Department

Abstract

COBIT[1] is a set of documents that provides guidance for computer security.[2] This report[3] introduces COBIT by answering the following questions, after first defining acronyms and presenting definitions:

1. Why is COBIT valuable?
2. What is COBIT?, and
3. What documents are related to COBIT? (The answer to the last question constitutes the bulk of this report.)

This report also provides more detailed review of three documents. The first two documents—COBIT Security Baseline™ and COBIT *Quickstart*™—are initial documents, designed to get people started. The third document—Control Practices—is a "final" document, so to speak, designed to take people all the way down into the details. Control Practices *is* the detail!

---

1. "COBIT," "ISACA," "ISACF," and "IT Governance Institute" are registered trademarks, and "COBIT Online" and COBIT *Quickstart*" are trademarks, all of the Information Systems Audit and Control Association and the IT Governance Institute.

"COBIT" is pronounced "COH-bit," "ISACA" is pronounced "eye-SOCK-ah," and "ITGI" is pronounced, unaccented, "eye-tee-gee-eye." (I have never heard "ISACF" pronounced.)

ITGI has asked that I include the following copyright statements for this document:

> "This Primer includes COBIT®, 3rd Edition, which is used by permission of the IT Governance Institute (ITGI). ©1996, 1998, 2000 IT Governance Institute. All rights reserved."
>
> "This Primer includes COBIT Security Baseline, which is used by permission of the IT Governance Institute (ITGI). ©2004 IT Governance Institute. All rights reserved."
>
> "This Primer includes Control Practices, which is used by permission of the IT Governance Institute (ITGI). ©2004 IT Governance Institute. All rights reserved."
>
> "This Primer includes COBIT Quickstart, which is used by permission of the IT Governance Institute (ITGI). ©2003 IT Governance Institute. All rights reserved."

2. Actually, COBIT provides guidance for "IT governance," a superset of computer security, as I describe in Section 2.

3. For clarity I use the word "report" to refer to the pages you are now reading and the word "document" to refer to the items that are discussed in this report.

This is a blank page.

Table of Contents

List of Figures

List of Tables

Acknowledgement

Thank you to William F. Hossley, of Sandia's Internal Audit Department (Organization 12830) and President of the local ISACA Chapter, for review of and pointers concerning this report, and Timothy S. McDonald, of Sandia's Cryptography and Information Systems Surety (Organization 5614) for careful editing.

This is a blank page.

1 Acronyms & Definitions

In this section I first present several acronyms, shown in Table 1, followed by several definitions, shown in Table 2

The acronyms used in this report are presented in Table 1.

Table 1 Acronyms

Acronym	Meaning	Comments
COBIT	Control Objectives for Information and related Technology	COBIT is published and maintained by ITGI (see below). Versions 1, 2, and 3 of COBIT were published in 1996, 1998, and 2000 respectively. The current version is 3.2 and is published on-line as "COBIT Online™." COBIT is a registered trademark of ISACA (see below) and ITGI.
ISACA®	Information Systems Audit and Control Association	This a non-profit, professional organization that was formerly the EDP[a] Auditors Foundation, founded in 1969. It is the organization that has spawned ISACF and ITGI (see below). ISACA's world headquarters are in Illinois.
ISACF®	Information Systems Audit and Control Foundation	This is a non-profit organization that serves as the research arm of ISACA and that developed COBIT. In 2003 the name of this organization was changed to ITGI (see below).
IT	information technology	IT is hardware and software. IT automates an "information system" (IS) which is independent of IT. An IS could be implemented in any number of ways, one of which is electronics.[b]
IT Governance Institute® (ITGI)	Information Technology Governance Institute	This is the new name for ISACF (see above), as of 2003.

a. EDP = Electronic Data Processing.

b. To better understand the difference between IS and IT, see Chapter 5, "The Information System which Won the War," of Information, Systems, and Information Systems by Checkland & Holwell, 2002, John Wiley & Sons.

For more authoritative information about ISACA, I contacted ISACA. This was their reply:

> The Information Systems Audit and Control Association (ISACA) is a non-profit professional association. With more than 47,000 members in more than 140 countries, ISACA (www.isaca.org) is the global leader in information governance, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the Information Systems Control Journal®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 35,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 5,000 professionals in its first two years.

For more authoritative information about ITGI, I contacted ISACA. This was their reply:

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

The discrepancies between my dates and the dates immediately above are resolved, I believe, if we posit that ISACA is using the founding date of the organization, independent of name changes.

The definitions used in this report are shown in Table 2.

Table 2 Definitions

Definition	Meaning
Control	"The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected." (Executive Summary, page 10)
Control Objective	"A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity." (Executive Summary, page 10)
IT Governance	"A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes." (Executive Summary, page 10)

For ease of reference, I capitalize the first letter of "Domain," "Process," "Control Objective," and "Control Practice," when referring to a part of COBIT and when the passage is not a direct quote. So, for example, a business process could use one of the COBIT Processes.

2 Why is COBIT valuable?

There are a number of reasons why COBIT (see Table 1 on page 7 for a list of acronyms) is valuable, including the following:

1. COBIT is a way to implement "IT governance" (see Table 2 on page 8 for definitions).
2. COBIT is inclusive.
3. COBIT was produced by a large group of people.
4. COBIT is maintained.
5. COBIT's sponsoring organization, ITGI, has deep roots.
6. ITGI is bold in its estimation of COBIT's value.
7. ITGI is a non-profit, professional organization.

