The IT Governance Institute™ is pleased to offer you this complimentary download of CobiT®

CobiT provides good practices for the management of IT processes in a manageable and logical structure, meeting the multiple needs of enterprise management by bridging the gaps between business risks, technical issues, control needs and performance measurement requirements. If you believe as we do, that CobiT enables the development of clear policy and good practices for IT control throughout your organisation, we invite you to support ongoing CobiT research and development.

There are two ways in which you may express your support: (1) Purchase CobiT through the Association (ISACA) Bookstore (please see the following pages for order form and Association membership application. Association members are able to purchase CobiT at a significant discount); (2) Make a generous donation to the Information Systems Audit and Control Foundation, which sponsors the IT Governance Institute.

The complete CobiT package consists of all six publications, an ASCII text diskette, four CobiT implementation/orientation Microsoft® PowerPoint® presentations and a CD-ROM.
A brief overview of each component is provided below. Thank you for your interest and support of CobiT!

For additional information about the IT Governance Institute visit www.ITgovernance.org

Management Guidelines

To ensure a successful enterprise, you must effectively manage the union between business processes and information systems. The new *Management Guidelines* is composed of Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators. These *Management Guidelines* will help answer the questions of immediate concern to all those who have a stake in enterprise success.

Executive Summary

Sound business decisions are based on timely, relevant and concise information. Specifically designed for time-pressed senior executives and managers, the CobiT *Executive Summary* consists of an Executive Overview which explains CobiT's key concepts and principles.

Framework

A successful organization is built on a solid framework of data and information. The *Framework* explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The *Framework* identifies which of the seven information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objective.

Audit Guidelines

Analyze, assess, interpret, react, implement. To achieve your desired goals and objectives you must constantly and consistently audit your 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.

Control Objectives

The key to maintaining profitability in a technologically changing environment is how well you maintain control. CobiT's *Control Objectives* provides the critical insight needed to delineate a clear policy and good practice for IT controls. Included are the statements of desired results or purposes to be achieved by implementing the 318 specific, detailed control objectives throughout the 34 high-level control objectives.

Implementation Tool Set

An Implementation Tool Set, which contains Management Awareness and IT Control Diagnostics, Implementation Guide, frequently asked questions, case studies from organizations currently using CobiT and slide presentations that can be used to introduce CobiT into organizations. The tool set is designed to facilitate the implementation of CobiT, relate lessons learned from organizations that quickly and successfully applied CobiT in their work environments and assist management in choosing implementation options.

CD-ROM

The CD-ROM, which contains all of CobiT, is published as a Folio infobase. The material is accessed using Folio Views®, which is a high-performance, information retrieval software tool. Access to CobiT's text and graphics is now easier than ever, with flexible keyword searching and built-in index links (optional purchase).

A network version (multi-user) of CobiT 3rd Edition will be available. It will be compatible with Microsoft Windows NT/2000 and Novell NetWare environments. Contact the ISACA Bookstore for pricing and availability.

See Order Form, Donation Information and Membership Application on the following pages.

We invite your comments and suggestions regarding CobiT. Please visit www.isaca.org/cobitinput.htm

ISACF Contribution Form

Contributor: _____

Address: _____

_____

City _____ State/Province _____

Zip/Postal Code _____ Country _____

Remitted by: _____

Phone: _____

e-mail: _____

For information on the Foundation and contribution benefits see www.isaca.org/finfo.htm

Contribution amount (US $):

☐ $25 (donor) ☐ $100 (Silver) ☐ $250 (Gold)

☐ $500 (Platinum) ☐ Other US $_____

☐ Check enclosed payable in US $ to ISACF

☐ **Charge my:** ☐ VISA ☐ MasterCard ☐ American Express ☐ Diners Club

Card number _____ Exp. Date _____

Name of cardholder: _____

Signature of cardholder: _____

Complete card billing address if different from address on left

_____

_____

_____

U.S. Tax ID number: 95-3080691

Fax your credit card contribution to ISACF at +1.847.253.1443, or mail your contribution to: ISACF, 135 S. LaSalle Street, Department 1055, Chicago, IL 60674-1055 USA

Direct any questions to Scott Artman at +1.847.253.1545, ext. 459 or finance@isaca.org

Thank you for supporting CobiT!

Recent ISACF Research Projects

Control Objectives for Net Centric Technology, NCC

Member - $90 Non-member - $130

Digital Signatures

Security & Controls, ISDS

Member - $35 Non-member - $50

In Partnership with

Deloitte & Touche

e-Commerce Security

A Global Status Report, ISEC

Member - $35 Non-member - $50

e-Commerce Security

Enterprise Best Practices, 2-EC

Member - $30 Non-member - $40

e-Commerce Security

Trading Partner Identification, Registration and Enrollment, TRS-1

Member - $35 Non-member - $50

For additional information on these publications and others offered through the Bookstore, please visit www.isaca.org/pubs1.htm

Pricing and Order Form

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

IT GOVERNANCE INSTITUTE™

	CODE	ISACA Members	Non-Members
Complete COBIT® 3rd Edition©	CB3S CB3SC	$70 (text only) $115 (text and CD-ROM)	 $225 (text and CD-ROM)

COBIT 2nd Edition purchasers - see *www.isaca.org/3upgrade.htm* for special upgrade pricing.
Individual components are also available for purchase:

	CODE	ISACA Members	Non-Members
Executive Summary	CB3E	$3	$3
Management Guidelines	CB3M	$40	$50
Framework	CB3F	$15	$20
Control Objectives	CB3C	$25	$30
Audit Guidelines	CB3A	$50	$155
Implementation Tool Set	CB3I	$15	$20

All prices are US dollars. Shipping is additional to all prices.

Name _____ Date _____

ISACA Member: ❑ Yes ❑ No Member Number _____
If an ISACA Member, is this a change of address? ❑ Yes ❑ No

Company Name _____

Address: ❑ Home ❑ Company _____

City _____ State/Province _____ Country _____ Zip/Mail Code _____

Phone Number ( ) _____ Fax Number ( ) _____

E-mail Address _____ Special Shipping Instructions or Remarks _____

_____

Code	Title / Item	Quantity	Unit Price	Total
All purchases are final. ***All prices are subject to change.***			***Subtotal***	
			Illinois (USA) residents, add 8.25% sales tax, or Texas (USA) residents, add 6.25% sales tax	
			Shipping and Handling – see chart below	
			TOTAL	

PAYMENT INFORMATION – PREPAYMENT REQUIRED

❑ Payment enclosed. Check payable in U.S. dollars, drawn on U.S. bank, payable to the Information Systems Audit and Control Association.
❑ Charge to ❑ VISA ❑ MasterCard ❑ American Express ❑ Diners Club
(Note: All payments by credit card will be processed in U.S. Dollars)

Account # _____ Exp. Date _____

Print Cardholder Name _____ Signature of Cardholder _____

Cardholder Billing Address if different than above _____

_____

Shipping and Handling Rates

For orders totaling	Outside USA and Canada	Within USA and Canada
Up to US$30	$7	$4
US$30.01 - US$50	$12	$6
US$50.01 - US$80	$17	$8
US$80.01 - US$150	$22	$10
Over US$150	15% of total	10% of total

Please send me information on: ❑ Association membership ❑ Certification ❑ Conferences ❑ Seminars ❑ Research Projects

ISACA BOOKSTORE
135 SOUTH LASALLE, DEPARTMENT 1055, CHICAGO, IL 60674-1055 USA
TELEPHONE: +1.847.253.1545, EXT. 401 FAX: +1.847.253.1443 E-MAIL: *bookstore@isaca.org*
WEB SITE: *www.isaca.org/pubs1.htm*

PDF

Information Systems Audit and Control Association

MEMBERSHIP APPLICATION

Please complete both sides
U.S. Federal I.D. No. 23-7067291
www.isaca.org
membership@isaca.org

Date_____
MONTH/DAY/YEAR

☐ MR. ☐ MS. ☐ MRS. ☐ MISS ☐ OTHER _____

Name_____
FIRST MIDDLE LAST/FAMILY

_____
PRINT NAME AS YOU WANT IT TO APPEAR ON MEMBERSHIP CERTIFICATE

Residence address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Residence phone _____ Residence facsimile _____
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

Company name _____

Business address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

Business phone _____ Business facsimile _____
AREA/COUNTRY CODE AND NUMBER AREA/COUNTRY CODE AND NUMBER

E-mail _____

Send mail to
☐ Home
☐ Business

Form of Membership requested
☐ Chapter Number *(see reverse)*_____
☐ Member at large *(no chapter within 50 miles/80 km)*
☐ Student *(must be verified as full-time)*
☐ Retired *(no longer seeking employment)*

☐ I do not want to be included on a mailing list, other than that for Association mailings.

How did you hear about ISACA?
1 ☐ Friend/Co-worker
2 ☐ Employer
3 ☐ Internet Search
4 ☐ IS Control Journal
5 ☐ Other Publication
6 ☐ Local Chapter
7 ☐ CISA Program
8 ☐ Direct Mail
9 ☐ Educational Event

Current field of employment *(check one)*
1 ☐ Financial
2 ☐ Banking
3 ☐ Insurance
4 ☐ Transportation
5 ☐ Retail & Wholesale
6 ☐ Government/National
7 ☐ Government/State/Local
8 ☐ Consulting
9 ☐ Education/Student
10 ☐ Education/Instructor
11 ☐ Public Accounting
12 ☐ Manufacturing
13 ☐ Mining/Construction/Petroleum
14 ☐ Utilities
15 ☐ Other Service Industry
16 ☐ Law
17 ☐ Health Care
99 ☐ Other

Date of Birth_____
MONTH/DAY/YEAR

Level of education achieved
(indicate degree achieved, or number of years of university education if degree not obtained)
1 ☐ One year or less
2 ☐ Two years
3 ☐ Three years
4 ☐ Four years
5 ☐ Five years
6 ☐ Six years or more
7 ☐ AS
8 ☐ BS/BA
9 ☐ MS/MBA/Masters
10 ☐ Ph.D.
99 ☐ Other _____

Certifications obtained (other than CISA)
1 ☐ CPA
2 ☐ CA
3 ☐ CIA
4 ☐ CBA
5 ☐ CCP
6 ☐ CSP
7 ☐ FCA
8 ☐ CFE
9 ☐ MA
10 ☐ FCPA
11 ☐ CFSA
12 ☐ CISSP
99 ☐ Other _____

Work experience
(check the number of years of Information Systems work experience)
1 ☐ No experience
2 ☐ 1-3 years
3 ☐ 4-7 years
4 ☐ 8-9 years
5 ☐ 10-13 years
6 ☐ 14 years or more

Current professional activity *(check one)*
1 ☐ CEO
2 ☐ CFO
3 ☐ CIO/IS Director
4 ☐ Audit Director/General Auditor
5 ☐ IS Security Director
6 ☐ IS Audit Manager
7 ☐ IS Security Manager
8 ☐ IS Manager
9 ☐ IS Auditor
10 ☐ External Audit Partner/Manager
11 ☐ External Auditor
12 ☐ Internal Auditor
13 ☐ IS Security Staff
14 ☐ IS Consultant
15 ☐ IS Vendor/Supplier
16 ☐ IS Educator/Student
99 ☐ Other _____

Payment due

• Association dues	$ 110.00 (US)
OR student/retired dues ($55 US)	$ _____ (US)
• Chapter dues *(see the following page)*	$ _____ (US)
• New Member processing fee	$ 30.00 (US)*
PLEASE PAY THIS TOTAL	$ _____ (US)

* Membership dues consist of Association dues, Chapter dues and New Member processing fee. (Processing fee does not apply to Student/Retired Members.)

Method of payment
☐ Check payable in U.S. dollars, drawn on U.S. bank
☐ Send invoice**
☐ MasterCard ☐ VISA ☐ American Express ☐ Diners Club

All payments by credit card will be processed in US$'s

** Applications cannot be processed until dues payment is received.

ACCT # _____

Print Name of Cardholder _____

Expiration Date _____
MONTH/DAY/YEAR

Signature _____

Cardholder billing address if different than address provided above:

_____

By accepting membership to the Information Systems Audit and Control Association, members agree to hold the Association and the Information Systems Audit and Control Foundation, its officers, directors, agents, trustees, and employees, harmless for all acts or failures to act while carrying out the purpose of the Association and the Foundation as set forth in its respective bylaws.

Initial payment entitles New Members to membership beginning the first day of the month following the date payment is received by International Headquarters through the end of that year. No rebate of dues is available upon early resignation of membership.

Contributions or gifts to the Information Systems Control Association are not tax-deductible as charitable contributions in the United States. However, they may be tax-deductible as ordinary and necessary business expenses.

Membership dues allocated to a 1-year subscription to the *IS Control Journal* are as follows: $45 for U.S. Members, $60 for non-U.S. members. This amount is non-deductible from dues.

Make checks payable to:
Information Systems Audit and Control Association

Mail your application and check to:
Information Systems Audit and Control Association
135 S. LaSalle, Dept. 1055
Chicago, IL 60674-1055 USA
Phone: +1.847.253.1545 x470 or x405
Fax: +1.847.253.1443

PDF

U.S. dollar amounts listed below are for local Chapter dues, and are subject to change without notice. Please include the appropriate amount with your remittance.

Contact the chapter in your area or the International Office for information on chapter dues if the amount is not listed below. Additional chapter information may be found at www.isaca.org/chap1.htm

ASIA

Chapter Name	Chapter Number	Dues
Hong Kong	64	$35
Bangalore, India	138	$15
Calcutta	165	✻
Coimbatore, India	155	✻
Delhi, India	140	$10
Hyderabad, India	164	$17
Madras, India (Chennai)	99	$5
Mumbai, India	145	$20
Pune, India	159	$17
Indonesia	123	✻
Nagoya, Japan	118	✻
Osaka, Japan	103	✻
Tokyo, Japan	89	$180
Korea	107	$30
Malaysia	93	$10
Muscat, Oman	167	✻
Karachi, Pakistan	148	$12.50
Manila, Philippines	136	$25
Jeddah, Saudi Arabia	163	$0
Riyadh, Saudi Arabia	154	$0
Singapore	70	$10
Sri Lanka	141	$15
Taiwan	142	$35
Bangkok, Thailand	109	$9
UAE	150	$10

CENTRAL/SOUTH AMERICA

Chapter Name	Chapter Number	Dues
Buenos Aires, Argentina	124	$150
Mendoza, Argentina	144	$120
São Paulo, Brazil	166	$25
Santiago de Chile	135	$40
Bogota, Colombia	126	$50
San Jose, Costa Rica	31	$33
Merida, Yucatan, Mexico	101	$50
Mexico City, Mexico	14	$65
Monterrey, Mexico	80	$0
Panama	94	$20
Lima, Peru	146	$0
Puerto Rico	86	$30
Montevideo, Uruguay	133	✻
Venezuela	113	✻

EUROPE/AFRICA

Chapter Name	Chapter Number	Dues
Austria	157	$50
Belux (Belgium and Luxembourg)	143	$40
Czech Republic	153	$110
Denmark	96	✻
Estonian	162	$10
Finland	115	$70
Paris, France	75	✻
German	104	$80
Athens, Greece	134	$10
Budapest, Hungary	125	$50
Irish	156	$35
Tel-Aviv, Israel	40	✻
Milano, Italy	43	$72
Kenya	158	$40
Latvia	139	$10
Netherlands	97	$30
Lagos, Nigeria	149	$20
Oslo, Norway	74	$40
Warsaw, Poland	151	$0
Slovenia	137	$50
Slovensko	160	$40
South Africa	130	$50
Madrid, Spain	112	✻
Sweden	88	$45
Switzerland	116	$35
London, UK	60	$88
Central UK	132	$35
Northern UK	111	$50

NORTH AMERICA

Canada

Chapter Name	Chapter Number	Dues
Calgary, AB	121	$0
Edmonton, AB	131	$25
Vancouver, BC	25	$15
Victoria, BC	100	$0
Winnipeg, MB	72	$15
Nova Scotia	105	$0
Ottawa Valley, ON	32	$10
Toronto, ON	21	$25
Montreal, PQ	36	$15
Quebec City, PQ	91	$35

Islands

Chapter Name	Chapter Number	Dues
Bermuda	147	$0
Trinidad & Tobago	106	$25

Midwestern United States

Chapter Name	Chapter Number	Dues
Chicago, IL	02	$50
Illini (Springfield, IL)	77	$30
Central Indiana (Indianapolis)	56	$25
Michiana (South Bend, IN)	127	$25
Iowa (Des Moines)	110	$25
Kentuckiana (Louisville, KY)	37	$30
Detroit, MI	08	$35
Western Michigan (Grand Rapids)	38	$25
Minnesota (Minneapolis)	07	$30
Omaha, NE	23	$30
Central Ohio (Columbus)	27	$25
Greater Cincinnati, OH	03	$20
Northeast Ohio (Cleveland)	26	$30
Kettle Moraine, WI (Milwaukee)	57	$25

Northeastern United States

Chapter Name	Chapter Number	Dues
Greater Hartford, CT (Southern New England)	28	$35
Central Maryland (Baltimore)	24	$25
New England (Boston, MA)	18	$30
New Jersey (Newark)	30	$40
Central New York (Syracuse)	29	$30
Hudson Valley, NY (Albany)	120	$0
New York Metropolitan	10	$50
Western New York (Buffalo)	46	$30
Harrisburg, PA	45	$30
Lehigh Valley (Allentown, PA)	122	$35
Philadelphia, PA	06	$40
Pittsburgh, PA	13	$20
National Capital Area, DC	05	$30

Southeastern United States

Chapter Name	Chapter Number	Dues
North Alabama (Birmingham)	65	$30
Jacksonville, FL	58	$30
Central Florida (Orlando)	67	$30
South Florida (Miami)	33	$40
West Florida (Tampa)	41	$35
Atlanta, GA	39	$30
Charlotte, NC	51	$35
Research Triangle (Raleigh, NC)	59	$25
Piedmont/Triad (Winston-Salem, NC)	128	$30
Greenville, SC	54	$30
Memphis, TN	48	$45
Middle Tennessee (Nashville)	102	$45
Virginia (Richmond)	22	$30