1. COBIT is a way to implement "IT governance." This is a superset of "computer security." A little history is in order. In the early days of computers, security meant the Bell-La-Padula (BLP) model, characterized by two rules: "no-write-down," and "no-read-up," meaning, in the former case, that BLP forbade a user at security level i from creating a file at security level i-1 or lower, and in the latter case, that BLP forbade a user at security level i from reading a file at security level i+1 or higher. As long as removable media resembled full-sized refrigerators in bulk and weight and as long as there was only one printer and no network, BLP could be proven to be secure. Unfortunately BLP tends to migrate documents to increasingly higher security levels until someone outside the system steps in and re-arranges the labels for the documents. Later came the DoD "Orange Book." This approach presented computer security as a hierarchy. At the bottom of the hierarchy was "Class D," which meant no security. At the top of the hierarchy was "Class A1," which meant provable security. I do not believe that any computers attained Class A1. Currently, we seem to be struggling to accept the notion of "adequate security," as articulated in OMB A-130. On the horizon, I believe, is IT "governance." This is the notion that the expense of security has to be justified in light of business objectives, just as office space and janitorial services do, for example. Business objectives provide the context within which resource allocations can be made rationally. COBIT is a way to implement this notion of IT governance.

2. COBIT is inclusive. ITGI has explicitly built upon previous work in its development of COBIT. The reference lists in the COBIT documents are among the most comprehensive. ITGI continues to "map" (i.e., compare) COBIT to other guidance material.

3. COBIT was produced by a large group of people. The COBIT documents usually list who was on the project team, who was on the project steering committee, and who were the researchers and expert reviewers. This implies a collaborative effort with named individuals.

4. COBIT is maintained. ITGI published version 1 in 1996, version 2 in 1998, and version 3 in 2000. ITGI has moved COBIT on-line, making updates more easy to generate. ITGI has a history of maintaining COBIT. This is important because the area of concern—IT governance—is unusually empirical.

5. COBIT's sponsoring organization, ITGI, has deep roots, tracing its ancestry back 35 years.

6. ITGI is bold in its estimation of COBIT's value:

> COBIT enables the development of clear policy and good practice for IT control through organisations worldwide. Thus, COBIT is designed to be the breakthrough IT governance tool that helps in understanding and managing the risks and benefits associated with information and related IT. (Framework, page 4, bold in the original)

COBIT claims to be "suitable for any enterprise and any platform, worldwide" (COBIT ***Quickstart***, page 44).

7. ITGI is a non-profit, professional organization. (The same is true of ISACA.) So there is no profit motive to muddy ITGI's claims. Most of the COBIT materials are available on-line at no charge.

3 What is COBIT?

COBIT is a way to implement IT governance. It is a "framework that must be tailored to [an] organisation" (Implementation Tool Set, page 25), that "must be used with other resources" (ibid.) in order to "customise this general set of guidelines to [one's own] specific environment" (page 26). In structure, COBIT consists of a set of "Control Objectives" for information technology, designed to enable auditing. The Control Objectives are "guidance," in that they describe what should be accomplished. The difficulty—and hence the rationale for COBIT's existence—is not with the individual Control Objectives, which are relatively simple and unsurprising, but with the sheer number of the Control Objectives from which COBIT was developed. Of the possible objectives, on which do you spend the effort? and which do you ignore? What confidence do you have that you have covered the necessary territory, so to speak, without wasting effort on unnecessary territory?

To make the number and the completeness of that set of Control Objectives easier to grasp, the Control Objectives are grouped into 34 "Processes" (also known as "high-level Control Objectives" in places in the COBIT documents) which, in turn, are grouped into four "Domains." At the other end of the spectrum, ITGI has recently published what it calls "Control Practices" which are amplifications of the Control Objectives. The entire structure—from Domain to Control Practice—is shown in Figure 1.