Southwestern United States

Chapter Name	Chapter Number	Dues
Central Arkansas (Little Rock)	82	$60
Central Mississippi (Jackson)	161	$25
Denver, CO	16	$35
Greater Kansas City, KS	87	$25
Baton Rouge, LA	85	$25
Greater New Orleans, LA	61	$20
St. Louis, MO	11	$25
New Mexico (Albuquerque)	83	$25
Central Oklahoma (OK City)	49	$30
Tulsa, OK	34	$25
Austin, TX	20	$25
Greater Houston Area, TX	09	$40
North Texas (Dallas)	12	$30
San Antonio/So. Texas	81	$25

Western United States

Chapter Name	Chapter Number	Dues
Phoenix, AZ	53	$30
Los Angeles, CA	01	$25
Orange County, CA (Anaheim)	79	$30
Sacramento, CA	76	$20
San Francisco, CA	15	$45
San Diego, CA	19	$30
Silicon Valley, CA (Sunnyvale)	62	$25
Hawaii (Honolulu)	71	$30
Boise, ID	42	$30
Willamette Valley, OR (Portland)	50	$30
Utah (Salt Lake City)	04	$30
Mt. Rainier, WA (Olympia)	129	$20
Puget Sound, WA (Seattle)	35	$35

✻Call Chapter for information

OCEANIA

Chapter Name	Chapter Number	Dues
Adelaide, Australia	68	$0
Brisbane, Australia	44	$16
Canberra, Australia	92	$30
Melbourne, Australia	47	$30
Perth, Australia	63	$5
Sydney, Australia	17	$30
Auckland, New Zealand	84	$24
Wellington, New Zealand	73	$22
Papua New Guinea	152	$0

To receive your copy of the *Information Systems Control Journal*, please complete the following subscriber information:

Size of Organization (at your primary place of business):
① ☐ Fewer than 50 employees
② ☐ 50-100 employess
③ ☐ 101-500 employees
④ ☐ More than 500 employees

What is the size of your professional audit staff? *(local office)*
① ☐ 1 individual
② ☐ 2-5 individuals
③ ☐ 6-10 individuals
④ ☐ 11-25 individuals
⑤ ☐ More than 25 individuals

Your level of purchasing authority:
① ☐ Recommend Products/Services
② ☐ Approve Purchase
③ ☐ Recommend and Approve Purchase

Education courses attended annually *(check one)*
① ☐ None
② ☐ 1
③ ☐ 2-3
④ ☐ 4-5
⑤ ☐ More than 5

Conferences attended annually *(check one)*
① ☐ None
② ☐ 1
③ ☐ 2-3
④ ☐ 4-5
⑤ ☐ More than 5

Primary reason for Joining the Association *(check one)*
① ☐ Discounts on Association products and services
② ☐ Subscription to *IS Control Journal*
③ ☐ Professional Advancement/ Certification
④ ☐ Access to Research, Publications, and Education
⑨⑨ ☐ Other_____

Information Systems Audit and Control Association®

proud sponsor of the

CISA®

CERTIFIED INFORMATION SYSTEMS AUDITOR

What does the Certified Information Systems Auditor credential mean to you?

As an Employer

By hiring or retaining the services of a CISA, an organization has invested in a professional who has:

- Distinguished himself/herself from other industry professionals
- Followed a learning path to demonstrate IT assurance knowledge and skill
- Committed to maintaining skills through future professional development

For more than twenty years organizations have turned to professionals who have earned a CISA designation. CISAs have the proven ability to perform reviews in accordance with generally accepted standards and guidelines to ensure that the organization's information technology and business systems are adequately controlled, monitored and assessed.

As an IT Professional

Earning the CISA designation helps assure a positive reputation as a qualified IS audit, control and/or security professional, and because the CISA program certifies individuals who demonstrate proficiency in today's most sought-after skills, employers prefer to hire and retain those who achieve and maintain their designation.

Although certification may not be mandatory for you at this time, a growing number of organizations are recommending employees to become certified. To help ensure your success in the global marketplace, it is vital that you select a certification program based on universally accepted technical practices. CISA delivers such a program. CISA is recognized worldwide, by all industries, as the preferred designation for IS audit, control and security professionals.

Requirements for CISA certification

See www.isaca.org/cert1.htm for specific details.

1. Successful completion of the CISA exam. The exam is offered annually at nearly 200 sites around the world in ten languages during the month of June.
2. Satisfy the work experience requirement pertaining to professional information systems (IS) auditing, control or security activity. Education waivers are available. See the CISA Bulletin of Information for details (*www.isaca.org/exam1.htm*).
3. Adhere to the Information Systems Audit and Control Association's *Code of Professional Ethics* (*www.isaca.org/standard/code2.htm*)
4. Comply with annual continuing education requirements (www.isaca.org/cisacep1.htm)

Although CobiT is not specifically tested on the CISA examination, the CobiT control objectives or processes do reflect the tasks identified in the CISA Practice Analysis. As such, a thorough review of CobiT is recommended for candidate preparation for the CISA examination.

For further information, please contact the Certification Department at *certification@isaca.org* or by phone at +1.847.253.1545 ext. 474 or 471.

GOVERNANCE INSTITUTE™

COBIT®

3rd Edition

Implementation Tool Set

July 2000

Released by the COBIT Steering Committee and the IT Governance Institute™

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 and auditors.

American Samoa
Argentina
Armenia
Australia
Austria
Bahamas
Bahrain
Bangladesh
Barbados
Belgium
Bermuda
Bolivia
Botswana
Brazil
British Virgin Islands
Canada
Cayman Islands
Chile
China
Colombia
Costa Rica
Croatia
Curacao
Cyprus
Czech Republic
Denmark
Dominican Republic
Ecuador
Egypt
El Salvador
Estonia
Faeroe Islands
Fiji
Finland
France
Germany
Ghana
Greece
Guam
Guatemala
Honduras
Hong Kong
Hungary
Iceland
India
Indonesia
Iran
Ireland
Israel
Italy
Ivory Coast
Jamaica
Japan
Jordan
Kazakhstan
Kenya
Korea
Kuwait

Information Systems Audit and Control Association

A Single International Source for Information Technology Controls

The Information Systems Audit and Control Association is a leading global professional organisation representing individuals in more than 100 countries and comprising all levels of IT — executive, management, middle management and practitioner. The Association is uniquely positioned to fulfil the role of a central, harmonising source of IT control practice standards for the world over. Its strategic alliances with other groups in the financial, accounting, auditing and IT professions are ensuring an unparalleled level of integration and commitment by business process owners.

Association Programmes and Services

The Association's services and programmes have earned distinction by establishing the highest levels of excellence in certification, standards, professional education and technical publishing.

- *Its certification programme (the Certified Information Systems Auditor™) is the only global designation throughout the IT audit and control community.*
- *Its standards activities establish the quality baseline by which other IT audit and control activities are measured.*
- *Its professional education programme offers technical and management conferences on five continents, as well as seminars worldwide to help professionals everywhere receive high-quality continuing education.*
- *Its technical publishing area provides references and professional development materials to augment its distinguished selection of programmes and services.*

The Information Systems Audit and Control Association was formed in 1969 to meet the unique, diverse and high technology needs of the burgeoning IT field. In an industry in which progress is measured in nano-seconds, ISACA has moved with agility and speed to bridge the needs of the international business community and the IT controls profession.

For More Information

To receive additional information, you may telephone (+1.847.253.1545), send an e-mail (research@isaca.org) or visit these web sites:

www.ITgovernance.org

www.isaca.org

Latvia
Lebanon
Liechtenstein
Lithuania
Luxemburg
Malaysia
Malta
Malawi
Mauritius
Mexico
Namibia
Nepal
Netherlands
New Guinea
New Zealand
Nicaragua
Nigeria
Norway
Oman
Pakistan
Panama
Paraguay
Peru
Philippines
Poland
Portugal
Qatar
Russia
Saudi Arabia
Scotland
Seychelles
Singapore
Slovak Republic
Slovenia
South Africa
Spain
Sri Lanka
St. Kitts
St. Lucia
Sweden
Switzerland
Taiwan
Tanzania
Tasmania
Thailand
Trinidad & Tobago
Tunisia
Turkey
Uganda
United Arab Emirates
United Kingdom
United States
Uruguay
Venezuela
Vietnam
Wales
Yugoslavia
Zambia
Zimbabwe

TABLE OF CONTENTS

Acknowledgments 4

Executive Overview 6-8

The COBIT Framework 9-13

The Framework's Principles 14-18

COBIT History and Background 19-20

Control Objectives—Summary Table 21

Guide for Implementation

How to Introduce COBIT in Your Organisation 23-29
How to Implement COBIT in Your Organisation 30-48
Management Awareness Diagnostics 49-52
IT Control Diagnostics 53-59

COBIT Case Studies 61-68

COBIT Frequently Asked Questions 69-75

Appendix I

IT Governance Management Guideline 79-82

Appendix II

COBIT Project Description 83

Appendix III

COBIT Primary Reference Material 84-85

Appendix IV

Glossary of Terms 86

Disclaimer
The Information Systems Audit and Control Foundation, IT Governance Institute and the sponsors of *COBIT: Control Objectives for Information and related Technology* have designed and created the publications entitled *Executive Summary, Framework, Control Objectives, Management Guidelines, Audit Guidelines* and *Implementation Tool Set* (collectively, the "Works") primarily as an educational resource for controls professionals. The Information Systems Audit and Control Foundation, IT Governance Institute and the sponsors make no claim that use of any of the Works will assure a successful outcome. The Works should not be considered inclusive 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, the controls professional should apply his or her own professional judgment to the specific control circumstances presented by the particular systems or IT environment.

Disclosure and Copyright Notice
Copyright © 1996, 1998, 2000 by the Information Systems Audit and Control Foundation (ISACF). Reproduction for commercial purpose is not permitted without ISACF's prior written permission. Permission is hereby granted to use and copy the *Executive Summary, Framework, Control Objectives, Management Guidelines* and *Implementation Tool Set* for non-commercial, internal use, including storage in a retrieval system and transmission by any means including, electronic, mechanical, recording or otherwise. All copies of the *Executive Summary, Framework, Control Objectives, Management Guidelines* and *Implementation Tool Set* must include the following copyright notice and acknowledgment: "Copyright 1996, 1998, 2000 Information Systems Audit and Control Foundation. Reprinted with the permission of the Information Systems Audit and Control Foundation and IT Governance Institute."

The *Audit Guidelines* may not be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), except with ISACF's prior written authorization; provided, however, that the *Audit Guidelines* may be used for internal non-commercial purposes only. Except as stated herein, no other right or permission is granted with respect to this work. All rights in this work are reserved.

Information Systems Audit and Control Foundation
IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *research@isaca.org*
Web sites: *www.ITgovernance.org*
www.isaca.org

ISBN 0-893209-16-14 (*Implementation Tool Set*)
ISBN 1-893209-13-X (Complete 6 book set with CD-ROM)

Printed in the United States of America.

Acknowledgments

Project Team

Erik Guldentops, S.W.I.F.T. sc, Belgium
Eddy Schuermans, PricewaterhouseCoopers, Belgium

Project Steering Committee

Erik Guldentops, S.W.I.F.T. sc, Belgium
John Beveridge, State Auditor's Office, Massachusetts, USA
Prof. Dr. Bart De Schutter, Vrije Universiteit Brussels, Chairman BRT Belgium
Gary Hardy, Arthur Andersen, United Kingdom
John Lainhart, PricewaterhouseCoopers, USA
Akira Matsuo, Chuo Audit Corporation, Japan
Eddy Schuermans, PricewaterhouseCoopers, Belgium
Paul Williams, Arthur Andersen, United Kingdom

Researcher

Prof. Ulric J. Gelinas, Jr.,
Bentley College, Watham, MA

Expert Review

ISACA Boston Chapter
ISACA National Capital Area Chapter

Special thanks to the members of the Board of the Information Systems Audit and Control Association and Trustees of the Information Systems Audit and Control Foundation, headed by International President Paul Williams, for their continuing and unwavering support of CobiT.

INTRODUCTION TO IMPLEMENTATION TOOL SET

The landmark introduction of *Control Objectives for Information and related Technology* (CobiT) in 1996 gave information technologists a framework of generally applicable and accepted Information Technology (IT) governance and control practices.

The primary purpose of CobiT is to provide clear policy and good practice for IT governance throughout organisations worldwide — to help senior management understand and manage the risks associated with IT. CobiT accomplishes this by providing an IT governance framework and detailed control objective guides for management, business process owners, users, and auditors.

CobiT starts with a simple and pragmatic premise: to provide the information needed to achieve its objectives, an organisation should manage its IT resources through a set of naturally grouped processes. CobiT groups processes in a simple, business-oriented hierarchy. Each process references IT resources, and quality, fiduciary, and security requirements for information.

Because CobiT is business oriented, using it to understand IT control objectives in order to manage IT related business risks is straightforward:

- start with your business objectives in the *Framework*,
- select the IT processes and controls appropriate to your enterprise from the *Control Objectives*,
- operate from your business plan,
- assess your procedures and results with the *Audit Guidelines*, and
- assess the status of your organization, identify critical activities leading to success and measure performance in reaching enterprise goals with the *Management Guidelines*.

Immediately after CobiT was released, the CobiT Steering Committee started evaluating how the 'global best practices' were being implemented. This *Implementation Tool Set* is the result of their findings. It takes the lessons learned from those organisations that quickly and successfully applied CobiT and places them in a Tool Set for others to use. The newly developed *Management Guidelines* introduce new concepts and tools that will open new perspectives and options for introducing CobiT to the enterprise and their use will evolve, as they are adapted to the specific needs of each organisation.

Those lessons included advice to: involve senior management, early on, in discussions; be prepared to explain the framework (both at an overview level and at a detailed level); and cite success stories from other organisations. The CobiT Steering Committee was also asked to improve their explanations of key points and give a step-by-step overview, with examples, of an ideal implementation process. Thus, this *Implementation Tool Set* contains:

- Executive Overview
- Guide to Implementation, including sample memos and presentations
- Management Awareness Diagnostics and IT Control Diagnostics
- Case Studies describing CobiT implementation
- Frequently Asked Questions and Answers
- Slide presentations for implementing/selling CobiT

EXECUTIVE OVERVIEW

Critically important to the survival and success of an organisation is effective management of information and related Information Technology (IT). In this global information society—where information travels through cyberspace without the constraints of time, distance and speed—this criticality arises from the:

- Increasing dependence on information and the systems that deliver this information
- Increasing vulnerabilities and a wide spectrum of threats, such as cyber threats and information warfare
- Scale and cost of the current and future investments in information and information systems
- Potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs

For many organisations, information and the technology that supports it represent the organisation's most valuable assets. Moreover, in today's very competitive and rapidly changing business environment, management has heightened expectations regarding IT delivery functions: management requires increased quality, functionality and ease of use; decreased delivery time; and continuously improving service levels—while demanding that this be accomplished at lower costs.

Many organisations recognise the potential benefits that technology can yield. Successful organisations, however, understand and manage the risks associated with implementing new technologies.

There are numerous changes in IT and its operating environment that emphasise the need to better manage IT-related risks. Dependence on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. This, in turn, is driven by increasing disclosures of information system disasters and increasing electronic fraud. The management of IT-related risks is now being understood as a key part of enterprise governance.

Within enterprise governance, IT governance is becoming more and more prominent, and is defined as 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. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. Furthermore, IT governance integrates and institutionalises good (or best) practices of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance to ensure that the enterprise's information and related technology support its business objectives. IT governance thus enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

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.

Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must understand the status of its own IT systems and decide what security and control they should provide.

Control Objectives for Information and related Technology (COBIT), now in its 3rd edition, helps 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" means consensus of the experts—they will help optimise information investments and will provide a measure to be judged against when things do go wrong.

Management must ensure that an internal control system or framework is in place which supports the business processes, makes it clear how each individual control activity satisfies the information requirements and impacts the IT resources. Impact on IT resources is highlighted in the COBIT *Framework* together with the business requirements for effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of information that need to be satisfied. Control, which includes policies, organisational structures, practices and procedures, is management's responsibility. Management, through its enterprise governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance or operation of information systems. An IT control objective is a statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity.

Implementation Tool Set

Business orientation is the main theme of CobiT. It is designed to be employed not only by users and auditors, but also, and more importantly, as comprehensive guidance for management and business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls.

The CobiT *Framework* provides a tool for the business process owner that facilitates the discharge of this responsibility. The *Framework* starts from a simple and pragmatic premise:

In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

The *Framework* continues with a set of 34 high-level *Control Objectives*, one for each of the IT processes, grouped into four domains: planning and organisation, 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.

IT governance guidance is also provided in the CobiT *Framework*. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

In addition, corresponding to each of the 34 high-level control objectives is an *Audit Guideline* to enable the review of IT processes against CobiT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement.

The *Management Guidelines*, CobiT's most recent development, further enhances and enables enterprise management to deal more effectively with the needs and requirements of IT governance. The guidelines are action oriented and generic and provide management direction for getting the enterprise's information and related processes under control, for monitoring achievement of organisational goals, for monitoring performance within each IT process and for benchmarking organisational achievement.

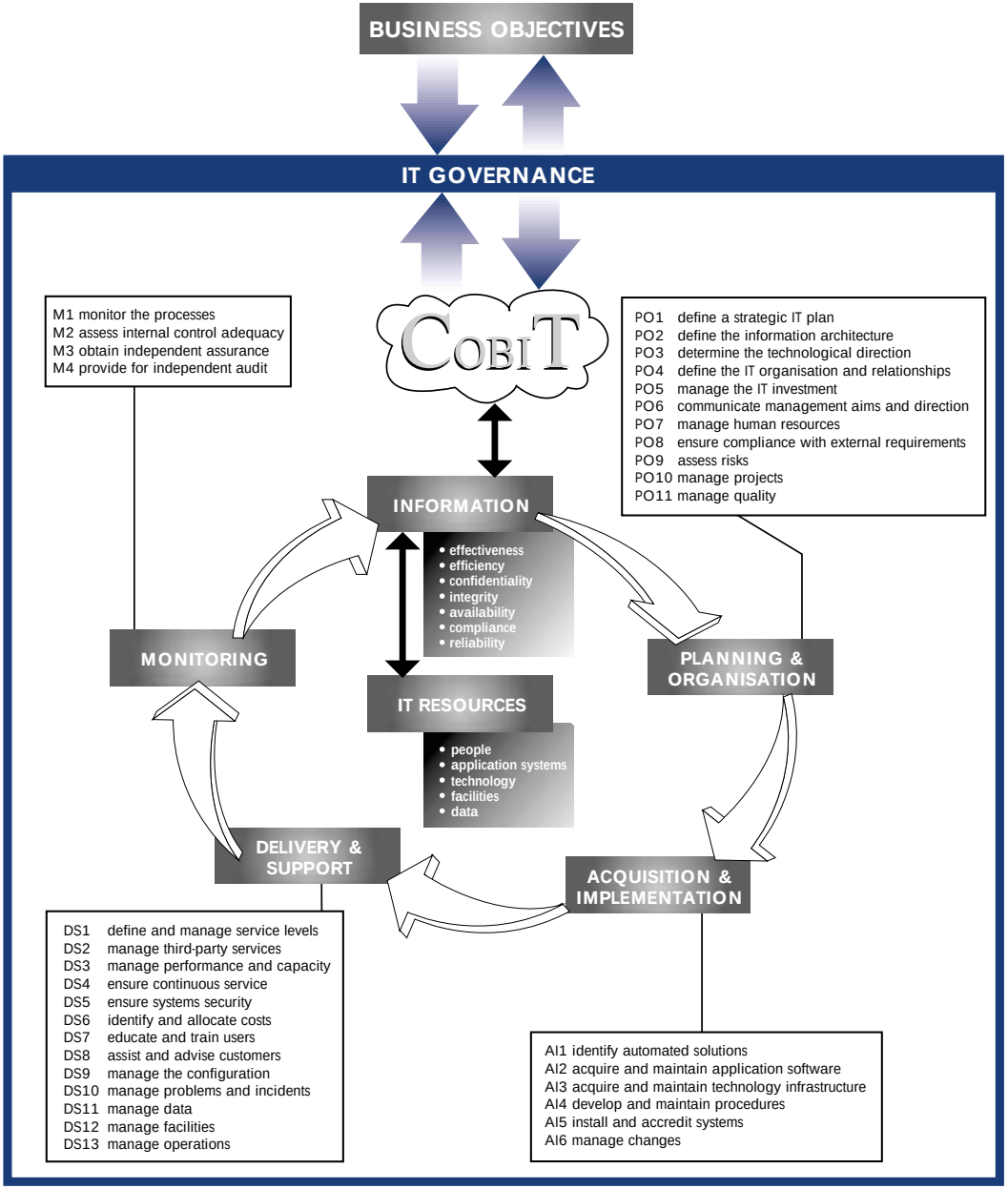
Specifically, CobiT provides **Maturity Models** for control over IT processes, so that management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be; **Critical Success Factors**, which define the most important management-oriented implementation guidelines to achieve control over and within its IT processes; **Key Goal Indicators**, which define measures that tell management—after the fact—whether an IT process has achieved its business requirements; and **Key Performance Indicators**, which are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

CobiT's *Management Guidelines* are generic and action oriented for the purpose of answering the following types of management questions: How far should we go, and is the cost justified by the benefit? What are the indicators of good performance? 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?

CobiT also contains an *Implementation Tool Set* that provides lessons learned from those organisations that quickly and successfully applied CobiT in their work environments. It has two particularly useful tools—Management Awareness Diagnostic and IT Control Diagnostic—to assist in analysing an organisation's IT control environment.

Over the next few years, the management of organisations will need to demonstrably attain increased levels of security and control. CobiT is a tool that allows managers to bridge the gap with respect to control requirements, technical issues and business risks and communicate that level of control to stakeholders. CobiT enables the development of clear policy and good practice for IT control throughout 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.**

COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS



THE COBIT FRAMEWORK

THE NEED FOR CONTROL IN INFORMATION TECHNOLOGY

In recent years, it has become increasingly evident that there is a need for a reference framework for security and control in IT. Successful organisations require an appreciation for and a basic understanding of the risks and constraints of IT at all levels within the enterprise in order to achieve effective direction and adequate controls.

MANAGEMENT has to decide what to reasonably invest for security and control in IT and how to balance risk and control investment in an often unpredictable IT environment. While information systems security and control help manage risks, they do not eliminate them. In addition, the exact level of risk can never be known since there is always some degree of uncertainty. Ultimately, management must decide on the level of risk it is willing to accept. Judging what level can be tolerated, particularly when weighted against the cost, can be a difficult management decision. Therefore, management clearly needs a framework of generally accepted IT security and control practices to benchmark the existing and planned IT environment.

There is an increasing need for **USERS** of IT services to be assured, through accreditation and audit of IT services provided by internal or third parties, that adequate security and control exists. At present, however, the implementation of good IT controls in information systems, be they commercial, non-profit or governmental, is hampered by confusion. The confusion arises from the different evaluation methods such as ITSEC, TCSEC, IS0 9000 evaluations, emerging COSO internal control evaluations, etc. As a result, users need a general foundation to be established as a first step.

Frequently, **AUDITORS** have taken the lead in such international standardisation efforts because they are continuously confronted with the need to substantiate their opinion on internal control to management. Without a framework, this is an exceedingly difficult task. Furthermore, auditors are increasingly being called on by management to proactively consult and advise on IT security and control-related matters.

THE BUSINESS ENVIRONMENT: COMPETITION, CHANGE AND COST

Global competition is here. Organisations are restructuring to streamline operations and simultaneously take advantage of the advances in IT to improve their competitive position. Business re-engineering, right-sizing, outsourcing, empowerment, flattened organisations and distributed processing are all changes that impact the way that business and governmental organisations operate. These changes are having, and will continue to have, profound implications for the management and operational control structures within organisations worldwide.

Emphasis on attaining competitive advantage and cost-efficiency implies an ever-increasing reliance on technology as a major component in the strategy of most organisations. Automating organisational functions is, by its very nature, dictating the incorporation of more powerful control mechanisms into computers and networks, both hardware-based and software-based. Furthermore, the fundamental structural characteristics of these controls are evolving at the same rate and in the same “leap frog” manner as the underlying computing and networking technologies are evolving.

Within the framework of accelerated change, if managers, information systems specialists and auditors are indeed going to be able to effectively fulfil their roles, their skills must evolve as rapidly as the technology and the environment. One must understand the technology of controls involved and its changing nature if one is to exercise reasonable and prudent judgments in evaluating control practices found in typical business or governmental organisations.

EMERGENCE OF ENTERPRISE AND IT GOVERNANCE

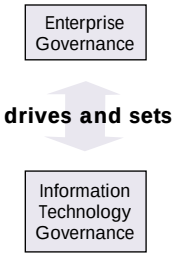
To achieve success in this information economy, enterprise governance and IT governance can no longer be considered separate and distinct disciplines. Effective enterprise governance focuses individual and group expertise and experience where it can be most productive, monitors and measures performance and provides assurance to critical issues. IT, long considered solely an

THE COBIT FRAMEWORK, *continued*

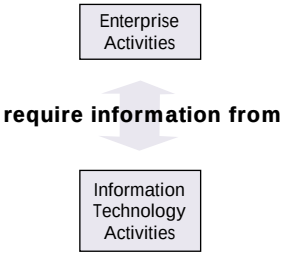
enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy.

IT governance provides the structure that links IT processes, IT resources, and information to enterprise strategies and objectives. IT governance integrates and institutionalises optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

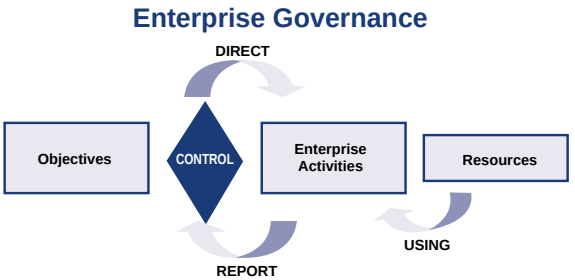
Looking at the interplay of enterprise and IT governance processes in more detail, enterprise governance, the system by which entities are directed and controlled, drives and sets IT governance. At the same time, IT should provide critical input to, and constitute an important component of, strategic plans. IT may in fact influence strategic opportunities outlined by the enterprise.



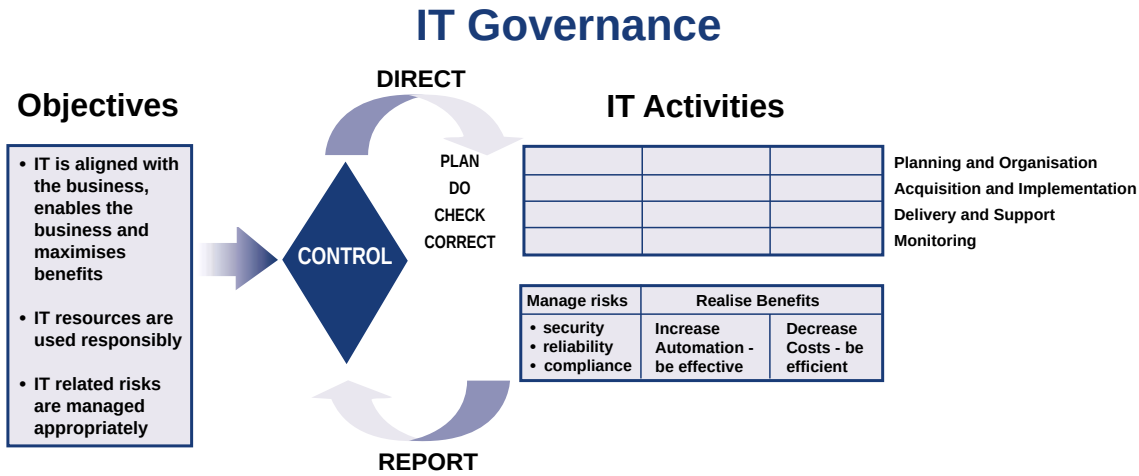
Enterprise activities require information from IT activities in order to meet business objectives. Successful organisations ensure interdependence between their strategic planning and their IT activities. IT must be aligned with and enable the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining a competitive advantage.



Enterprises are governed by generally accepted good (or best) practices, to ensure that the enterprise is achieving its goals-the assurance of which is guaranteed by certain controls. From these objectives flows the organisation's direction, which dictates certain enterprise activities, using the enterprise's resources. The results of the enterprise activities are measured and reported on, providing input to the constant revision and maintenance of the controls, beginning the cycle again.



IT also is governed by good (or best) practices, to ensure that the enterprise's information and related technology support its business objectives, its resources are used responsibly and its risks are managed appropriately. These practices form a basis for direction of IT activities, which can be characterised as planning and organising, acquiring and implementing, delivering and supporting, and monitoring, for the dual purposes of managing risks (to gain security, reliability and compliance) and realising benefits (increasing effectiveness and efficiency). Reports are issued on the outcomes of IT activities, which are measured against the various practices and controls, and the cycle begins again.



In order to ensure that management reaches its business objectives, it must direct and manage IT activities to reach an effective balance between managing risks and realising benefits. To accomplish this, management needs to identify the most important activities to be performed, measure progress towards achieving goals and determine how well the IT processes are performing. In addition, it needs the ability to evaluate the organisation's maturity level against industry best practices and international standards. **To support these management needs, the COBIT *Management Guidelines* have identified specific Critical Success Factors, Key Goal Indicators, Key Performance Indicators and an associated Maturity Model for IT governance, as presented in Appendix I.**

The CobiT Framework, *continued*

RESPONSE TO THE NEED

In view of these ongoing changes, the development of this framework for control objectives for IT, along with continued applied research in IT controls based on this framework, are cornerstones for effective progress in the field of information and related technology controls.

On the one hand, we have witnessed the development and publication of overall business control models like COSO (Committee of Sponsoring Organisations of the Treadway Commission-Internal Control—*Integrated Framework*, 1992) in the US, Cadbury in the UK, CoCo in Canada and King in South Africa. On the other hand, an important number of more focused control models are in existence at the level of IT. Good examples of the latter category are the Security Code of Conduct from DTI (Department of Trade and Industry, UK), Information Technology Control Guidelines from CICA (Canadian Institute of Chartered Accountants, Canada), and the Security Handbook from NIST (National Institute of Standards and Technology, US). However, these focused control models do not provide a comprehensive and usable control model over IT in support of business processes. The purpose of CobiT is to bridge this gap by providing a foundation that is closely linked to business objectives while focusing on IT.

(Most closely related to CobiT is the recently published *AICPA/CICA SysTrust™ Principles and Criteria for Systems Reliability*. SysTrust is an authoritative issuance of both the Assurance Services Executive Committee in the United States and the Assurance Services Development Board in Canada, based in part on the CobiT *Control Objectives*. SysTrust is designed to increase the comfort of management, customers and business partners with the systems that support a business or a particular activity. The SysTrust service entails the public accountant providing an assurance service in which he or she evaluates and tests whether a system is reliable when measured against four essential principles: availability, security, integrity and maintainability.)

A focus on the business requirements for controls in IT and the application of emerging control models and related international standards evolved the original Information Systems Audit and Control Foundation's *Control Objectives* from an auditor's tool to CobiT, a management tool. Further, the development of IT *Management Guidelines* has taken CobiT to the next level-providing management with Key Goal Indicators (KGIs), Key Performance Indicators (KPIs), Critical Success Factors (CSFs) and Maturity Models so that it can assess its IT environment and make choices for control implementation and control improvements over the organisation's information and related technology.

Hence, the main objective of the CobiT project is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and professional organisations. It is the goal of the project to develop these control objectives primarily from the business objectives and needs perspective. (This is compliant with the COSO perspective, which is first and foremost a management framework for internal controls.) Subsequently, control objectives have been developed from the audit objectives (certification of financial information, certification of internal control measures, efficiency and effectiveness, etc.) perspective.

AUDIENCE: MANAGEMENT, USERS AND AUDITORS

CobiT is designed to be used by three distinct audiences.

MANAGEMENT:
to help them balance risk and control investment in an often unpredictable IT environment.

USERS:
to obtain assurance on the security and controls of IT services provided by internal or third parties.

AUDITORS:
to substantiate their opinions and/or provide advice to management on internal controls.

BUSINESS OBJECTIVES ORIENTATION

COBIT is aimed at addressing business objectives. The control objectives make a clear and distinct link to business objectives in order to support significant use outside the audit community. Control objectives are defined in a process-oriented manner following the principle of business re-engineering. At identified domains and processes, a high-level control objective is identified and rationale provided to document the link to the business objectives. In addition, considerations and guidelines are provided to define and implement the IT control objective.

The classification of domains where high-level control objectives apply (domains and processes), an indication of the business requirements for information in that domain, as well as the IT resources primarily impacted by the control objectives, together form the COBIT *Framework*. The *Framework* is based on the research activities that have identified 34 high-level control objectives and 318 detailed control objectives. The *Framework* was exposed to the IT industry and the audit profession to allow an opportunity for review, challenge and comment. The insights gained have been appropriately incorporated.

GENERAL DEFINITIONS

For the purpose of this project, the following definitions are provided. "Control" is adapted from the COSO Report (*Internal Control—Integrated Framework*, Committee of Sponsoring Organisations of the Treadway Commission, 1992) and "IT Control Objective" is adapted from the SAC Report (*Systems Auditability and Control Report*, The Institute of Internal Auditors Research Foundation, 1991 and 1994).

Control is defined as 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.

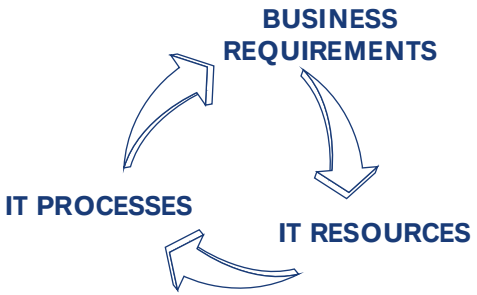
IT Control Objective is defined as a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

IT Governance is defined as 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.

The Framework's Principles

There are two distinct classes of control models currently available: those of the "business control model" class (e.g., COSO) and the "more focused control models for IT" (e.g., DTI). CobiT aims to bridge the gap that exists between the two. CobiT is therefore positioned to be more comprehensive for management and to operate at a higher level than technology standards for information systems management. **Thus, CobiT is the model for IT governance!**

The underpinning concept of the CobiT *Framework* is that control in IT is approached by looking at information that is needed to support the business objectives or requirements, and by looking at information as being the result of the combined application of IT-related resources that need to be managed by IT processes.



To satisfy business objectives, information needs to conform to certain criteria, which CobiT refers to as business requirements for information. In establishing the list of requirements, CobiT combines the principles embedded in existing and known reference models:

Quality Requirements	Quality Cost Delivery
Fiduciary Requirements (COSO Report)	Effectiveness and Efficiency of operations Reliability of Information Compliance with laws and regulations
Security Requirements	Confidentiality Integrity Availability

Quality has been retained primarily for its negative aspect (no faults, reliability, etc.), which is also captured to a large extent by the Integrity criterion. The positive but less tangible aspects of Quality (style, attractiveness, "look and feel," performing beyond expectations, etc.) were, for a time, not being considered from an IT control objectives point of view. The premise is that the first priority should go to properly managing the risks as opposed to the opportunities. The usability aspect of Quality is covered by the Effectiveness criterion. The Delivery aspect of Quality was considered to overlap with the Availability aspect of the Security requirements and also to some extent Effectiveness and Efficiency. Finally, Cost is also considered covered by Efficiency.

For the Fiduciary Requirements, CobiT did not attempt to reinvent the wheel—COSO's definitions for Effectiveness and Efficiency of operations, Reliability of Information and Compliance with laws and regulations were used. However, Reliability of Information was expanded to include all information—not just financial information.

With respect to the Security Requirements, CobiT identified Confidentiality, Integrity, and Availability as the key elements—these same three elements, it was found, are used worldwide in describing IT security requirements.

Starting the analysis from the broader Quality, Fiduciary and Security requirements, seven distinct, certainly overlapping, categories were extracted. CobiT's working definitions are as follows:

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.