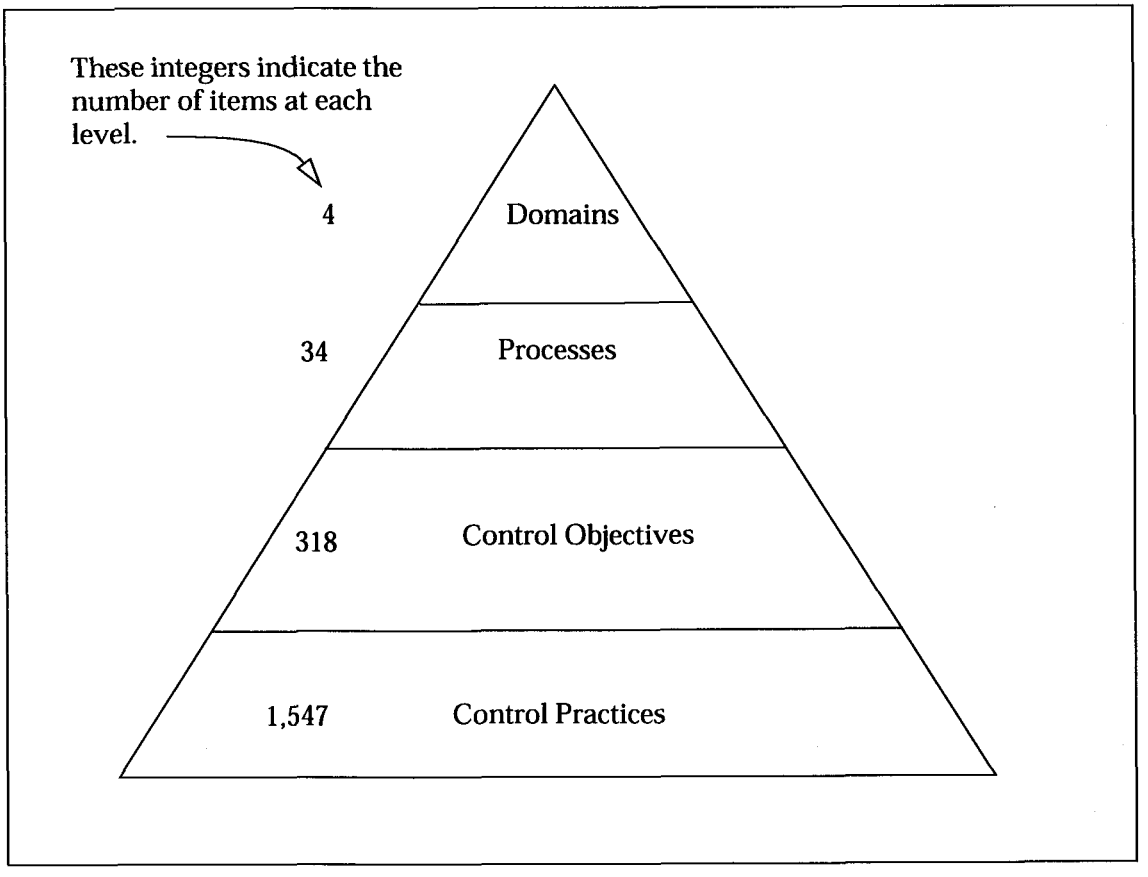

Figure 1 COBIT's Hierarchy

4 What documents are related to COBIT?

In this section I first present ITGI's structure for its documents, shown in Figure 2, followed by the list of documents that ITGI has published associated with COBIT, shown in Table 3, which Table is the substance of this report.

The structure that ITGI uses to organize most of the COBIT documents is shown in Figure 2, reproduced from COBIT *Quickstart*.

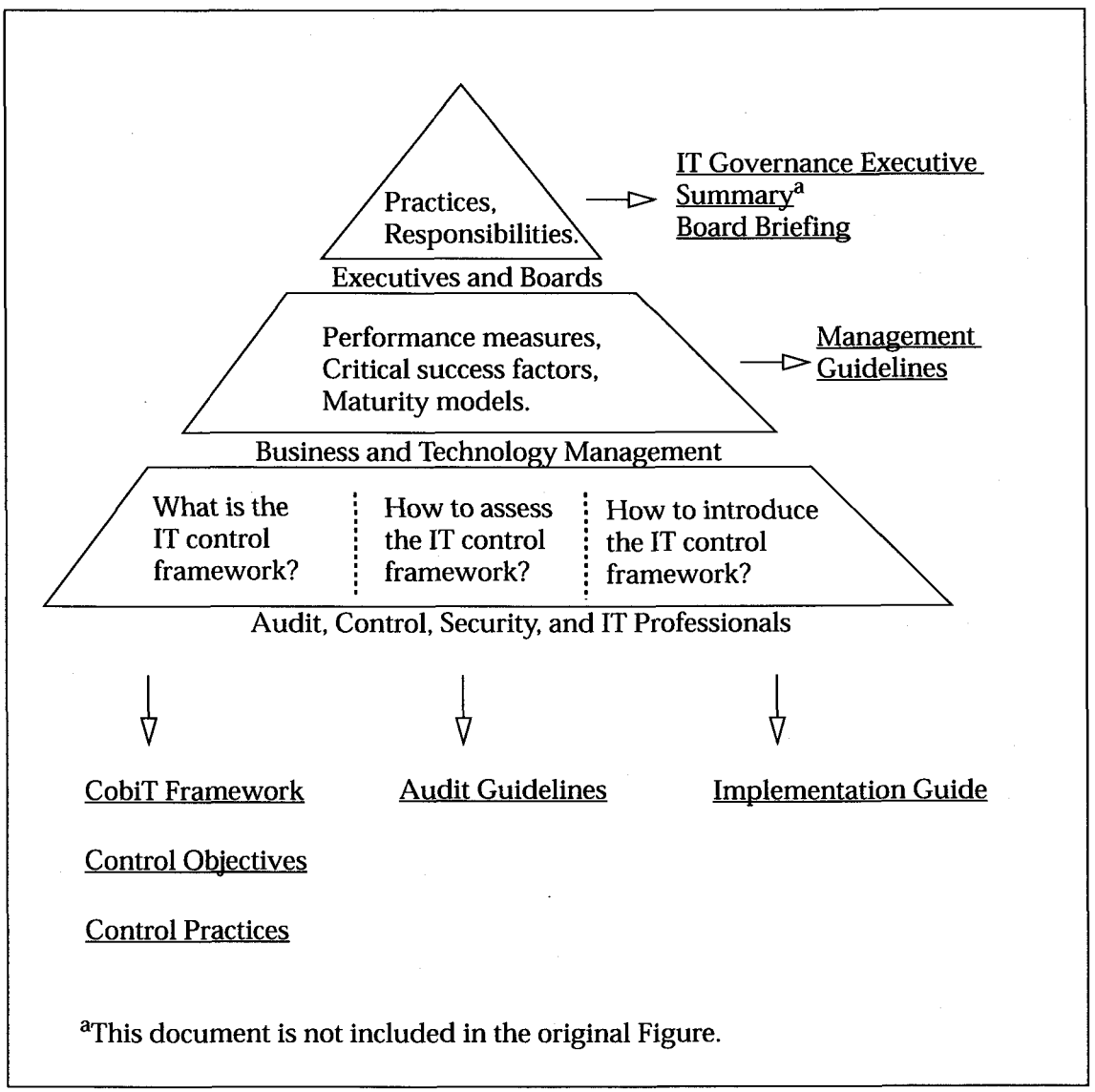

Figure 2 COBIT "Family of Products" (Figure 2, page 8, COBIT *Quickstart*)

I have organized the COBIT documents shown in Table 3 below into the following groups:

1. Initial documents:
   COBIT Security Baseline; and
   COBIT *Quickstart*.
2. COBIT components:[4]
   Executive Summary;
   Framework;
   Control Objectives;
   Control Practices;
   Implementation Tool Set;
   Management Guidelines; and
   Audit Guidelines.
3. COBIT Mapping:[5]
   Information Security Harmonisation: Classification of Global Guidance;
   COBIT Mapping: Overview of International IT Guidance; and
   COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT.
4. Governance documents:
   IT Governance Executive Summary;
   Board Briefing on IT Governance, 2nd Edition; and
   IT Governance Implementation Guide: How do I use COBIT to implement IT Governance?
   Information Security Governance: Guidance for Boards of Directors and Executive Management.
5. Documents produced by others:[6]
   IT Governance Global Status Report; and
   IT Governance—A Pocket Guide Based on COBIT.