Confidentiality concerns the protection of sensitive information from unauthorised disclosure.

Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

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 of Information relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

The IT resources identified in CobiT can be explained/defined as follows:

Data are objects in their widest sense (i.e., external and internal), structured and non-structured, graphics, sound, etc.

Application Systems are understood to be the sum of manual and programmed procedures.

Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.

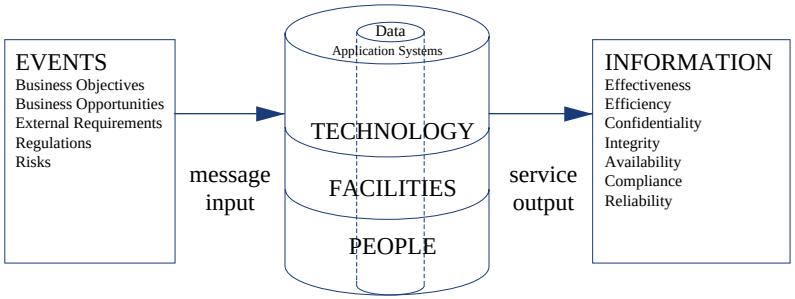
Facilities are all the resources to house and support information systems.

People include staff skills, awareness and productivity to plan, organise, acquire, deliver, support and monitor information systems and services.

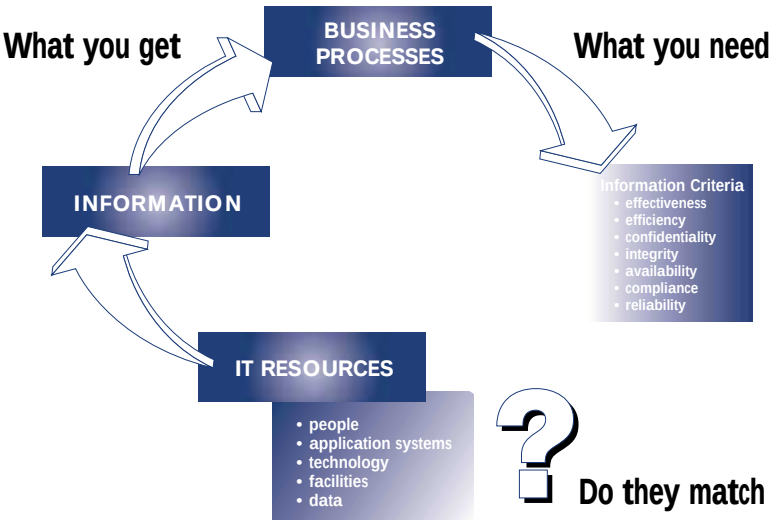
THE FRAMEWORK'S PRINCIPLES, *continued*

Money or capital was not retained as an IT resource for classification of control objectives because it can be considered as being the investment into any of the above resources. It should also be noted that the *Framework* does not specifically refer to documentation of all material matters relating to a particular IT process. As a matter of good practice, documentation is considered essential for good control, and therefore lack of documentation would be cause for further review and analysis for compensating controls in any specific area under review.

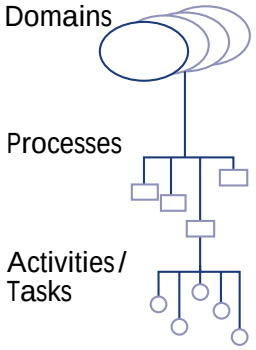
Another way of looking at the relationship of IT resources to the delivery of services is depicted below.



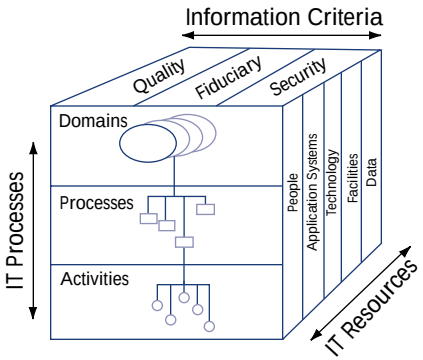
In order to ensure that the business requirements for information are met, adequate control measures need to be defined, implemented and monitored over these resources. How then can organisations satisfy themselves that the information they get exhibits the characteristics they need? This is where a sound framework of IT control objectives is required. The next diagram illustrates this concept.



The COBIT *Framework* consists of high-level control objectives and an overall structure for their classification. The underlying theory for the classification is that there are, in essence, three levels of IT efforts when considering the management of IT resources. Starting at the bottom, there are the activities and tasks needed to achieve a measurable result. Activities have a life-cycle concept while tasks are more discrete. The life-cycle concept has typical control requirements different from discrete activities. Processes are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. At the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organisational structure and is in line with the management cycle or life cycle applicable to IT processes.



Thus, the conceptual framework can be approached from three vantage points: (1) information criteria, (2) IT resources and (3) IT processes. These three vantage points are depicted in the COBIT Cube.



With the preceding as the framework, the domains are identified using wording that management would use in the day-to-day activities of the organisation—not auditor jargon. Thus, four broad domains are identified: planning and organisation, acquisition and implementation, delivery and support, and monitoring.

Definitions for the four domains identified for the high-level classification are:

Planning and Organisation

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place.

Acquisition and Implementation

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

Delivery and Support

This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up.
This domain includes the actual processing of data by application systems, often classified under application controls.

THE FRAMEWORK'S PRINCIPLES, *continued*

Monitoring

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organisation's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

It should be noted that these IT processes can be applied at different levels within an organisation. For example, some of these processes will be applied at the enterprise level, others at the IT function level, others at the business process owner level, etc.

It should also be noted that the Effectiveness criterion of processes that plan or deliver solutions for business requirements will sometimes cover the criteria for Availability, Integrity and Confidentiality—in practice, they have become business requirements. For example, the process of "identify solutions" has to be effective in providing the Availability, Integrity and Confidentiality requirements.

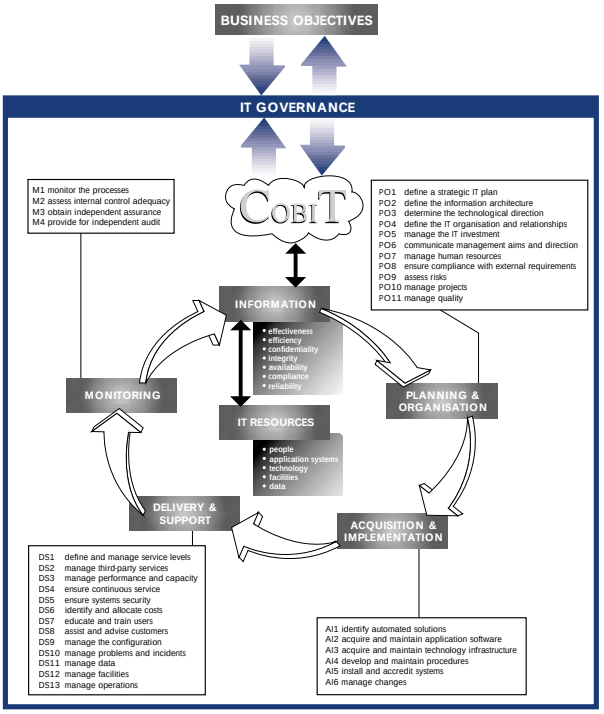
It is clear that all control measures will not necessarily satisfy the different business requirements for information to the same degree.

- **Primary** is the degree to which the defined control objective directly impacts the information criterion concerned.
- **Secondary** is the degree to which the defined control objective satisfies only to a lesser extent or indirectly the information criterion concerned.
- **Blank** could be applicable; however, requirements are more appropriately satisfied by another criterion in this process and/or by another process.

Similarly, all control measures will not necessarily impact the different IT resources to the same degree. Therefore, the COBIT *Framework* specifically indicates the applicability of the IT resources that are specifically managed by the process under consideration (not those that merely take part in the process). This classification is made within the COBIT *Framework* based on a rigorous process of input from researchers, experts and reviewers, using the strict definitions previously indicated.

In summary, in order to provide the information that the organisation needs to achieve its objectives, IT governance must be exercised by the organisation to ensure that IT resources are managed by a set of naturally grouped IT processes. The following diagram illustrates this concept.

COBIT IT PROCESSES DEFINED WITHIN THE FOUR DOMAINS



COBIT HISTORY AND BACKGROUND

COBIT 3rd Edition is the most recent version of Control Objectives for Information and related Technology, first released by the Information Systems Audit and Control Foundation (ISACF) in 1996. The 2nd edition, reflecting an increase in the number of source documents, a revision in the high-level and detailed control objectives and the addition of the *Implementation Tool Set*, was published in 1998. The 3rd edition marks the entry of a new primary publisher for COBIT: the IT Governance Institute.

The IT Governance Institute was formed by the Information System Audit and Control Association (ISACA) and its related Foundation in 1998 in order to advance the understanding and adoption of IT governance principles. Due to the addition of the Management Guidelines to COBIT 3rd Edition and its expanded and enhanced focus on IT governance, the IT Governance Institute took a leading role in the publication's development.

COBIT was originally based on ISACF's *Control Objectives*, and has been enhanced with existing and emerging international technical, professional, regulatory and industry-specific standards. The resulting control objectives have been developed for application to organisation-wide information systems. The term "generally applicable and accepted" is explicitly used in the same sense as Generally Accepted Accounting Principles (GAAP).

COBIT is relatively small in size and attempts to be both pragmatic and responsive to business needs while being independent of the technical IT platforms adopted in an organisation.

While not excluding any other accepted standard in the information systems control field that may have come to light during the research, sources identified are:

Technical standards from ISO, EDIFACT, etc.
Codes of Conduct issued by the Council of Europe, OECD, ISACA, etc.
Qualification criteria for IT systems and processes: ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria, etc.
Professional standards for internal control and auditing: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, etc.
Industry practices and requirements from industry forums (ESF, I4) and government-sponsored platforms (IBAG, NIST, DTI), etc., and
Emerging industry-specific requirements from banking, electronic commerce, and IT manufacturing.

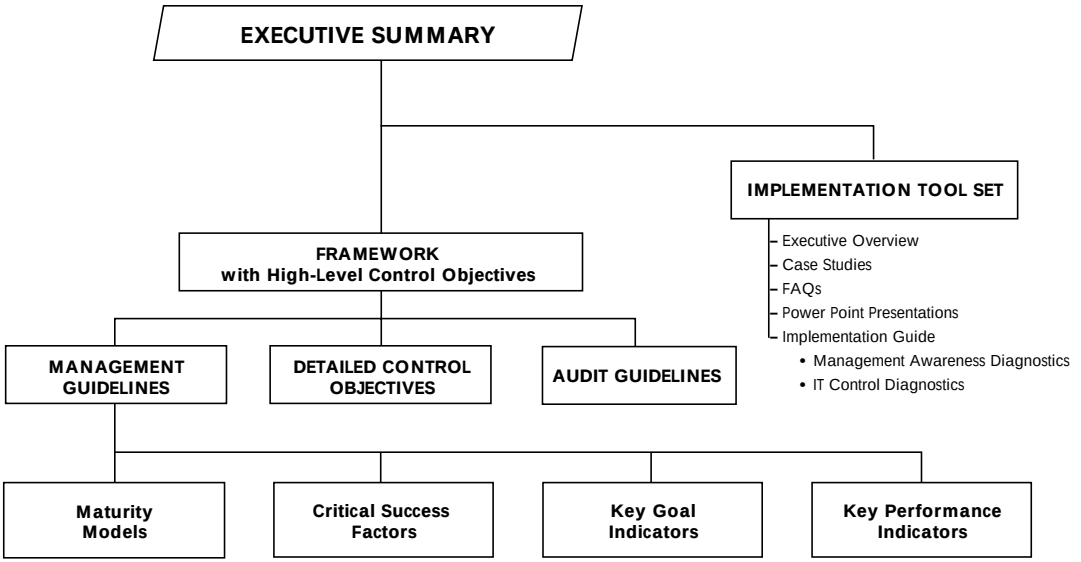
Refer to Appendix II, COBIT Project Description; Appendix III, COBIT Primary Reference Material; and Appendix IV, Glossary of Terms.

COBIT PRODUCT EVOLUTION

COBIT will evolve over the years and be the foundation for further research. Thus, a family of COBIT products will be created and, as this occurs, the IT tasks and activities that serve as the structure to organise control objectives will be further refined, and the balance between domains and processes reviewed in light of the industry's changing landscape.

Research and publication have been made possible by significant grants from PricewaterhouseCoopers and donations from ISACA chapters and members worldwide. The European Security Forum (ESF) kindly made research material available to the project. The Gartner Group also participated in the development and provided quality assurance review of the *Management Guidelines*.

COBIT Family of Products



CONTROL OBJECTIVES
SUMMARY TABLE

The following chart provides an indication, by IT process and domain, of which information criteria are impacted by the high-level control objectives, as well as an indication of which IT resources are applicable.

DOMAIN		PROCESS	Information Criteria: effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	IT Resources: people	applications	technology	facilities	data
Planning & Organisation	PO1	Define a strategic IT plan	P	S						✔	✔	✔	✔	✔
	PO2	Define the information architecture	P	S	S	S					✔			✔
	PO3	Determine technological direction	P	S								✔	✔	
	PO4	Define the IT organisation and relationships	P	S						✔				
	PO5	Manage the IT investment	P	P					S	✔	✔	✔	✔	
	PO6	Communicate management aims and direction	P					S		✔				
	PO7	Manage human resources	P	P						✔				
	PO8	Ensure compliance with external requirements	P					P	S	✔	✔			✔
	PO9	Assess risks	P	S	P	P	P	S	S	✔	✔	✔	✔	✔
	PO10	Manage projects	P	P						✔	✔	✔	✔	
	PO11	Manage quality	P	P		P			S	✔	✔	✔	✔	
Acquisition & Implementation	AI1	Identify automated solutions	P	S							✔	✔	✔	
	AI2	Acquire and maintain application software	P	P		S		S	S		✔			
	AI3	Acquire and maintain technology infrastructure	P	P		S						✔		
	AI4	Develop and maintain procedures	P	P		S		S	S	✔	✔	✔	✔	
	AI5	Install and accredit systems	P			S	S			✔	✔	✔	✔	✔
	AI6	Manage changes	P	P		P	P		S	✔	✔	✔	✔	✔
Delivery & Support	DS1	Define and manage service levels	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS2	Manage third-party services	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	DS3	Manage performance and capacity	P	P			S				✔	✔	✔	
	DS4	Ensure continuous service	P	S			P			✔	✔	✔	✔	✔
	DS5	Ensure systems security			P	P	S	S	S	✔	✔	✔	✔	✔
	DS6	Identify and allocate costs		P					P	✔	✔	✔	✔	✔
	DS7	Educate and train users	P	S						✔				
	DS8	Assist and advise customers	P	P						✔	✔			
	DS9	Manage the configuration	P				S		S		✔	✔	✔	
	DS10	Manage problems and incidents	P	P			S			✔	✔	✔	✔	✔
	DS11	Manage data				P			P					✔
	DS12	Manage facilities				P	P						✔	
	DS13	Manage operations	P	P		S	S			✔	✔		✔	✔
Monitoring	M1	Monitor the processes	P	P	S	S	S	S	S	✔	✔	✔	✔	✔
	M2	Assess internal control adequacy	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M3	Obtain independent assurance	P	P	S	S	S	P	S	✔	✔	✔	✔	✔
	M4	Provide for independent audit	P	P	S	S	S	P	S	✔	✔	✔	✔	✔

(**P**) primary (**S**) secondary (✓) applicable to

This page intentionally left blank

HOW TO INTRODUCE COBIT IN YOUR ORGANISATION

INTRODUCTION

COBIT provides generally accepted practices for managing and controlling Information and Information Technology (IT) resources. COBIT was designed for three audiences—management, users, and auditors (or persons performing evaluations or assessments):

- For management — COBIT helps "balance the risks and control investments in an often unpredictable IT environment."
- For users — COBIT helps "obtain assurances on the security and controls of IT services provided by internal and third parties."
- For auditors — COBIT helps "substantiate their opinions to management on IT internal controls and to be proactive business advisors."

Furthermore, all audiences can use COBIT to guide self-assessments.

Any functional area of an organisation can realise benefits from using COBIT. Managers can use COBIT to guide their IT investment decisions and to obtain assurance that they are obtaining optimal results from their information and IT resources. With COBIT, users can obtain assurance that their business processes are well supported by their IT services. COBIT is extremely valuable to auditors by providing criteria for review and examination, and by providing, through the framework, an approach to improve audit efficiency and effectiveness. In addition, with the introduction of the *Management Guidelines*, all users now have a maturity model, critical success factors, key goal indicators and key performance indicators for each of the IT processes identified by COBIT. In the final analysis, however, COBIT does not have to start as a top-down process—it can be initiated as a bottom-up initiative. No matter how one arrives at COBIT, maximum benefits are obtained when COBIT is adopted by consensus of all three of these groups.

In a typical organisation there will be a person or group, the COBIT champion, advocating the formal adoption of COBIT in the organisation. To obtain an adoption consensus, the COBIT champion should determine who needs to be influenced and how to best affect that influence. To determine that best approach, the champion needs to identify the organisation's policy makers and understand the key organisational relationships and objectives. The challenge is to tie COBIT adoption to the direction of the organisation and build the case that COBIT makes sense from a strategic perspective. This implementation Guide is designed to assist the COBIT champion in having COBIT adopted organisation-wide.

TO ADOPT COBIT, WHO NEEDS TO BE INFLUENCED?

COBIT is first, a framework for management of an organisation's information and related technology. Therefore, management, especially IT policy makers, plays a major role in influencing the adoption of COBIT in the organisation. Examples of such policy makers include, the chief executive (e.g., CEO), the senior IT executive (e.g., CIO, VP for IT), and the IT steering committee. This group should be very interested in the role that COBIT can play in ensuring that information and IT resources are directed at achievement of the organisation's objectives.

Users of IT may have a somewhat narrower view than senior IT policy makers. They are typically more focused on how IT assists them in their day-to-day tasks. However, these users also want to know that IT resources are used wisely and can help them achieve their objectives. Key persons to be influenced in this group include the chief operating officer (COO), business process owners, and front-line managers.

Several functions within an organisation may be responsible for evaluating IT. First, auditors provide independent assurance that IT is secure, is meeting the needs of the organisation, and is otherwise operating in a controlled manner. Second, the users may periodically perform reviews to see that they are obtaining and properly using the IT resources that they require. Finally, the IT function may perform self-assessments to determine that they provide an efficient and effective IT resource to the organisation. Key functions to be influenced in this group include audit, the audit committee, business process owners, and IT professionals and management.

How To Introduce CobiT Into Your Organisation, *continued*

Existing organisational relationships, both formal and personal, can affect with whom the champion might form alliances and the overall implementation approach. The following factors might be considered:

1. What is the size and organisational structure of IT? Large, centralised, tall organisations will require formalised adoption processes preceded by top-level buy-in. Flatter organisations may be able to follow a consensus approach whereby all affected parties agree on the goals to be achieved and work together to implement CobiT.
2. What is the size and structure of the audit organisation? CobiT implementations within large audit organisations, with large and separate IS audit groups, may start within the IS audit function and then branch over to their IT counterparts or up to their audit management. This approach can lead to the development of a consensus.
3. What is the relationship of IT and IS audit and between audit and management? What is the philosophy of the audit organisation? Audit entities that are pro-active business advisors may easily reach consensus about adopting CobiT. Indeed, the CobiT framework, with its emphasis on business processes, management of IT resources, and achievement of business objectives, will provide additional guidance for this pre-existing pro-active, management-oriented audit philosophy. Compliance-focused audit entities and those with less than warm relationships with their audit clients will need to depend on a mandate for adoption of the CobiT framework. These mandates may come from the chief executive and/or audit committee.
4. How much of IT is outsourced? How well managed are the third party relationships? If the third-party relationships are well managed, or little of IT is outsourced, the adoption of CobiT will be easier because the decisions may be made within the entity. Otherwise, the leverage of third-party contract renewals and external audits (e.g., SysTrust™ and SAS 70 reviews in the U.S.) may be necessary to produce change.
5. To what degree has the organisation re-engineered business processes? What is going on at the organisation with respect to business process reengineering? CobiT can provide valuable input for those looking to change business processes and for business process improvements. CobiT's emphasis on enhancing information and information related technology use within organisations can provide good practice guidance in making business process improvements.

WHY SHOULD AN ORGANISATION ADOPT CobiT?

What selling points can be used to develop a consensus among these key decision makers?

1. High profile problems experienced by organisations have focused attention on corporate governance issues. As a result, management is experiencing increasing pressure to maintain an effective system of internal control. There are legal requirements, fiduciary responsibilities, contractual requirements, and societal pressures. CobiT can be used to provide reasonable assurance that business objectives, supported by IT, will be achieved, and that IT risks have been identified and remaining exposures are managed.
2. Management is accountable for the stewardship of the organisation's resources. How does management know that IT investments are optimal? CobiT-based reviews of the effectiveness of IT can help answer that question. For example, CobiT recommends that IT processes be in place to manage complex technology and to plan for the rapid obsolescence of that technology.
3. In addition to the above, the following four factors may motivate management to embrace CobiT:
   a) By controlling IT resources, the overall cost of providing IT services may decline. The CobiT *Management Guidelines* provide the tools that allow management to self-assess and make choices for control implementation and improvements over its information and related technology. These guidelines assist in aligning the IT organisation with the goals of the enterprise and provide performance measurements to ensure that these goals are achieved.
   b) CobiT reduces management fear, uncertainty, and doubt that IT resources are vulnerable to exposures and that business objectives will not be achieved.

c) Adopting CobiT will help ensure that the organisation is complying with applicable rules, regulations, and contractual obligations.
d) A "CobiTised" organisation may be able to differentiate itself from its competitors, as they would with ISO 9000 certification, by demonstrating that their IT operations are well managed and controlled.

4. An organisation that has or is about to adopt COSO (*Internal Control & Integrated Framework*) has an opportunity to simultaneously adopt CobiT. Several organisations report that joint COSO/CobiT implementations went very smoothly because the two frameworks are so complementary—COSO addressing all internal control related issues and CobiT addressing those specific to IT. (Similar arguments can be made for implementing CoCo in Canada, Cadbury in the UK, and King in South Africa.)
5. Similarily, the alignment of CobiT and SysTrust™ provides the opportunity for organisations to self-assess their IT operations against CobiT's processes prior to undergoing a SysTrust™ examination. This way, the organisation can identify and correct control weaknesses prior to the assurance services examination by independent auditors.
6. The authoritative nature of the CobiT framework has convinced many organisations to adopt it. The 318 control objectives were developed from 41 IT security, audit and control standard and best practice resources, worldwide.
7. In some organisations there have been problems for which CobiT seemed a solution. For example, one organisation had determined that their IT solutions were not meeting business needs. While they had an adequate project management process, they did not have an adequate systems development life cycle process. They used CobiT as guidance for the implementation of such a process.
8. People in many organisations that have adopted CobiT report that they have experienced improved communication among management, users, and auditors. Audit plans and audit reports prepared using CobiT, speak in management terms (e.g., process orientation, Total Quality Management) and to management issues (e.g., accountability, achievement of business objectives).
9. As organisations downsize, resources for management and control become more limited. CobiT provides a framework for risk assessment to identify and manage IT-related exposures.
10. Several internal audit organisations and public accounting firms have reported that by using CobiT they have improved their integrated audits. IS and non-IS auditors have used CobiT to coordinate their audit objectives and to communicate their audit findings.
11. The CobiT *Management Guidelines* provide new tools to assist enterprise and IT management in determining the appropriate level of control over IT so that it supports enterprise objectives. Through the definition of maturity models, critical success factors, key goal indicators and key performance indicators, these guidelines support self-assessment of strategic organisational status, identification of actions to improve IT processes and monitoring of the performance of these IT processes.

In short, management desires reasonable assurance of IT's contribution to business objectives, and seeks benchmarks to determine that IT operations are satisfactory and that they will continue to adapt in a timely manner to trends in their environment. CobiT can be used to provide such assurance.

WHAT ARE CobiT'S SCOPE AND LIMITATIONS

To be successfully implemented, everyone must be clear on what CobiT is, what it applies to, what it can do, what it is not and what it cannot do. Several points apply:

1. CobiT is a way of thinking—a new way of thinking for some. Successful adoption requires orientation, education, and training. Several auditors report spending 40 or more hours in this process.
2. CobiT is a framework that must be tailored to the organisation. For example, CobiT's IT processes must be compared to the organisation's existing processes, the organisation's risks must be reviewed, and responsibilities for the IT processes must be established.
3. As a governance, control and audit reference, CobiT must be used with other resources including: industry

audit guides such as those published by the American Institute of Certified Public Accountants (AICPA) or the Federal Financial Institutions Examination Council (FFIEC), general control and audit guides such as the Information Systems Audit and Control Foundation's *Computerized Information Systems (CIS) Audit Manual*, the AICPA/CICA SysTrust™ Systems Reliability Assurance Services, the Institute of Internal Auditors' *Systems Auditability and Control* (SAC), and platform-specific guides (i.e., those for hardware, such as IBM and Sun, and those for software such as Novell, VMS, and Top Secret).

4. CobiT is not a collection of IT controls and audit programmes. CobiT contains IT control objectives that generally must be addressed by most organisations and audit guidelines that may be used to assess performance against those IT control objectives. It is the identification and understanding of the high-level IT control objectives that serves as the framework for internal control and the selection, implementation and exercise of appropriate internal controls to meet those IT control objectives. CobiT also indirectly allows users to consider prioritised risks that threaten the achievement of IT control objectives. Since CobiT builds on IT control objectives germane to most organisations, using it helps ensure assessment efficiency. Why? Because experience shows that merely approaching a process using a controls "checklist" methodology generally results in an organisation adding unnecessary controls or those that mitigate no particular risks. Therefore, it makes sense to use an assessment tool that is built on IT control objectives first, relevant and significant IT risks second, and relevant, effective IT controls third.
5. The CobiT *Management Guidelines* are generic, generally applicable guidance and do not provide industry specific measures. Organisations will in many cases need to customise this general set of guidelines to their specific environment.
6. As described in the section below, "How To Implement CobiT In Your Organisation," to achieve a successful implementation, the CobiT champion must identify the key players, make them aware of CobiT, provide CobiT education, and train those who will use CobiT.

CobiT: A PRODUCT FOR MANY AUDIENCES

Exhibit 1 suggests why and how CobiT might be effectively used by a variety of audiences.

CobiT MANAGEMENT AWARENESS DIAGNOSTIC TOOLS

This implementation guide assists in "selling", using and implementing CobiT in any organisation. One of the most challenging tasks, however, will be getting top management's attention. The guide is therefore supplemented with two fundamental and useful tools for getting management's attention and raising management's awareness:

- IT Governance Self-Assessment
- Management's IT Concerns Diagnostic

These tools assist in analysing, understanding and communicating an organisation's IT control environment and IT control issues.

IT Governance Self-Assessment

The concise IT Governance Self-Assessment checklist provided in the section Management Awareness Diagnostics, asks management to determine, for each of the CobiT processes:

- how important the process is for their business objectives;
- whether the process is well performed (the combination of importance and performance provide a strong indicator of risk);
- who performs the process and who is accountable for the process (and is accountability unequivocal and accepted);
- whether the process and its control is formalised, i.e., is there a thorough contract for an outsourced activity or a clear set of documented procedures for internal processes; and
- whether the process is audited.

Management's awareness is then heightened by the combination of risk indicators, degree of formality and clarity of responsibility and accountability. Additionally, high risk indicators combined with answers of 'Don't know' pass a strong message.

(See Section Management Awareness Diagnostics— IT Governance Self-Assessment)

EXHIBIT 1

WHEN YOU ARE…	COBIT COULD SERVE THE FOLLOWING OBJECTIVES FOR YOU…	SOME SPECIFIC APPROACHES WHICH COULD PROVE TO BE USEFUL TO YOU…
Executive manager	Accept and promote COBIT's IT governance model for all entities within the enterprise.	Use COBIT to complement existing internal control frameworks (e.g., COSO) for IT specific matters. Use COBIT to self-assess the organisation against generally accepted international standards and take actions to improve their IT operations, as warranted. Use the COBIT process model to establish a common language between business and IT as well as to allocate clear responsibilities.
Business manager	Use COBIT to establish a common entity-wide control model so as to manage and monitor IT's contribution to the business.	Use the COBIT control objectives as code of good practice for dealing with IT at large within the business function. Use the COBIT control objectives to determine the different aspects which need to be covered by the Service Level Agreement (SLA) agreed upon with the IT function (whether internally or outsourced).
IT manager	Use the COBIT process model and detailed control objectives so as to structure the IT services function into manageable and controllable processes focussing on the business contribution. The latter is the domain of quality, security and effectiveness.	Use the COBIT control model to establish SLAs and to communicate with business functions. Use the COBIT control model as the basis for process-related performance measures. Use the COBIT control model as the basis for IT-related policies and norms. Use COBIT as the baseline model to establish the appropriate level of generally accepted control objectives as well as for external certifications (e.g., SysTrust™ and SAS 70).

How To Introduce CobiT Into Your Organisation, *continued*

Exhibit 1, *continued*

When you are…	CobiT could serve the following objectives for you…	Some specific approaches which could prove to be useful to you…
Project Manager	As general framework for minimal project and quality assurance standards.	Use CobiT to help ensure that project plans incorporate generally accepted phases in IT planning, acquisition and development, service delivery, and project management and assessment.
Developer	As minimal guidance for controls to be applied within development processes as well as for internal control to be integrated in information systems being built.	Use CobiT to ensure that all applicable IT control objectives in the development project have been addressed.
Operations	As general framework for minimal controls to be integrated into service delivery and support processes, placing clear focus on client objectives.	Use CobiT to ensure that operational policies and procedures are sufficiently comprehensive.
User	As minimal guidance for internal control to be integrated within information systems, being fully operational or under development.	Use CobiT to guide service level agreements.
Information security officer	As harmonising framework providing a way to integrate information security with other business related IT objectives.	Use CobiT to structure the information security program, policies, and procedures.
Auditor	As basis for determining the IT audit universe and as IT control reference.	Use CobiT as criteria for review and examination and for framing IT-related audits.

MANAGEMENT'S IT CONCERNS DIAGNOSTIC

The second tool, Management's IT Concerns Diagnostic, is another strong management tool because it identifies for a number of recent and specific management concerns in IT (e.g., interconnectivity, Client/Server, groupware, etc.) which processes are important to be under control to address the concerns raised.

In any particular organisation, a number of factors will influence the significance of the individual controls within the COBIT *Control Objectives*. These factors include the risks that are particularly relevant to one's type of business and IT environment, how well current controls function, and also areas where there is a desire to improve efficiencies or reduce overall costs. By mapping known risk conditions or priority issues within one's organisation onto the COBIT set of control objectives, it is possible to pinpoint those that are particularly relevant.

KEYWORDS	MANAGEMENT'S IT CONCERNS
	Management
ALIGNED	IT initiatives in line with business strategy
GOVERNANCE	IT policies and corporate governance
COMPETITIVE	Utilising IT for competitive advantage
CONSOLIDATED	Consolidating the IT infrastructure
OWNERSHIP COST	Reducing cost of IT ownership
REQUIRED SKILLS	Acquiring and developing skills
	Internet/Intranet
NETWORK ACCESS	Unauthorized access to corporate network
CONFIDENTIAL MESSAGES	Unauthorized access to confidential messages
TRANSACTION INTEGRITY	Loss of integrity -- corporate transactions
CONFIDENTIAL DATA	Leakage of confidential data
AVAILABILITY	Interruption to service availability
VIRUS	Virus infection
	Enterprise Packaged Solutions
USER NEEDS	Failure to meet user requirements
INTEGRATED	Failure to integrate
COMPATIBLE	Not compatible with technical infrastructure
SUPPORT	Vendor support problems
COST/COMPLEXITY	Expensive/complex implementation

KEYWORDS	MANAGEMENT'S IT CONCERNS
	Client Server Architecture
COORDINATED	Failure to coordinate requirements
ACCESS CONTROL	Access control problems
COMPATIBLE	Not compatible with technical infrastructure
END USER MANAGEMENT	End user management problems
VERSION CONTROL	Control of software versions
OWNERSHIP COSTS	High costs of ownership
	Workgroups & Groupware
QUALITY CONTROL	Quality control
ACCESS CONTROL	Access control
PROCEDURES	Informal procedures
DATA INTEGRITY	Data integrity
CONFIGURATION CONTROL	Configuration control
	Network Management
AVAILABILITY	Availability
SECURITY	Security
CONFIGURATION CONTROL	Configuration control
INCIDENT MANAGEMENT	Incident management
COST	Costs
SUPPORT/MAINTENANCE	Support and maintenance

The Management's IT Concerns Diagnostic matrix shown in the Management Awareness Diagnostic section, is an example of how this can be done using the Gartner Group's 1997 findings relating to management concerns with respect to IT. The issues, developed into a set of risks by ISACA, have been mapped into COBIT's 34 high-level control objectives, and show at a glance where controls are relevant. Using this technique, COBIT can be focussed onto one's organisation and the control priorities reconciled back to business risk arguments.

Furthermore, the COBIT *Management Guidelines* provide a full set of tools that allow management to self-assess the current status of their organisation. They include generic process management and IT governance guidelines that apply to the entire IT organisation, as well as IT process specific maturity models, critical success factors, key goal indicators and key performance indicators that can be used to define the organisation's strategy for improvement.

(See Section Management Awareness Diagnostics — Management's IT Concerns)

How To Implement CobiT In Your Organisation

INTRODUCING CobiT TO THE KEY PLAYERS

So, you are the CobiT champion. You have advocated the adoption of CobiT, identified the key players, and understand the formal and informal organisational relationships within your organisation. Now you must become the CobiT ambassador, the one officially charged with rolling CobiT out into the organisation. Successful adoption of CobiT requires that orientation, education, and training sessions be conducted. A generic process for the ambassador is described below. (You may have to adapt it to the implementation approach that you have selected.)

The senior management team should receive a one-hour *orientation* session. Using the short ISACA slide presentation—you might emphasise the following issues:

1. The purpose of an internal control system is to (i) "keep an organisation on course toward achievement of its mission and minimise surprises along the way," and (ii) "deal with rapidly changing economic and competitive environments, shifting customer demands and priorities, and restructuring for future growth" (*COSO Executive Summary*, p. 1). Organisations that adopt a framework of control that all employees embrace have been shown to outperform their competitors in measures of success, such as profitability, market penetration, customer service, and industry leadership.
2. Internal control is broadly defined (by COSO) as "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: efficiency and effectiveness of operations, reliability of financial reporting, and compliance with applicable laws and regulations" (*COSO Executive Summary*, p. 1). COSO defines internal control as primarily influenced by people, and is "objectives based." As such, everyone in the organisation is responsible for the quality of the risk control evaluation. COSO recognises that control is everyone's job.
3. Control is defined (by CobiT) as 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 and detected.
   [Summarise these three points (1 through 3) by stating that internal control is a process by which management increases the possibility of achieving organisational objectives while minimising the risks that bad things will happen along the way. CobiT and COSO are complementary frameworks addressing the IT and non-IT control issues, respectively. (Similar summaries could be provided for CoCo in Canada and Cadbury in the UK.)]
4. Review the impact that technology has on control. That is, while operational and control objectives change little (some technology-specific control objectives will change), it is the *methods* for control that are most directly impacted by changes in technology. Then, emphasise that CobiT's emphasis on control *objectives* will provide a fundamental framework that will provide guidance to those responsible for designing, implementing and exercising controls as technology changes.
5. CobiT includes technology-related control objectives and methods derived from 41 international, generally-accepted security, audit, and control references.
   [Summarise these two points (4 and 5) by stating that by adopting CobiT as a standard for management and control of IT, the organisation can obtain reasonable assurance that its IT resources are directed at attaining organisational objectives.]
6. Conclude the orientation session by reviewing CobiT's content.
   a. In the CobiT *Framework* describe how CobiT documents the relationships between information criteria, IT resources, and IT processes.
   b. In CobiT *Control Objectives* describe the relationship between the 34 high-level control objectives and the 318 detailed control objectives.
   c. In CobiT *Audit Guidelines* review the generic audit guideline and the structure of the audit process. These guidelines can direct evaluation of IT processes.
   d. In *Management Guidelines* describe how the maturity models, critical success factors, key goal indicators and key performance indicators

can be used to assist management in assessing IT processes against CobiT's 34 IT processes and the organisation's IT governance environment.