4. In Table 3 these documents do not have publication dates since they are assumed, with the advent of COBIT Online, to be current.
5. That is, how does COBIT compare with other guidance documents? and how should it be used?
6. This is not an exhaustive list: ISACA's catalogue for its bookstore runs to 50 pages.

The COBIT documents are shown in Table 3.

Table 3 COBIT documents

Document	Pages	Description	Comments
1. Initial documents			
COBIT Security Baseline (2004)	40	This document describes security DOs and DON'Ts for the following six communities of users: • home user; • professional user; • managers; • executives; • senior executives; and • board of directors/trustees. (See my review of this document in Section 5 on page 25 below.)	This document is similar to but more general than COBIT ***Quickstart***. This document could almost stand independently of COBIT and ITGI, though it is based on the former.
COBIT *Quickstart* (2003)	48	This document describes a 20% subset of COBIT. (See my review of this document in Section 6 on page 27 below.)	This document is intended for those who find COBIT in its entirety to be overwhelming and would like a more gradual way to begin. Two self-tests are provided to enable a reader to gauge where to start. The bulk of the document is its description of 62 of COBIT's 318 Control Objectives.

Table 3 COBIT documents

Document	Pages	Description	Comments
2. COBIT components[a]			
Executive Summary	16	This document describes the basics of COBIT. The material in this document is repeated at the beginning of the Framework document. And the material in the Framework, in turn, is repeated at the beginning of three other documents: Control Objectives, Audit Guidelines, and Implementation Tool Set. An Appendix of Executive Summary document includes material from the Management Guidelines (see below).	This is the document to begin with in order to understand COBIT. But then, since this same material is repeated at the beginning of various other COBIT documents, this is the material that you begin with almost regardless of which of the COBIT component documents you choose as a starting point. This is on purpose, I am sure.
Framework	68	This document describes the 4 Domains and the 34 Processes of COBIT.	This document provides a high-level description of the Domains and Processes.
Control Objectives	148	This document describes the 4 Domains, the 34 Processes, and the 318 Control Objectives of COBIT. Each Control Objective, as the definitions in Table 2 on page 8 note, is a statement. For example, the following is Control Objective DS5.12: "Management should ensure that reaccreditation of security (e.g., through 'tiger teams') is periodically performed to keep up-to-date the formally approved security level and the acceptance of risk." The average Control Objective is approximately twice as long as DS5.12.	A "Control Objective" is "a statement of desired result" (see Table 2 on page 8). The level of detail in this document is such that the reader should consider no more than one Process at a time: considering more is daunting, resulting in loss of focus.

Table 3 COBIT documents

Document	Pages	Description	Comments
Control Practices (2004)	228	This document extends COBIT's 318 Control Objectives with 1,549 (by my count) Control Practice statements.	A set of "Control Practice statements" describes how one would go about fulfilling a Control Objective. Note that Control Practice statements constitute a fourth level of detail in COBIT, the first three being the 4 Domains, the 34 Processes, and the 318 Control Objectives.
Implementation Tool Set	86	This document describes how to introduce and implement COBIT in an organization. It includes "Management Awareness Diagnostics" and "IT Control Diagnostics" in the form of spreadsheets. The document also includes case studies and an FAQ.	If you already know that you want to implement COBIT, this is the document that will help you do so in a rational manner. If you are unsure whether you want to implement COBIT, see COBIT *Quickstart*. If you are just interested in general security, see COBIT Security Baseline.
Management Guidelines	122	This document describes the following for each of the 34 Processes: • "Maturity Model," • "Critical Success Factors," • "Key Goal Indicators," and • "Key Performance Indicators.	The model, factors and indicators described in this document are intended for use by management, as the name of the document implies. They should provide a way for management to keep tabs on organizational processes.
Audit Guidelines	226	This document provides audit guidance on the following for each Process: • "Obtaining an understanding," • "Evaluating the controls," • "Assessing compliance," • "Substantiating the risk of the control objectives not being met."	This document is thorough and intended to provide auditors with sufficient structure to gather sufficient evidence to support their conclusions.

Table 3 COBIT documents

Document	Pages	Description	Comments
3. COBIT Mapping[b]			
Information Security Harmonisation: Classification of Global Guidance (2005)	150	This document reviews the "most commonly known and accepted worldwide guidance" (page 1): •BS 7799 •COBIT •SSE-CMM® •GAISP Version 3.0 •ISF's "Standard for Good Practice for Information Security" •ISO/IEC 13335 •ISO/TR 13569:1997 •ISO/IEC 15408:1999 •ISO/IEC 17799:2000 •ITIL's "Security Management" •NIST 800-12 •NIST 800-14 •NIST 800-18 •NIST 800-53 •OCTAVE® Criteria Version 2.0 •OECD's "Guidelines for the Security of Information Systems and Networks and Associated Implementation Plan" •Open Group's "Manager's Guide to Information Security"	For reference to additional guidance material, see Philip L. Campbell, An Introduction to Control Frameworks. SAND2002-0131, September 2003, available from Sandia National Laboratories. Guidance I helped develop for the U.S. House Government Reform Committee in November 2004 is available at http://www.educause.edu/ir/library/pdf/CSD3661.pdf