The remaining key players should receive a one to two day *education* session. Using the long ISACA slide presentation, these implementation workshops should help people understand and begin to use all of the CobiT products. (NOTE: The ISACA Professional Seminar Series [PSS] CobiT workshop includes case studies that complement the slide presentation.) The following sequence often has been used. One or more people receive an introduction to CobiT (between one hour and 2 days) at local or international ISACA workshops. Then, they conduct workshops themselves, or engage others to do so, within the organisation. These workshops could be for the IS auditors, other auditors, management (general, audit, and IT), users, and IT staff.

Finally, those who will actually use CobiT may require more extensive *training* to effectively utilise CobiT. In the section below (Beginning To Use CobiT) we describe ways that CobiT has been successfully implemented. Among these are activities that can be used to provide on-the-job training in how to use CobiT.

BEGINNING TO USE COBIT

Once you have chosen to use CobiT in your organisation, consider doing the following to formalise its use:

1. Specify in your audit policies manual that CobiT is an example of clear policy and good practices for IT control and audit that will be used to guide audits conducted within the organisation.
2. Include in the audit procedures manual the "Generic Audit Guideline" contained in the CobiT *Audit Guidelines*.
3. As explained in the section below, "Risk Assessment and Audit Planning Using CobiT," use the CobiT *Framework* to perform risk assessments and to guide the development of audit plans.
4. As explained in the section below "Conducting Audits Using CobiT," use the CobiT *Framework* and *Control Objectives* to plan specific audit engagements.
5. As explained in the section below "Conducting Audits Using CobiT," tailor your audit programmes to include activities from CobiT *Audit Guidelines*.

The following activities, documents, and ideas have been used by organisations that have successfully implemented CobiT. Many of these will be appropriate in any organisation.

Exhibit 2 is an implementation action plan developed by an IS auditor at a bank. Notice the implementation objectives and goals in addition to the process. While this plan was developed by an IS auditor, such a plan could be developed and the memo issued by an implementation team that includes upper management and other key players.

Not being willing or able to launch a full CobiT implementation, some organisations have rolled CobiT out by beginning to use it in carefully chosen audit engagements. These pilot implementations were then used to identify the benefits of a CobiT implementation. In all cases these pilots have led to full implementations of CobiT. Examples are included in the last section, "Using the CobiT Audit Guidelines."

The CobiT *Management Guidelines* introduce new concepts and tools that will increase the acceptance and effectiveness of CobiT. Their use will open new perspectives and new options for introducing CobiT to the organisation. The *Management Guidelines* volume of CobiT includes a "How to Use" guide in Appendix I. This initial guide is only a beginning and it will evolve based on the feedback provided by security and control professionals who will implement these newly developed guidelines. This Implementation Tool Set will be updated in future editions to reflect the newly gained experience of the CobiT champions.

Exhibit 2— CobiT Implementation Action Plan

OBJECTIVE

To gain acceptance of and integration of CobiT concepts into our technology organisation including Audit, Operations and Technology, and outsourced services.

GOALS

1. Continue to provide essential audit and control consulting services, expanded and adapted to ensure coverage of CobiT business processes relevant to the banking industry.
2. Ensure the bank's information needs are satisfied by our technology organisation consistent with the information criteria identified in CobiT.
3. Ensure significant planning and organisation activities identified in CobiT are integrated into the technology organisation at the bank.
4. Ensure significant acquisition and implementation activities identified in CobiT are employed in the Computer Services department and incorporated in the project management approach used at the bank.
5. Ensure significant delivery and support activities identified in CobiT are provided to internal bank customers by our Network Services department and outsourced service vendors.
6. Ensure significant monitoring processes identified in CobiT are employed by the bank's technology and audit organisations.

APPROACH

- Familiarisation
- Education
- Commitment
- Adaptation
- Implementation

SEQUENCE

- Audit organisation
- Technology organisation
- Outsourced service providers
- Senior management
- Audit Committee

PROCESS

1. Distribute copies of the CobiT *Executive Summary* and preliminary survey (see Exhibit 3) to key managers, triggering analysis of and thoughts about the existing organisation.
2. Compile survey results and develop a presentation relating results to CobiT concepts.
3. Present to Operations and Technology management team.
4. Present to Operations and Technology staff.
5. Present to outsourced service provider management and key staff people.
6. Assist key managers in developing action plans to integrate CobiT concepts into the bank's business processes.
7. Present CobiT concepts and activities progress reports to senior management to inform and gain commitment.
8. Restructure audit inventory to reflect a CobiT process orientation.
9. Develop or update audit programs consistent with CobiT audit guides.
10. Develop CobiT education opportunities consistent with organisational needs.
11. Conduct CobiT training as necessary.
12. Monitor progress on IT action plans.
13. Present CobiT concepts, progress, and results to Audit Committee.

MILESTONES

1. May — complete survey and action plans
2. July — present CobiT to senior management
3. August — present CobiT to Audit Committee

RISK ASSESSMENT AND AUDIT PLANNING USING COBIT

The following COBIT-based matrices could be used by the audit team during pre-audit work to help identify potential areas for audit or management advisory services work. Some of the matrices can be effectively used by having them completed by auditee management, or business process owners. In that light, should the audit team decide to complete the forms jointly with the auditee, the matrices may serve to facilitate pre-audit interview discussions. Some of these discussions may prove very helpful to management at the start of the engagement by identifying early on operational areas performing IT functions that should be subject to the organisation's control or operational standards, but may not be in compliance. It may also assist management in ensuring that there are clear points of accountability for all IT processes, and in identifying who the audit team needs to interview or from whom they need to obtain information. These matrices may assist the auditor in performing a high-level assessment of internal control documentation. The audit team should determine whether internal control documentation has been reviewed and approved by management. The absence of documented controls for any of the IT processes should be considered as a red flag for control weaknesses, and an opportunity for management advisory services.

PRIOR AUDIT WORK FORM

Purpose: To identify whether audit work related to the IT process was included in the prior audit scope. If it was, then the form requires the auditor to identify the conclusion(s) drawn from the prior audit work. Completion of this form presumes use of COBIT in previous engagements.

To be completed by: The audit team during pre-audit work before conducting an on-site visit with the auditee.

Discussion: If the prior audit work resulted in the equivalent of a clean opinion, then there would not be an audit finding in need of resolution. Since there also may be more than one finding per IT process, the form requires the auditor to identify the number of findings and to characterise their disposition. If there were more than one finding for a process, the auditor would use numerical values in the disposition columns.

(See Section IT Control Diagnostics—Prior Audit Work Form)

ENTITY SHORT FORM

Purpose: To identify which IT processes are considered the most important and how well management believes these processes are being performed.

To be completed by:

1.a. Auditee management (IT or non-IT) or the business process owners during the pre-audit phase of the audit. If given to a representative sample of managers across various departments or divisions, the matrix may be used to identify differences in understanding of the relative importance and level of performance of each IT process.

b. If certain IT processes have been outsourced, the matrix can be used to obtain a reading on management's, or the business process owner's, level of satisfaction with the third-party provider's service. And, again, when completed by a representative sample of managers across organisational boundaries, it may provide some insight into varied perceptions of services provided.

2. The audit team during pre-audit to record their understanding of the relative importance and performance of each IT process. The latter may be a reading obtained through surveying user satisfaction or may be based upon results obtained from management's performance assessments. (The column "Formally Rated" would be marked 'Y' for 'yes' and 'N' for 'no' to indicate whether management has a process to formally rate performance.)

Discussion: Could be sent to managers and business process owners. If sent, descriptions of the IT processes, such as those found in the COBIT *Framework*, should be attached to the form. (The "Entity Long Form" should be used when audit obtains information first hand via interview.)

How To Implement CobiT Into Your Organisation, *continued*

This matrix can be used for risk assessment to answer the questions "what is important to us?" and "how are we doing?" There are instances where this was used for a discussion among management, auditors, and IT. Alternatively, this matrix could be used to gather information from these groups separately and to compare the results to determine where there is disagreement about importance and performance. In any case, this matrix can be the catalyst for very useful discussions. For example, where any group cannot decide on the level of importance, some education may be indicated. And, where the performance of any process can't be evaluated, additional investigation may be required.

This matrix can also be used for multiple iterations. You might first use only the importance columns to determine the perceived level of performance. Some time later (perhaps a week) use the matrix again with only the performance columns. Because it may be difficult to assess important functions as poorly performed, this two-step process might lead to more useful performance assessments.

(See Section IT Control Diagnostics—Entity Short Form)

Entity Long Form

Purpose: To document management and business process owner assessments of which IT processes are most important and how well they believe these processes are being performed. The form also makes reference where there are documented internal controls for the IT processes.

To be completed by: The audit team during the pre-audit phase of the audit. The matrix should be completed either jointly with management and business process owners, during the course of an auditor's interview, or by the audit team itself.

Discussion: The auditor can gain insights into management's understanding of the degree to which internal controls are documented for the IT processes. Since the audit team will be requesting copies of documented controls during pre-audit, the workpaper reference should be used to cross reference copies of the documented controls (control manuals, procedures, standards, etc.), or any preliminary reviews performed.

(See Section IT Control Diagnostics—Entity Long Form)

Risk Assessment Form

Purpose: To assist the audit team in identifying those IT processes where risk-based auditing would indicate that audit work (or management advisory services work) may be warranted.

To be completed by: Either the audit team or management, or both jointly, during pre-audit work

Discussion: The audit team should complete this after they have completed the "Entity Short Form" and "Entity Long Form", and after they have gained and recorded a sufficient understanding of the organisation's mission, primary business objectives, critical success factors, regulatory or legal (including contractual) requirements, and control structure. The audit team may have performed some analytics by this time.

(See Section IT Control Diagnostics—Risk Assessment Form)

Responsible Party Form

Purpose: To identify who performs each IT process and who has final responsibility for each process.

To be completed by:
The audit team, jointly with auditee management, during the pre-audit phase of the audit.

Could be sent to managers and business process owners. If sent, descriptions of the IT processes, such as those found in the CobiT *Framework*, should be attached to the form. See Exhibit 3, CobiT Survey, for an example.

Discussion: It is suggested that this form be completed along with the contract service/service level agreement (SLA) form (discussed in the next section) in order to fully identify services provided within the entity by IT Services, within the entity but not by IT Services, or by a third-party provider.

Given the pervasive nature of IT, it is likely that more than one process will be performed by both IT Services and by non-IT Services personnel. In that light, completing the form jointly with senior management will provide insight into management's understanding of what processes are performed by whom. It will also highlight the spread of IT responsibilities across the organisation where IT has taken on a pervasive nature.

Although the IT process and what would be addressed by it may be somewhat self-evident, it is recommended that the audit team be prepared to provide an overview to management of what is covered by each process. Also, the form may be used while interviewing managers from different departments or divisions across the organisation to identify the extent to which they have a clear understanding of which functional units, internally or outsourced, are performing IT processes.

Although the form requires the audit team to identify who has primary responsibility, it should be considered as a starting point for pre-audit discussions regarding assigned responsibilities, points of accountability, and given decentralised or "spread" IT process activities, the degree of required standardisation needed. As an example of the latter, if within the given organisation there has been a shift of processing from IT Services to the individual departments, it does not mean that the control objectives of data security and system availability associated with IT services no longer apply. The control objectives must still be addressed, but now by different organisational units and generally with different control strategies.

(See Section IT Control Diagnostics—Responsible Party Form)

CONTRACT SERVICE/SLA FORM

Purpose: Where the "Responsible party" matrix indicates that one or more IT services are NOT performed by IT Services, this form identifies whether formal contracts or SLAs exist and controls are documented for each "contracted" IT process. Contracted/SLA IT processes include: outsourced services, internally-contracted services (within the organisation but not by IT Services), and services for which an internal SLA exists. The form may assist the auditor in identifying functions that have been "contracted" without explicit contracts or agreements. Accordingly, the form would help identify the potential need for including contract/SLA audit work in the scope of the audit.

To be completed by: The audit team during the pre-audit phase of the audit.

Discussion: The contract service/SLA form assists the auditor with his/her assessment of internal controls. Before evaluating the appropriateness of stated controls, the auditor would determine the extent to which controls are documented.

(See Section IT Control Diagnostics—Contract Service/SLA Form)

EXAMPLES OF THE USE OF THE PLANNING MATRICES

As an initial assessment at the beginning of his COBIT implementation, an IS Auditor conducted a survey at a bank. The survey, included as Exhibit 3, is an application of the "Responsible Party Form." The survey is addressed to those who directly report to the Senior VP of Operations and Technology. The four pages attached to the survey were printed from a database that the IS Auditor had developed using the text files that are included with the COBIT package. The responses from the survey indicated that everyone was responsible for most of the COBIT processes! The IS Auditor attributed the absence of clearly assigned responsibilities to a lack of clear direction from the VP. As a result of this survey, and the findings of a regulatory audit, a technology management function was added to the Operations and Technology organisation. This function was assigned responsibility for many of the COBIT Planning & Organisation processes.

Exhibit 3 — CobiT Survey

Memorandum

To: Network Services Manager, Telecommunications Manager, Programming Supervisor, Data Center Operations Manager, Trust Data Center Manager

cc: Senior VP of Operations and Technology, Outsource Account Manager

From: IS Audit Manager

Date: March 19, 20xx

Re: IT Business Processes and Control Objectives

I would like to take a moment to introduce you to a new way of looking at internal controls in the IT area; and to ask your help as we become more proactive and supportive auditors. Our old approach to controls and IT auditing tended to emphasise technical issues. The Information Systems Audit and Control Foundation (ISACF) recently published, through its IT Governance Institute, the 3rd Edition of its Control Objectives document, which focuses the control spotlight on information criteria, business processes and IT process control and manageability.

This document, called Control Objectives for Information and related Technology, or CobiT, identifies 34 significant IT business processes within four domains of Planning and Organisation (PO), Acquisition and Implementation (AI), Delivery and Support (DS), and Monitoring (M). CobiT then ties 318 different tasks and activities to these 34 processes. Each of these tasks, activities, and processes has a related control component, on which audit activities can focus.

Consequently, CobiT provides a great opportunity for IS Audit to re-engineer our audits toward IT business processes. It also presents an opportunity for the IT function to perform a self-assessment, ensuring all necessary services are being provided to the bank. I have attached a copy of the CobiT Executive Summary for your review (those of you who do not already have one).

To begin re-engineering the audit function, I would like to know how you view your ownership of or responsibility for these IT business processes. I have included with this memo a preliminary survey, which lists all 34 processes and asks respondents to indicate whether or not they have responsibility for the process. It would help if I had your responses, and any thoughts you might have on CobiT, by March 28. I expect to find overlaps and gaps; keep in mind the purpose of this survey is to develop a picture of where we are today. I will provide the results so each of you can understand how the others see their roles in the IT function.

I am excited about this change in focus because it will help us conduct IS Audit activities consistent with how you operate the IT function part of the business. We can perform “process” audits in addition to “product” audits. We can concentrate on continuous process improvement. Audits can more easily address information and technology risks and criteria such as confidentiality, integrity, availability, efficiency, effectiveness, compliance and reliability. They can also relate controls to our data, application systems, technology, people and facilities resources. In short, auditing can become a better resource for you if we use CobiT as a tool and guide.

If there are other management staff who you believe should complete the survey; or if you have any questions or observations about the survey, or CobiT concepts in general, please call me at ext. xx, or send a message via e-mail. Please return the surveys via interoffice mail by March 28. Thank you.

EXHIBIT 3, *continued*

Preliminary Survey – IT Process Responsibilities for:

Area: _____ Date: _____

Respondent: _____ Auditor: _____

DOMAIN ID	PROCESS ID	IS THE AREA RESPONSIBLE FOR THE IT PROCESS OF:	WHICH SATISFIES THE BUSINESS REQUIREMENT:	(YES/NO/UNKNOWN)
PO	1	defining a strategic IT plan	to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment	_____
	2	defining the information architecture	of optimising the organisation of the information systems	_____
	3	determining technological direction	to take advantage of available and emerging technology to drive and make possible the business strategy	_____
	4	defining the IT organisation and relationships	to deliver the right IT services	_____
	5	managing the IT investment	to ensure funding and to control disbursement of financial resources	_____
	6	communicating management aims and direction	to ensure user awareness and understanding of those aims	_____
	7	managing human resources	to acquire and maintain a motivated and competent workforce and maximise personnel contributions to the IT process	_____
	8	ensuring compliance with external requirements	to meet legal, regulatory and contractual obligations	_____
	9	assessing risks	of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors	_____
	10	managing projects	to set priorities and to deliver on time and within budget	_____
	11	managing quality	to meet the IT customer requirements	_____

Notes and Comments:

HOW TO IMPLEMENT COBIT INTO YOUR ORGANISATION, *continued*

EXHIBIT 3, *continued*

DOMAIN ID	PROCESS ID	IS THE AREA RESPONSIBLE FOR THE IT PROCESS OF:	WHICH SATISFIES THE BUSINESS REQUIREMENT:	(YES/NO/UNKNOWN)
AI	1	identifying automated solutions	of ensuring an effective and efficient approach to satisfy the user requirements	_____
	2	acquiring and maintaining application software	to provide automated functions which effectively support the business process	_____
	3	acquiring and maintaining technology infrastructure	to provide the appropriate platforms for supporting business applications	_____
	4	developing and maintaining procedures	to ensure the proper use of the applications and the technological solutions put in place	_____
	5	installing and accrediting systems	to verify and confirm that the solution is fit for the intended purpose	_____
	6	managing changes	to minimise the likelihood of disruption, unauthorised alterations and errors	_____

Notes and Comments:

DOMAIN ID	PROCESS ID	IS THE AREA RESPONSIBLE FOR THE IT PROCESS OF:	WHICH SATISFIES THE BUSINESS REQUIREMENT:	(YES/NO/UNKNOWN)
DS	1	defining and managing service levels	to establish a common understanding of the level of service required	_____
	2	managing third-party services	to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements	_____
	3	managing performance and capacity	to ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs	_____
	4	ensuring continuous service	to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption	_____
	5	ensuring systems security	to safeguard information against unauthorised use, disclosure or modification, damage or loss	_____
	6	identifying and allocating costs	to ensure a correct awareness of the costs attributable to IT services	_____
	7	educating and training users	to ensure that users are making effective use of technology and are aware of the risks and responsibilities involved	_____
	8	assisting and advising customers	to ensure that any problem experienced by the user is appropriately resolved	_____
	9	managing the configuration	to account for all IT components, prevent unauthorised alterations, verify physical existence and provide a basis for sound change management	_____
	10	managing problems and incidents	to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence	_____
	11	managing data	to ensure that data remains complete, accurate and valid during its input, update and storage	_____
	12	managing facilities	to provide a suitable physical surrounding, which protects the IT equipment and people against man-made and natural hazards	_____
	13	managing operations	to ensure that important IT support functions are performed regularly and in an orderly fashion	_____

Notes and Comments:

HOW TO IMPLEMENT COBIT INTO YOUR ORGANISATION, *continued*

EXHIBIT 3, *continued*

DOMAIN ID	PROCESS ID	IS THE AREA RESPONSIBLE FOR THE IT PROCESS OF:	WHICH SATISFIES THE BUSINESS REQUIREMENT:	(YES/NO/UNKNOWN)
M	1	monitoring the processes	to ensure the achievement of the performance objectives set for the IT processes	_____
	2	assessing internal control adequacy	to ensure the achievement of the internal control objectives set for the IT processes	_____
	3	obtaining independent assurance	to increase confidence and trust among the organisation, customers, and third-party providers	_____
	4	providing for independent audit	to increase confidence levels and benefit from best practice advice	_____

Notes and Comments:

Using the matrix in Exhibit 4, another IS auditor at a different organisation mapped CobiT's 34 high-level control objectives to the IS policies, procedures, and standards at his organisation. This was an iterative process as the IS auditor gradually discovered the documented policies. Initially a quantitative appraisal, this process continues at the organisation with an assessment of the quality and adequacy of the existing policies, procedures, and standards. This is an adaptation of the "Entity Long Form" with the entries in the columns that cross-reference to existing policies and procedures representing documentation of controls.