Table 3 COBIT documents

Document	Pages	Description	Comments
COBIT Mapping: Overview of International IT Guidance (2004)	56	This document compares COBIT with the following guidance material: •ITIL •ISO/IEC 17799 •ISO/IEC 13335 •ISO/IEC 15408 •TickIT •NIST •COSO	This document concludes that COBIT is "broader" than these documents and almost as "deep" as the deepest (see Figure 3 on page 23 below). This document is the "first deliverable" for the COBIT Mapping project.
COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT (2004)	146	This document compares COBIT with ISO/IEC 17799:2000, addressing the following questions: •"Can we use COBIT instead of ISO/IEC 17799:2000? •"Why do we need to follow two standards? •"What are the differences between these two standards? •"How do we use these two standards? •"Can we use these two standards together to meet regulatory compliance?" (from the summary of this document on the ISACA site)	The summary on the ISACA site notes that "...these two standards do not compete against each other, in fact they are mutually complementary. COBIT by its nature is broader and ISO/IEC 17799 tends to be deeper in the areas of security." However, the document itself, I believe, suggests that COBIT is a proper superset: the "Conclusion" is primarily a table that shows ISO's coverage of COBIT and not vice versa. (The "Control Practices," which provide more depth to COBIT, do not appear in the document, that I could see. They would lend more weight to the idea that COBIT is a proper superset.) This document is the "second deliverable" for the COBIT Mapping project.

Table 3 COBIT documents

Document	Pages	Description	Comments
4. Governance documents			
IT Governance Executive Summary (undated)	7	This short document describes the why, what, and how of IT governance, noting that IT involves "hugh costs, "enormous risks," and "extraordinary opportunities." This document encourages the use of an (1) IT Strategy Committee, (2) risk management, and (3) an IT Balanced Scorecard.	This is an easy, board-level document with which to begin "IT governance."
Board Briefing on IT Governance 2nd Edition (2003)	64	This document provides guidance on (1) the meaning and importance of IT governance, and (2) how to implement IT governance (using a simple, seven point plan) and how to measure performance. IT governance consists of five aspects: •strategic alignment, •value delivery, •risk management, •resource management, and •performance management. Appendices include checklists, tools, and models, as well as notes about governance standards" such as COSO, Cadbury, Turnbull, OECD Guidelines, BIS, and COBIT.	This document explains, in a conceptual fashion, how boards can implement IT governance.
IT Governance Implementation Guide: How do I use COBIT to implement IT Governance? (2003)	58	The bulk of this document is a four phase, 12 step "implementation action plan." This is preceded by a discussion on the nature and importance of IT governance.	This document describes, in a chronological fashion, how to implement IT governance via COBIT. The audience for this document is primarily "Audit, Control, Security, and IT Professionals," as suggested by its placement in Figure 2 on page 13.

Table 3 COBIT documents

Document	Pages	Description	Comments
Information Security Governance: Guidance for Boards of Directors and Executive Management (2001)	28	This document answers questions such as • What is information security? • Why is it important? • What should the board do about it? Part of the answer includes the following advice: • adopt best practices; • consider critical success factors; and • introduce performance measures. This document briefly reviews other guidance documents, namely OECD, IFAC, ISO/IEC 17799, AICPA's SysTrust™, and COBIT. This document is the basis for the Board Briefing document (see above).	This is a readable, sensible document.

Table 3 COBIT documents

Document	Pages	Description	Comments
5. Documents produced by others			
IT Governance Global Status Report (2004)	72	This document describes results from a worldwide survey in 2003 on IT governance, paid for by ITGI and carried out by PricewaterhouseCoopers.	ITGI wanted to know the status of IT governance across the world—how is it perceived (i.e., do people see a need?) and what tools are used? The interviewers asked 25 questions of 335 people. The findings suggest that business leaders acknowledge the importance of IT and, among the 18% who know about COBIT, they consider COBIT to be the preferred way to implement IT governance (page 6).
IT Governance—A Pocket Guide Based on COBIT (2004) ITSM Pocket Library, published by Van Haren Publishing	151	Koen Brand & Harry Boonen wrote this document, independently of ITGI, with over 70 people on the "International Review Team." Brand & Boonen found COBIT to be "best practice," but they note that the document they have produced "differs from COBIT in several ways, by adding new information to the structure from the perspective of IT Service Management" (page 13). The bulk of this document describes activities in COBIT Processes using bullets and flowcharts. This document also describes COBIT's background and publication. It summarizes various "sources" for IT governance, namely COSO, ISO/IEC 17799, CMM/SPICE, Common Criteria, quality models, Balanced Scorecard, and COBIT.	This is a concise and handy document, small enough to fit in a shirt pocket. The description of COBIT and the various sources is good.

a. I believe that all of the documents in the COBIT components are available on-line at no cost except for Audit Guidelines and Control Practices.

b. The documents in this category "map" (or compare) COBIT with other guidance material.

The following figure is referenced in the "COBIT Mapping: Overview of International IT Guidance" cell of Table 3 above.

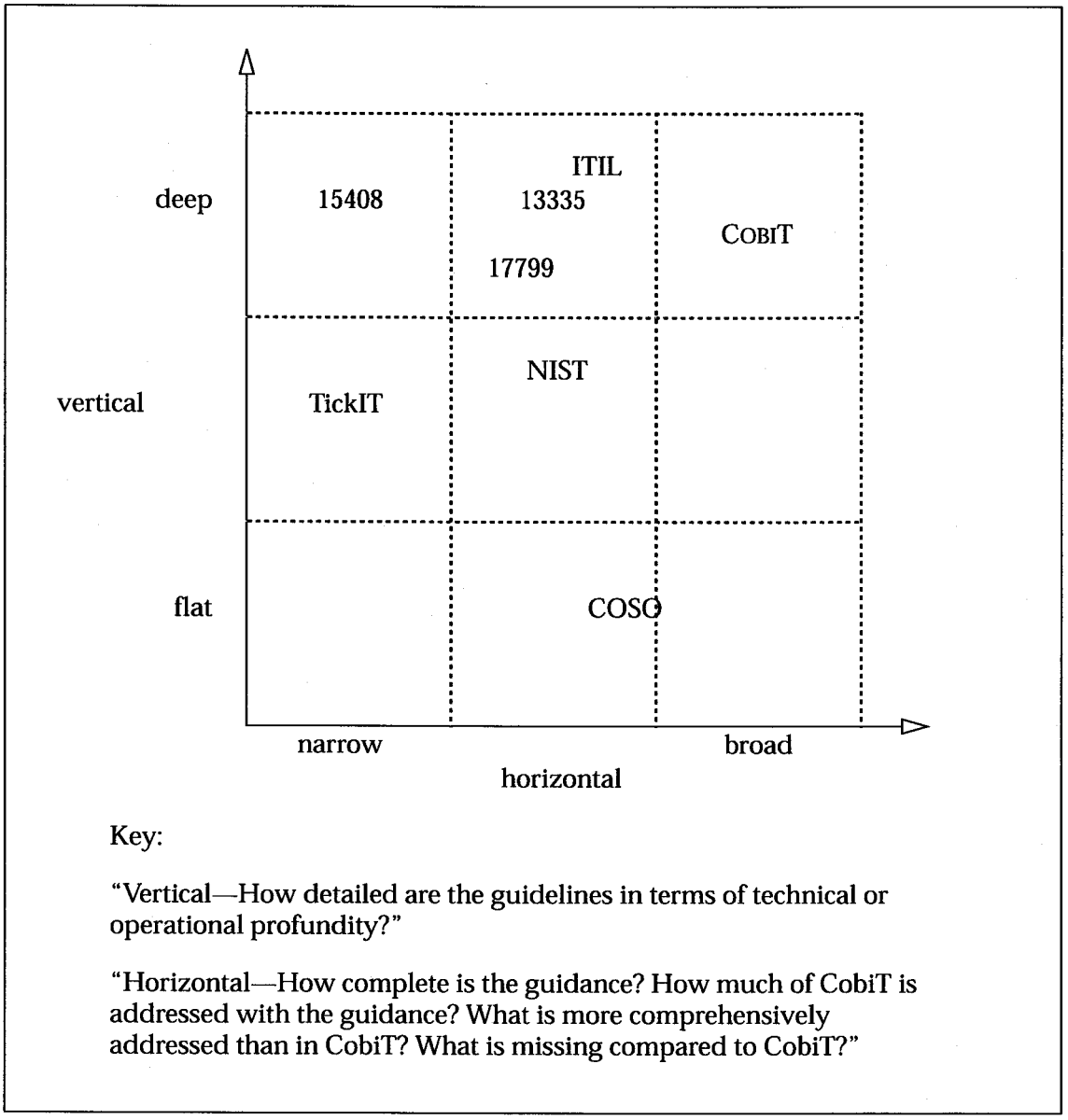

Figure 3 "High-level Mapping of Guidance to COBIT Domains" (Figure 7, page 50, CobiT Mapping: Overview of International IT Guidance.)

This is a blank page.

5 Review of CobiT Security Baseline

5.1 Summary

The Cobit Security Baseline document is a distillation of CobiT for various user groups. The document consists of the following parts:

"Introduction"

"Information Security Defined"

"Security—Why is it Important?"

The document lists ten reasons, such as "Competitive Disadvantage" (page 10).

"The CobiT Security Baseline—39 Steps to Security"

This section describes 39 "steps" to security and maps each to Control Objectives in Cobit and ISO 17799. For example, the following is the first such step: "Identify information and services critical to the enterprise and consider their security requirements" (page 12).

"Information Security Survival" Kits

There are in this section the following "kits" for the following groups:

Home Users (one part of the kit for the "nontechnical" Home User and another part of the kit for the "technically competent" Home User),

Professional Users,

Managers,

Executives,

Senior Executives, and

Boards of Directors/Trustees.

Each section consists of approximately two dozen items, such as the following, which is the first item for "non-technical" Home Users: "Obtain guidance from time to time from qualified and reputable advisors (certified technicians) to ensure that the computer installation has no significant security flaws" (page 19).

"Summary of Technical Security Risks"

(e.g., "Trojan Horse programs," "Back door and administration programs")

"References"

This section presents publications, periodicals, and URLs in the following sub-sections:

General information security and IT governance standards and frameworks;

General information security web sites;

Technical information security guides;

Information security news;

CobiT materials; and

Other CobiT materials.

The printed version of this document comes with six, separate cards, each of which has the information for one of the "information security survival kits."

5.2 Comments

This is a handy document that should enable just about anyone to begin the process of security. The references and pointers provide the way to continue and add more depth. That all this fits into only 40 pages is impressive.

6 Review of CobiT *Quickstart*

6.1 Summary

CobiT *Quickstart*, is a subset (about 20%) of CobiT. It claims to be a "simple-to-use tool that will speed up implementation of key IT Control Objectives" (page 10). It is "a set of 'smart things to do'" (page 4). The heart of the document is a "baseline" presented in 15 pages and described below. *Quickstart* is designed with three cases in mind:

1. for "small and medium-sized enterprises" (SMEs);
2. for organizations where "IT is not strategic or absolutely critical for survival;"
3. as a "starting point...toward an appropriate of control and governance for IT." (page 4)

Quickstart implements the "top-down" philosophy of the "IT Governance Implementation Guide" (see Table 3 on page 15) produced by ITGI, namely

1. start with business goals;
2. do a risk analysis;
3. identify IT goals and important IT processes;
4. identify the set of "Control Practices" to be implemented or continuously improved.