EXHIBIT 4: REVIEW OF POLICIES, PROCEDURES, AND STANDARDS

CobiT's 34 Processes	**IT Policies & Procedures** A B C D E F – – –
PO1 PO2 • • • M4	A = Addresses CobiT objective C = Could provide desired control E = Evaluate (tests of compliance) R = Report • Positive conclusion • Finding

Another IS auditor, at a different organisation, used CobiT to assess risks and to choose those audit areas that required his attention. Exhibit 5 depicts the matrix that he used for this assessment. Notice that the CobiT Information Criteria and IT Resources played prominent roles in this assessment. This matrix combines elements of the "Prior Audit Work" and "Risk Assessment" forms.

EXHIBIT 5: USING COBIT FOR RISK ASSESSMENT

Audit area	**Factors: Date last audited, Information criteria, IT resources, complain/request, $ exposure**
	Risk rankings –10 to +10 Totals for each process and then totaled for each audit area.

At another organisation, an IS auditor and IT professional teamed up to use the matrix depicted in Exhibit 6 to focus their attention on those areas that required additional policies, procedures, or standards, or additional audit attention during the year. This is an adaptation of the "Risk Assessment" form.

EXHIBIT 6: RISK ASSESSMENT

CobiT's 34 Processes	Level of Assessed Risk			
	High	Medium	Low	Notes
PO1 PO2 • • • M4				

In an audit organisation, the IS auditors are using CobiT's 34 processes to assess their existing and planned audit coverage (see Exhibit 7). They want to know how much audit effort is dedicated to what kinds of IT processes and whether any IT processes are problematic (i.e., many audit findings). Further, they want to

HOW TO IMPLEMENT COBIT INTO YOUR ORGANISATION, *continued*

know which entities have received, or will receive, audits and what types of audits (i.e., what IT processes) have been, or will be, performed.

EXHIBIT 7: AUDIT PLANNING

COBIT's 34 Processes	**Audits (or audit entities)** A B C D E F – – –
PO1 PO2 • • • M4	S = Pre-audit survey A = Audit R = Report • Positive conclusion • Finding

In summary, all of these benchmarking/assessment/planning activities provide additional information to the organisation, such as:

- Additional (or documented) policies, procedures, or standards are required.
- IT processes (or controls) need to be added or eliminated.
- Responsibilities for IT processes need to be assigned or reassigned.
- There are risks that need to be addressed.
- There are internal or outsourced functions that need to be managed better.
- There are audits that need to be performed.

CONDUCTING AUDITS USING COBIT

The following describes in outline form how the various pieces of COBIT and the risk assessment and planning matrices described above might be used in a "typical" audit process.

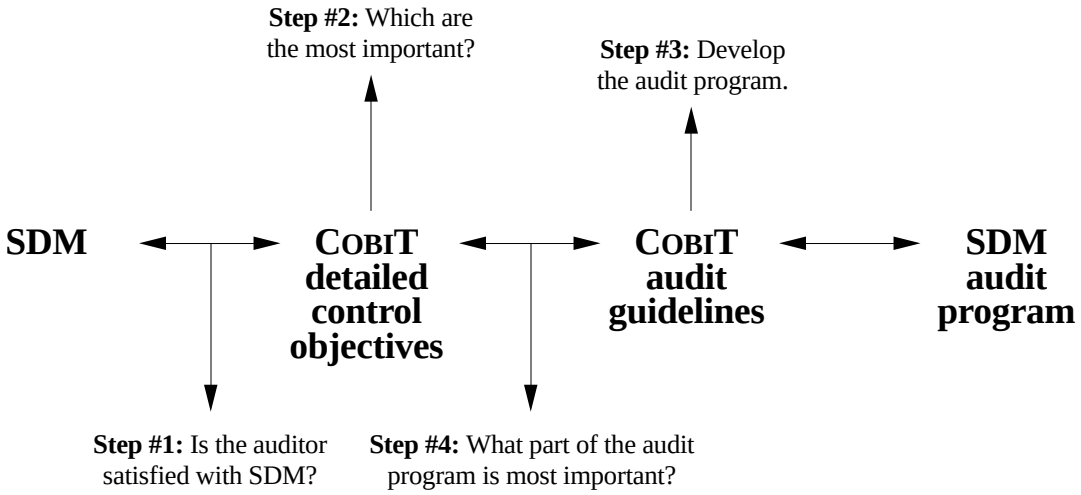
1. **An Optional Step.** If necessary, *select the type of audit engagement* for the entity to be audited. The following are the types of audits that might be conducted: financial, performance, compliance, IT (facility, system under development, post-implementation review, planning & organisation, management advisory service), integrated audit, agreed-upon procedures, etc. These audit types are not mutually exclusive. A risk assessment, using the COBIT *Framework* and tools similar to the "Entity Short Form," "Responsible Party," and "Contract Service/SLA" matrices explained above might facilitate selection of the type of audit engagement.
2. **Refine Scope and Determine Audit Objectives.** Having selected an entity and type of audit engagement, it is now time to use the COBIT detailed control objectives (from the COBIT *Control Objectives*) to obtain additional insights into the IT processes (from the COBIT *Framework*) selected for this audit. Once the scope has been refined, develop audit objectives using the COBIT *Control Objectives*. The scope and audit objectives should be discussed with the client during the pre-engagement conference. NOTE: This step may be repeated as required throughout the audit.
3. **Develop the Audit Work Program.**
   a. If there is an existing audit work program:
      i. Compare the audit objectives to the COBIT *Control Objectives*.
      ii. Compare the steps in the audit program to the activities in the COBIT *Audit Guidelines*.
      iii. Add audit activities suggested by platform-specific (e.g., security packages, LANs), organisational, legal, and regulatory guides and manuals.
   b. If there is no existing audit work program. Perform the steps as above, but develop the audit program, using COBIT, rather than comparing an existing program to COBIT for completeness.
4. **Perform the Audit.** At the entrance conference as the type, scope, and objectives are discussed, describe how COBIT contributed to these and will be used to guide the audit.
5. **Write the audit report.** Write-up conclusions focusing on the objectives achieved and not achieved. Using COBIT, make the business case to substantiate the results. Include COBIT in the section where criteria is cited in the audit findings and in the section describing the methodology used in performing the audit.

USING THE COBIT *AUDIT GUIDELINES*

As described above, use of the COBIT *Audit Guidelines* falls into two main categories: the auditor has an existing audit program or the auditor does not have an existing audit program.

IF THERE IS NO EXISTING AUDIT PROGRAM

The diagram below depicts the steps that would apply if there were an IT process that is to be audited, but no audit program exists. The IT process used in this example is a systems development methodology (SDM).



In **Step # 1** the auditors determine, by comparing the SDM to the applicable COBIT detailed control objectives (in *Control Objectives*), if the SDM provides adequate control over systems development.

Assuming that they are satisfied, the auditors choose, in **Step # 2**, those detailed control objectives which are the most important, given their understanding of the risks and related objectives for the subject IT process (the SDM). COBIT helps the auditors to make this determination because it is focused on control of IT resources to ensure that the seven qualities of information provided are addressed to achieve organisational objectives.

In **Step # 3** the auditors develop an audit program with the assistance of the COBIT *Audit Guidelines*. Notice that we have defined the ***detailed*** objectives of interest, yet the COBIT *Audit Guidelines* are grouped by ***high-level*** control objectives (i.e., IT processes). The mapping process into the audit guidelines required for step # 3 is described below.

In **Step # 4** the auditor determines which steps in the audit program require more of their attention. Having determined the most important detailed objectives in step # 2, this step is straightforward.

At one organisation, the use of COBIT for a change control audit accelerated the audit planning process and led to further uses of COBIT by audit and by IT. Exhibit 8 is an excerpt from this change control audit program. The "Business Objectives" were adapted from the COBIT *Framework* (the high-level control objectives). The "Effects" are the risks written by the organisation for

How To Implement CobiT Into Your Organisation, *continued*

this audit. The "Control Objectives" were adapted from the CobiT *Control Objectives*. The "Items to Review-Test" were adapted from the CobiT *Audit Guidelines*. This process is typical for the development of a CobiT-based audit program:

a. Review CobiT's 34 high-level control objectives and select those objectives that apply to this audit.
b. Describe the risks (or "exposures" or "effects") that may result from failure to achieve each objective chosen in step a.
c. Select from the CobiT Control Objectives those detailed control objectives that apply to this audit. Typically, we should only need to review the detailed control objectives for the high-level control objectives chosen in step a, above.
d. Using the CobiT *Audit Guidelines*, enumerate the audit procedures to be performed. In this step the IS auditor should choose those audit procedures that relate to the detailed control objectives selected in step c, above. If in step c, the IS auditor only selected detailed objectives for the high-level control objectives identified in step a, we should only need to review the audit guidelines for those high-level control objectives.
e. To complete the audit program the IS auditor may then need to include additional audit tests that relate to the specific platform being audited. For example, the auditor may need to refer to the manual(s) for the database management system selected for this system development effort.

EXHIBIT 8 — EXCERPT FROM AUDIT PROGRAM

	BUSINESS OBJECTIVE	EFFECT	CONTROL OBJECTIVES	ITEMS TO REVIEW — TEST	REF.
AI6	MANAGING CHANGES				
	To ensure that the automated solutions were identified via an analysis of all possible alternatives which met user requirements.	Failure to follow change control procedures causes failures, corrupted data and files, processing delays, increased costs and users and systems needs are not met. Increased risk during emergency situations.	*Change Request Initiation And Control* IT management should ensure that all requests for changes, system maintenance and supplier maintenance are standardised and are subject to formal change management procedures. Changes should be categorised and prioritised and specific procedures should be in place to handle urgent matters. Change requestors should be kept informed about the status of their request.	Review system change procedures for sufficient internal controls, etc. Test to see if system change procedures are effective and enforced even during emergency situations.	
		Insufficient integration with configuration management system may affect other platforms.	*Control of Changes* IT management should ensure that change management and software control and distribution are properly integrated with a comprehensive configuration management system. The system used to monitor changes to application systems should be automated to support the recording and tracking of changes made to large, complex information systems.	Review and test appropriate documentation to ensure compliance with comprehensive management system.	

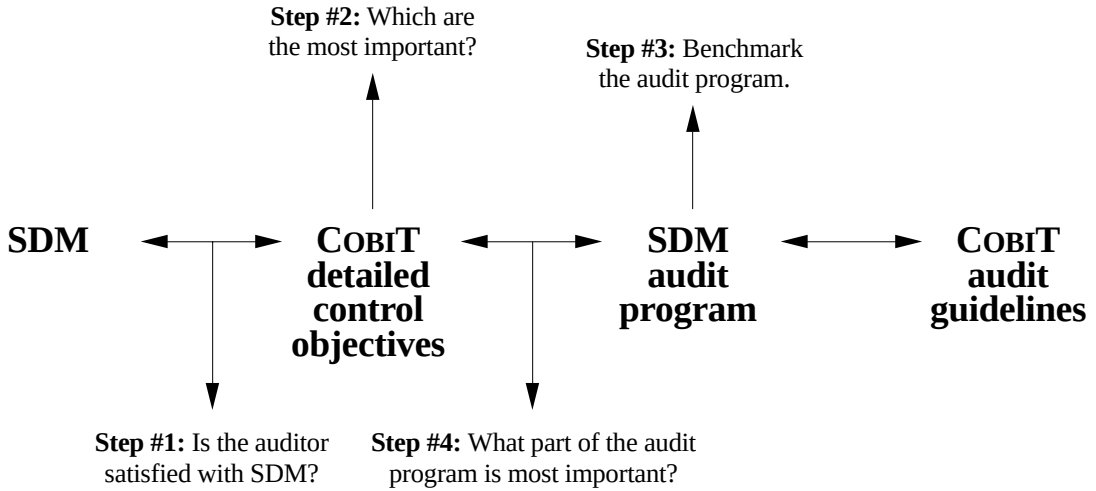
How To Implement CobiT Into Your Organisation, *continued*

If There Is An Existing Audit Program

The diagram below depicts the steps that would apply if there is an IT process that is to be audited and an existing audit program exists that we want to benchmark against the CobiT *Audit Guidelines*. Again, the IT process used in this example is a systems development methodology (SDM).

Step # 1, **Step #2**, and **Step # 4** are the same as when there is no existing audit program.

In **Step # 3** the auditor compares his/her audit program to the CobiT Audit Guidelines to determine if there are activities suggested by CobiT that may improve the existing audit program.



Mapping CobiT Detailed Control Objectives to Audit Guidelines

As previously mentioned, the activities in the CobiT *Audit Guidelines* are grouped by the 34 high-level control objectives. Since an auditor would typically develop audit programs to assess accomplishment of detailed control objectives, an auditor must map their detailed objectives into the CobiT *Audit Guidelines*.

For example, if the auditor were to audit one detailed control objective (an absurd task to be sure). Assume further that the ***one*** objective is AI 1.18 Acceptance of Technology (see *Control Objectives*). The audit activities, beginning on the following page, were selected from the audit activities of the *Audit Guidelines* because they related to the detailed control objective AI 1.18.

Obtaining an understanding by:

J **Interviewing:**

- Project owners/sponsors
- Contractor management

J **Obtaining:**

- Policies and procedures relating to the system development life cycle and procurement of software
- IT objectives and long- and short-range plans
- Selected project documentation, including requirements definition, alternatives analyses, technological feasibility studies, economic feasibility studies, information architecture/enterprise data model analyses, risk analyses, internal control/security cost-effectiveness studies, audit trail analyses, ergonomic studies, and facilities and specific technology acceptance plans and test results
- Selected contracts relating to software purchase, development or maintenance

Evaluating the controls by:

J **Considering whether:**

- Policies and procedures exist requiring that:
  - the solution's functional and operational requirements be satisfied including performance, safety, reliability, compatibility, security and legislation
  - products be reviewed and tested prior to their use and financial settlement
  - the end products of completed contract programming services be tested and reviewed according to the related standards by the IT quality assurance group and other concerned parties before payment for the work and approval of the end product
  - an acceptance plan for specific technology is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria
- Testing included in contract specifications consists of system testing, integration testing, hardware and component testing, procedure testing, load and stress testing, tuning and performance testing, regression testing, user acceptance testing, and finally, pilot testing of the total system to avoid any unexpected system failure
- Specific technology acceptance tests should include inspection, functionality tests and workload trials

HOW TO IMPLEMENT COBIT INTO YOUR ORGANISATION, *continued*

Assessing the compliance by:

- **Testing that:**
  - Purchased products are reviewed and tested prior to their use and the financial settlement
  - Appropriateness and completeness of specific technology acceptance plan, including inspections, functionality tests and workload trials

Substantiating the risk of control objectives not being met by:

- **Performing:**
  - Benchmarking of the identification of user requirements to meet automated solutions against similar organisations or appropriate international standards/recognised industry best practices
  - A detailed review of the acceptance process for specific technology to ensure that inspections, functionality tests and workload trials meet the requirements specified in the contract

- **Identifying:**
  - Deficiencies in the organisation's system development life cycle methodology
  - Solutions that do not meet user requirements
  - Solutions that did not follow the organisations established procurement approach and thus resulted in additional costs being borne by the organisation
  - Where a specific technology is accepted but inspections, functionality tests, and workload trials, have not been adequately performed, and as a result the technology does not meet user requirements and/or does not comply with contract terms
  - Any system failures

MANAGEMENT AWARENESS DIAGNOSTICS

MANAGEMENT AWARENESS DIAGNOSTICS

IT GOVERNANCE SELF-ASSESSMENT

Importance – how important for the organisation on a scale from 1 (not at all) to 5 (very)

Performance – how well it is done from 1 (don't know or badly) to 5 (very well)

Audited – Yes, No or ?

Formality – is there a contract, an SLA or a clearly documented procedure (Yes, No or ?)