Quickstart consists of two parts: a "framework" and a "baseline." The framework describes (1) what *Quickstart* is, (2) why it is needed, (3) how to determine its suitability for a given organization, and (4) how to use the baseline. Suitability is determined via two "tests." The first test, "Stay in the Blue," enables the organization to gauge itself in seven areas, such as "Simple Command Structure." For each area a discrete scale is given. For example, this is the scale for the first area (i.e., an organization would rank itself based on this scale by choosing the appropriate number):

Simple Command Structure (SCS)

1. *CS is informal and verbal, only short-term and tactical.*
2. *CS is primarily informal and verbal, somewhat short-term but largely medium-term-oriented, and still primarily tactical.*
3. *CS is primarily formal and documented, begins looking at the long-term but is more medium term-oriented, somewhat tactical with strategic views emerging.*
4. *CS is strictly formal and documented, covers short-, medium- and long-term and is strategy oriented. (page 12)*

The framework bifurcates each scale, coloring the low part of the bifurcation blue in Figure 4 of the document (page 12). If an organization gauges itself "mainly" in the blue (i.e., low) area, then *Quickstart* is probably appropriate; otherwise the organization needs more than *Quickstart*, possibly the full set of Control Objectives in Cobit. However, the framework lists environmental variables that could suggest that the organization needs more than *Quickstart*, even if the organization ranks in the blue on this test. This set of environmental variables, along with a scale for each, is the second suitability test. The points on each scale in Figure 5 of the document (page 13) are colored from "cool" to "hot"—from green, to yellow, to orange, to red.

The name of this second test is "Watch the Heat." (Both of these tools, in Excel spreadsheet form, are on a CD that accompanies the document.)

The *Quickstart* baseline consists of 62 Control Objectives derived from many but not all of CobiT's 318 original Control Objectives. For each Control Objective in the baseline, "Critical Success Factors" and "Metrics" are listed, along with a "potential assessment approach" consisting of a seven-point scale from "Management not aware" to "Solution optimised." (Alternatively, CobiT's five-point "maturity" scale ("Ad-Hoc" to "Optimised") could be used.) As an example, here are the first two Control Objectives (the two of them share the same Critical Success Factors and Metrics; the original Control Objective in CobiT from which the current Control Objective is derived, is suffixed to each objective (e.g., "(CO ref. 1.1)"):

PO1—Define a strategic plan

IT strategy is aligned with and supports the overall business strategy.

1. *Consider what support you need from IT to achieve business goals and verify whether the application of IT can create business opportunities. (CO ref. 1.1)*
2. *Evaluate how IT is supporting your current and future business goals in terms of availability and functionality. Do this on a regular basis with key staff. Consider value for money, current total cost of ownership and future replacement cost. Adapt your plans accordingly. (CO ref. 1.5, 1.7, 1.8)*

Critical Success Factors

- *Quantification and tracking of the business contribution of IT investments*
- *A clear position on the balance between cost, speed and quality*

Metrics

- *A clear position on the balance*
- *Acceptable and reasonable number of outstanding requirements*
- *Extent of staff participation*
- *Time since last evaluation*

The first Appendix in the document contains two "Diagnostic Tables," both of which are binary tables (i.e., each cell has two possible "values," either an "X" or blank). In the first table, the rows list approximately 77 "Risk Factors" (such as "IT failing to help the organization maintain competitive position" and "Inadequate IT capability to develop new IT requirements") and the columns list five "Governance Issues" (such as "Strategic Alignment" and "Value Delivery") and nine "Technology Issues for Management" (such as "Cost Optimisation" and "Service Delivery"). If the Risk Factor applies, there is an X in the appropriate cell, a blank otherwise.

In the second table, the rows list the 62 Control Objectives from the *Quickstart* baseline, and the columns are the same as in the previous table. This table enables management to understand the relevance of given Control Objectives to management issues. Since the two tables share columns, they together enable management to connect Risk Factors with Control Objectives, though in a tedious way.

The second Appendix in the document summarizes the "components" in CobiT, i.e., the "Family of Products" described in Figure 2 of this report and summarized above.

6.2 Comments

I think *Quickstart* fulfills its goal of providing a core subset of CobiT. I would say that it is adequate for organizations that are considering implementing only a subset of CobiT or find CobiT overwhelming and want to implement it gradually. The document is remarkably succinct. The document provides a good description of its context, which provides the assurance that more depth and breadth is available. It is reasonable to presume that this document, like the others from ITGI, will be maintained.

This is a blank page.

7 Review of Control Practices

IT Governance Institute (ITGI), Control Practices. 2004. 224 pages. ISBN 1-893209-83-0.

7.1 Summary

Control Practices describes the almost 1,600 "Control Practices" (1,547 by my count) that extends the Domain-Process-Control-Objective hierarchy. If a Control Objective could be said to describe what is to be accomplished, then the set of Control Practices for a given Control Objective describes why and how that Control Objective is to be accomplished (see page 6) by making what appear to be statements of fact, such as, "The need to prepare and maintain a systematic risk assessment process is defined in a policy" (PO9.2.1).[7] Given such a Control Practice, it is simple to ask questions such as, What is our policy? Is it effective and efficient? If we do not have a policy—and management could legitimately decide not to have one—what are the reasons for our not having one?

Here is another example Control Practice: "An impact analysis is conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control" (AI5.6.2). For each Control Practice it should be a reasonable exercise to identify the relevant controls and evaluate their effectiveness and efficiency.

The format in the "Control Practices" document for each of the 34 Processes is the same. An "Introduction" section consists of three sub-sections entitled, "What?" "How?" and "Why?" that answer those questions for that Process. This is followed by a section for each Control Objective, each of which, in turn, consists of two subsections, the first entitled "Why Do It?" and the second a listing of the Control Practices themselves. The following shows this organization in outline form:

Introduction
- *What?*
- *How?*
- *Why?*

Control Objective 1
- *Why Do It?*
- *<control practices>*

Control Objective 2
- *Why Do It?*
- *<control practices>*

...

As an example of a Control Objective section, consider DS5.5 (this is an exceptionally short

7. Syntax: "PO9.2.1," reading from right to left, identifies this Control Practice as the first Control Practice for the second Control Objective of the ninth Process in the "Plan & Organise" Domain.

one):[8]

DS5.5 Management Review of User Accounts

Why Do It?

The appropriate organization of management review of user accounts in line with the control practices will:

- ***Ensure that unauthorized changes to access rights are detected in a timely manner.***

1. Control Practice

Access rights are reviewed periodically to confirm that they are still as granted and they correspond to the user's and the organisation's needs. (page 133)

This Control Practice, like all of the Control Practices, is intended to explain how the goals or purposes of the Control Objective are to be achieved. We could develop a control based on this Control Practice if we added at least (a) the period within which the review is to take place, (b) who is to do the reviewing, and (c) which rights are to be reviewed.

To flesh out the example above, consider another example (this one almost as short as DS5.5):

DS5.4 Security of Online Access to Data

Why Do It?

Proper implementation of security of online access to data in line with the control practices will ensure that:

- ***Access to data is granted on a need-to know basis***
- ***Appropriate segregation exists amongst production, test and development environments***

Control Practices

1. ***Access to data is granted on a need-to know basis.***
2. ***Strict controls are maintained over access to production libraries.***
3. ***Production source libraries are updated only via a formal change process by designated staff with change control responsibilities.***
4. ***Key security parameters and processes are identified and their content is periodically compared to protected baseline of authorized contents. (page 132)***

The Control Practices are quite evenly spread through the Control Objectives: there are usually 4 per Control Objective. The highest number of Control Practices per Control Objective is 21, shared by DS 5.1 and DS5.2, and there are five that have only one (all of them in DS5, oddly enough). Almost all of the Control Practices are short sentences such as those shown above. A few of the Control Practices are longer, such as PO5.3.2 which contains 7 bulleted items, or

8. I have chosen this Control Objective and a subsequent one based on two criteria: they are both short and they both deal with subjects that are familiar to anyone who deals with computer security.

AI1.15.2 which is 9 sentences in 26 lines of text, to take two examples.

There are recurring patterns in the Control Practices. Each Introduction section notes that "The desired control is accomplished by implementing a selection of..." the Control Objectives for the Process, implying that the Control Objectives are intended to be suggestions from which an organization should choose the appropriate set, rather than blindly attempt to implement all of them.

Most of the Introduction sections end with the following sentence: "The implementation of the control objectives and related practices [for this Process] is based on a collaborative, informed, holistic, cost-benefit-risk trade-off assessment."[9] One of the Processes for which this sentence does not appear is the first Process, PO1. The Introduction for that Process begins with the following sentence: "The high-level control objective [i.e., Process] of accomplishing an optimum balance of information technology opportunities and business requirements for IT is enabled by a strategic planning process undertaken at regular intervals giving rise to long-range plans that are periodically translated into operational plans setting clear and concrete short-range goals" (page 8).

Another pattern is at the beginning of the "Why?" subsection: "Organisations that have successfully implemented processes to [fulfill the intent of the Process, such as, for PO1, "define a strategic IT plan"] have reported many benefits."

There are almost no internal references in the set of Control Practices. The only one I noticed is in DS10.1.8, which refers to AI6, DS9, and DS13. I believe that this scarcity of internal references is deliberate, so that the Control Practices are independent of each other and can be assessed without the complexity inherent with loops.

7.2 Comments

This last layer in the Cobit hierarchy seems to "touch ground" so to speak. That is, the set of Control Practices seems sufficiently detailed to enable organizations to implement and evaluate their own controls.

At approximately 1,600 Control Practices, there is overwhelming detail that can be considered if IT governance is to be taken seriously (and presuming that the approach that ITGI advocates does not have superfluous material). Attending to this amount of detail would be impossible—like floundering in a Sargasso Sea—without some systematic way to proceed. The hierarchy provides that systematic way to proceed. There is no way automatically to generate such detail. For example, I do not believe that there is a grammar that we could define and could then use to generate this detail. Without a grammar we can only estimate necessity and sufficiency, and that both of those can be estimated only empirically, using judgment gleaned from experience to expand, contract, and generally adjust the CobiT hierarchy. Hopefully, over time the CobiT

9. "Most" in this case is 24 of 34. The Processes that do not include this sentence are PO1, PO4, PO7, PO10, AI4, DS3, DS8, DS11, M1, and M2. M1 and M2 use the phrase "based on a collaborative, informed, and holistic process" (page 186); others refer to "the most efficient and cost-effective manner" (DS3, page 117); for still others different standards apply, or the Process, such as PO1, is part of the collaborative process.

hierarchy comes increasingly closer to some ineffable ideal.

I note that there were eight people on the committee that produced this document, and there were 58 "contributors." The name and credentials and employer of each person is included, which bodes well for the document. The bibliography is extensive, one of the best I have seen (pages 206-10).

(I got a chuckle out of the photograph on the cover of this document: it is a close up of a "ctrl" key.)

Distribution:

2	MS	0899	Technical Library, 9616
1	MS	9018	Central Technical Files, 8945-1