Accountable – Name or "don't know"

Risk				Who Does It?						
Importance	Performance	COBIT's Domains and Processes		IT	Other	Outside	Don't Know	Audited	Formally	Who is accountable?
		PLANNING & ORGANISATION								
		PO1	Define a Strategic IT Plan							
		PO2	Define the Information Architecture							
		PO3	Determine the Technological Direction							
		PO4	Define the IT Organisation and Relationships							
		PO5	Manage the Information Technology Investment							
		PO6	Communicate Management Aims and Direction							
		PO7	Manage Human Resources							
		PO8	Ensure Compliance with External Requirements							
		PO9	Assess Risks							
		PO10	Manage Projects							
		PO11	Manage Quality							
		ACQUISITION & IMPLEMENTATION								
		AI1	Identify Automated Solutions							
		AI2	Acquire and Maintain Application Software							
		AI3	Acquire and Maintain Technology Infrastructure							
		AI4	Develop and Maintain Procedures							
		AI5	Install and Accredit Systems							
		AI6	Manage Changes							
		DELIVERY & SUPPORT								
		DS1	Define and Manage Service Levels							
		DS2	Manage Third-Party Services							
		DS3	Manage Performance and Capacity							
		DS4	Ensure Continuous Service							
		DS5	Ensure Systems Security							
		DS6	Identify and Allocate Costs							
		DS7	Educate and Train Users							
		DS8	Assist and Advise Customers							
		DS9	Manage the Configuration							
		DS10	Manage Problems and Incidents							
		DS11	Manage Data							
		DS12	Manage Facilities							
		DS13	Manage Operations							
		MONITORING								
		M1	Monitor the Processes							
		M2	Assess Internal Control Adequacy							
		M3	Obtain Independent Assurance							
		M4	Provide for Independent Audit							

MANAGEMENT'S IT CONCERNS

RISK FACTORS	Management						Internet/Intranet						Enterprise Packaged Solutions					Client/Server Architecture						Workgroups and Groupware					Network Management					
Technology Concerns to Management (Gartner Group) ►	IT initiatives in line with business strategy	IT policies and corporate governance	Utilising IT for competitive advantage	Consolidating the IT infrastructure	Reducing cost of IT ownership	Acquiring and developing skills	Unauthorised access to corporate network	Unauthorised access to confidential messages	Loss of integrity — corporate transactions	Leakage of confidential data	Interruption to service availability	Virus infection	Failure to meet user requirements	Failure to integrate	Not compatible with technical infrastructure	Vendor support problems	Expensive/complex implementation	Failure to coordinate requirements	Access control problems	Not compatible with technical infrastructure	End user management problems	Control of software versions	High costs of ownership	Quality control	Access control	Informal procedures	Data integrity	Configuration control	Availability	Security	Configuration control	Incident management	Costs	Support and maintenance
PLANNING & ORGANISATION																																		
PO1 Define a Strategic IT Plan	●		●										●		●			●		●			●											
PO2 Define the Information Architecture	●	●	●	●			●	●	●	●				●	●				●	●			●		●		●			●			●	
PO3 Determine the Technological Direction	●	●	●	●							●			●	●		●			●			●						●				●	●
PO4 Define the IT Organisation and Relationships	●	●	●			●	●	●	●	●	●			●		●	●	●			●		●			●		●			●		●	●
PO5 Manage the Information Technology Investment		●			●												●						●										●	
PO6 Communicate Management Aims and Direction		●				●	●	●	●	●		●							●		●			●	●	●				●				
PO7 Manage Human Resources						●	●	●	●	●	●	●																		●				
PO8 Ensure Compliance with External Requirements		●					●	●	●	●									●						●	●				●				
PO9 Assess Risks		●	●				●	●	●	●									●						●					●				
PO10 Manage Projects	●												●	●	●		●	●		●	●		●	●	●								●	
PO11 Manage Quality																	●						●	●									●	
ACQUISITION & IMPLEMENTATION																																		
AI1 Identify Automated Solutions	●						●	●	●	●			●	●	●	●	●	●	●	●					●				●	●				
AI2 Acquire and Maintain Application Software							●	●	●	●	●		●	●			●					●		●	●		●	●	●	●	●		●	●
AI3 Acquire and Maintain Technology Infrastructure							●	●	●	●	●				●				●	●		●	●		●				●	●	●		●	●
AI4 Develop and Maintain Procedures						●					●										●		●			●		●	●			●	●	●
AI5 Install and Accredit Systems							●	●			●		●				●	●	●		●	●	●	●	●		●	●		●	●			●
AI6 Manage Changes					●						●		●				●	●				●	●					●	●	●	●	●	●	
DELIVERY & SUPPORT																																		
DS1 Define and Manage Service Levels	●			●							●					●	●						●						●				●	●
DS2 Manage Third-Party Services							●	●			●		●	●		●		●	●						●				●	●				●
DS3 Manage Performance and Capacity				●	●						●												●						●			●	●	●
DS4 Ensure Continuous Service		●									●												●						●					●
DS5 Ensure Systems Security		●					●	●	●	●	●	●			●		●		●	●					●		●			●		●	●	●
DS6 Identify and Allocate Costs					●												●																	
DS7 Educate and Train Users	●						●	●				●							●		●				●	●				●				
DS8 Assist and Advise Customers	●																				●		●			●							●	
DS9 Manage the Configuration					●							●										●	●				●	●		●	●		●	●
DS10 Manage Problems and Incidents					●												●						●									●	●	●
DS11 Manage Data					●		●	●	●	●	●								●		●		●	●	●	●	●		●	●				
DS12 Manage Facilities							●	●		●	●	●							●						●				●	●				
DS13 Manage Operations											●												●						●					
MONITORING																																		
M1 Monitor the Processes	●	●					●	●	●	●			●						●					●	●				●	●		●		●
M2 Assess Internal Control Adequacy		●					●	●	●	●	●	●							●			●		●	●		●	●	●	●		●		●
M3 Obtain Independent Assurance		●					●	●	●	●	●	●	●				●	●	●	●		●		●	●		●	●	●	●		●		●
M4 Provide for Independent Audit	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

IT GOVERNANCE INSTITUTE

IT CONTROL DIAGNOSTICS

IT Control Diagnostics

Prior Audit Work Form

In Prior Scope				Prior Audit						Disposition of Findings			
				Opinion									
Yes	No		IT Process	Unqualified	Qualifed	Adverse	Disclainer	Material Weaknesses	Findings	Resolved	Unresolved	N/A	Not Determined
		PO1	Define a Strategic IT Plan										
		PO2	Define the Information Architecture										
		PO3	Determine the Technological Direction										
		PO4	Define the IT Organisation and Relationships										
		PO5	Manage the Information Technology Investment										
		PO6	Communicate Management Aims and Direction										
		PO7	Manage Human Resources										
		PO8	Ensure Compliance with External Requirements										
		PO9	Assess Risks										
		PO10	Manage Projects										
		PO11	Manage Quality										
		AI1	Identify Automated Solutions										
		AI2	Acquire and Maintain Application Software										
		AI3	Acquire and Maintain Technology Infrastructure										
		AI4	Develop and Maintain Procedures										
		AI5	Install and Accredit Systems										
		AI6	Manage Changes										
		DS1	Define and Manage Service Levels										
		DS2	Manage Third-Party Services										
		DS3	Manage Performance and Capacity										
		DS4	Ensure Continuous Service										
		DS5	Ensure Systems Security										
		DS6	Identify and Allocate Costs										
		DS7	Educate and Train Users										
		DS8	Assist and Advise Customers										
		DS9	Manage the Configuration										
		DS10	Manage Problems and Incidents										
		DS11	Manage Data										
		DS12	Manage Facilities										
		DS13	Manage Operations										
		M1	Monitor the Processes										
		M2	Assess Internal Control Adequacy										
		M3	Obtain Independent Assurance										
		M4	Provide for Independent Audit										
			Insert the number of material weaknesses and/or findings if there is more than one per process category and then reflect the appropriate number under each column.										

ENTITY SHORT FORM

Importance					IT Process		Performance							
Very Important	Somewhat Important	Not Important	Not Sure	Not Applicable			Excellent	Very Good	Satisfactory	Poor	Not Sure	Formally Rated	Not Rated	Not Applicable
					PO1	Define a Strategic IT Plan								
					PO2	Define the Information Architecture								
					PO3	Determine the Technological Direction								
					PO4	Define the IT Organisation and Relationships								
					PO5	Manage the Information Technology Investment								
					PO6	Communicate Management Aims and Direction								
					PO7	Manage Human Resources								
					PO8	Ensure Compliance with External Requirements								
					PO9	Assess Risks								
					PO10	Manage Projects								
					PO11	Manage Quality								
					AI1	Identify Automated Solutions								
					AI2	Acquire and Maintain Application Software								
					AI3	Acquire and Maintain Technology Infrastructure								
					AI4	Develop and Maintain Procedures								
					AI5	Install and Accredit Systems								
					AI6	Manage Changes								
					DS1	Define and Manage Service Levels								
					DS2	Manage Third-Party Services								
					DS3	Manage Performance and Capacity								
					DS4	Ensure Continuous Service								
					DS5	Ensure Systems Security								
					DS6	Identify and Allocate Costs								
					DS7	Educate and Train Users								
					DS8	Assist and Advise Customers								
					DS9	Manage the Configuration								
					DS10	Manage Problems and Incidents								
					DS11	Manage Data								
					DS12	Manage Facilities								
					DS13	Manage Operations								
					M1	Monitor the Processes								
					M2	Assess Internal Control Adequacy								
					M3	Obtain Independent Assurance								
					M4	Provide for Independent Audit								

IT Control Diagnostics, *continued*

Entity Long Form

Importance							Performance								Internal Controls			WP Ref.
Very Important	Somewhat Important	Not Important	Not Sure	Not Applicable	IT Process		Excellent	Very Good	Satisfactory	Poor	Not Sure	Formally Rated	Not Rated	Not Applicable	Documented	Not Documented	Not Sure	
					PO1	Define a Strategic IT Plan												
					PO2	Define the Information Architecture												
					PO3	Determine the Technological Direction												
					PO4	Define the IT Organisation and Relationships												
					PO5	Manage the Information Technology Investment												
					PO6	Communicate Management Aims and Direction												
					PO7	Manage Human Resources												
					PO8	Ensure Compliance with External Requirements												
					PO9	Assess Risks												
					PO10	Manage Projects												
					PO11	Manage Quality												
					AI1	Identify Automated Solutions												
					AI2	Acquire and Maintain Application Software												
					AI3	Acquire and Maintain Technology Infrastructure												
					AI4	Develop and Maintain Procedures												
					AI5	Install and Accredit Systems												
					AI6	Manage Changes												
					DS1	Define and Manage Service Levels												
					DS2	Manage Third-Party Services												
					DS3	Manage Performance and Capacity												
					DS4	Ensure Continuous Service												
					DS5	Ensure Systems Security												
					DS6	Identify and Allocate Costs												
					DS7	Educate and Train Users												
					DS8	Assist and Advise Customers												
					DS9	Manage the Configuration												
					DS10	Manage Problems and Incidents												
					DS11	Manage Data												
					DS12	Manage Facilities												
					DS13	Manage Operations												
					M1	Monitor the Processes												
					M2	Assess Internal Control Adequacy												
					M3	Obtain Independent Assurance												
					M4	Provide for Independent Audit												

RISK ASSESSMENT FORM

Importance						Risk					Internal Controls			WP Ref.
Very Important	Somewhat Important	Not Important	Not Sure	IT Process		High	Medium	Low	Immaterial	Not Sure	Documented	Not Documented	Not Sure	
				PO1	Define a Strategic IT Plan									
				PO2	Define the Information Architecture									
				PO3	Determine the Technological Direction									
				PO4	Define the IT Organisation and Relationships									
				PO5	Manage the Information Technology Investment									
				PO6	Communicate Management Aims and Direction									
				PO7	Manage Human Resources									
				PO8	Ensure Compliance with External Requirements									
				PO9	Assess Risks									
				PO10	Manage Projects									
				PO11	Manage Quality									
				AI1	Identify Automated Solutions									
				AI2	Acquire and Maintain Application Software									
				AI3	Acquire and Maintain Technology Infrastructure									
				AI4	Develop and Maintain Procedures									
				AI5	Install and Accredit Systems									
				AI6	Manage Changes									
				DS1	Define and Manage Service Levels									
				DS2	Manage Third-Party Services									
				DS3	Manage Performance and Capacity									
				DS4	Ensure Continuous Service									
				DS5	Ensure Systems Security									
				DS6	Identify and Allocate Costs									
				DS7	Educate and Train Users									
				DS8	Assist and Advise Customers									
				DS9	Manage the Configuration									
				DS10	Manage Problems and Incidents									
				DS11	Manage Data									
				DS12	Manage Facilities									
				DS13	Manage Operations									
				M1	Monitor the Processes									
				M2	Assess Internal Control Adequacy									
				M3	Obtain Independent Assurance									
				M4	Provide for Independent Audit									

IT Control Diagnostics, *continued*

Responsible Party Form

Performed by (1)	IT Process		Primary Responsible Party
	PO1	Define a Strategic IT Plan	
	PO2	Define the Information Architecture	
	PO3	Determine the Technological Direction	
	PO4	Define the IT Organisation and Relationships	
	PO5	Manage the Information Technology Investment	
	PO6	Communicate Management Aims and Direction	
	PO7	Manage Human Resources	
	PO8	Ensure Compliance with External Requirements	
	PO9	Assess Risks	
	PO10	Manage Projects	
	PO11	Manage Quality	
	AI1	Identify Automated Solutions	
	AI2	Acquire and Maintain Application Software	
	AI3	Acquire and Maintain Technology Infrastructure	
	AI4	Develop and Maintain Procedures	
	AI5	Install and Accredit Systems	
	AI6	Manage Changes	
	DS1	Define and Manage Service Levels	
	DS2	Manage Third-Party Services	
	DS3	Manage Performance and Capacity	
	DS4	Ensure Continuous Service	
	DS5	Ensure Systems Security	
	DS6	Identify and Allocate Costs	
	DS7	Educate and Train Users	
	DS8	Assist and Advise Customers	
	DS9	Manage the Configuration	
	DS10	Manage Problems and Incidents	
	DS11	Manage Data	
	DS12	Manage Facilities	
	DS13	Manage Operations	
	M1	Monitor the Processes	
	M2	Assess Internal Control Adequacy	
	M3	Obtain Independent Assurance	
	M4	Provide for Independent Audit	

(1) Identify organisational units (IT department, within organisation, outsourced or not sure) which perform activities incorporated within the IT process.

CONTRACT SERVICE/SERVICE LEVEL AGREEMENT (SLA) FORM

Performed By				IT Process		Internal Controls			Formal Contract/SLA in place?					WP Ref.
IT Department	Within Organisation	Outsourced	Not Sure			Documented	Not Documented	Not Sure	Yes	No	Not Applicable	Not Sure		
				PO1	Define a Strategic IT Plan									
				PO2	Define the Information Architecture									
				PO3	Determine the Technological Direction									
				PO4	Define the IT Organisation and Relationships									
				PO5	Manage the Information Technology Investment									
				PO6	Communicate Management Aims and Direction									
				PO7	Manage Human Resources									
				PO8	Ensure Compliance with External Requirements									
				PO9	Assess Risks									
				PO10	Manage Projects									
				PO11	Manage Quality									
				AI1	Identify Automated Solutions									
				AI2	Acquire and Maintain Application Software									
				AI3	Acquire and Maintain Technology Infrastructure									
				AI4	Develop and Maintain Procedures									
				AI5	Install and Accredit Systems									
				AI6	Manage Changes									
				DS1	Define and Manage Service Levels									
				DS2	Manage Third-Party Services									
				DS3	Manage Performance and Capacity									
				DS4	Ensure Continuous Service									
				DS5	Ensure Systems Security									
				DS6	Identify and Allocate Costs									
				DS7	Educate and Train Users									
				DS8	Assist and Advise Customers									
				DS9	Manage the Configuration									
				DS10	Manage Problems and Incidents									
				DS11	Manage Data									
				DS12	Manage Facilities									
				DS13	Manage Operations									
				M1	Monitor the Processes									
				M2	Assess Internal Control Adequacy									
				M3	Obtain Independent Assurance									
				M4	Provide for Independent Audit									

This page intentionally left blank

COBIT CASE STUDIES

MICHAEL P. RAS, CISA, SENIOR IT AUDIT MANAGER
CEDEL GROUP
LUXEMBOURG

ABSTRACT

Tremendous change in the way Cedel Group does business created a need to review controls and update policy statements. Successful COBIT implementation has been a team effort among senior management, IT and end users. Business objectives are tied in closely with audit and control policies, as business leaders receive added value from IT audit and control activities.

BACKGROUND

Created as a clearing organisation in 1970 by 66 of the world's major financial institutions, Cedel Group minimises risk in the settlement of cross-border securities trading, particularly in the growing Eurobond market. It has more than 800 employees in Luxembourg, Dubai, Hong Kong, London, New York and Tokyo and links have been established to the securities markets of more than 30 countries. Settlement turnover for 1997 exceeded US $15 trillion and Cedel Bank holds US $1.4 trillion of customers' securities in safekeeping. Growing international business has resulted in trades worth up to US $100 billion being settled in an average business day.

While our previous IT environment was stable, reliable and met business needs, change was needed to maintain a controlled environment. In the late 1980s we experienced a growth of major new business opportunities, sophisticated IT demands, the development of new client/server applications, and dramatic changes in the PC and telecommunications network environments.

While the Cedel Group System Policy Statements remained applicable and enforced, situations increasingly arose where the methods stipulated to meet the control requirements were not appropriate in the new environment. For example, the policy associated with the previous DOS/Novell environment required that a control exist to prevent a user from signing onto the system more than once at the same time. This now prevented a user from accessing the system from a contingency site if the user was unable to sign-off from the normal work place. Waiver and change requests to policy requirements were becoming commonplace.

PROCESS

Faced with the challenge of developing and maintaining control policies that applied to significant technological, environmental and process changes, we used the opportunity to examine the IT audit approach. Several alternative methodologies were reviewed, and the most appropriate was found to be COBIT.

We began implementing COBIT in 1996 by applying the framework to an audit, which was subsequently successfully carried out.

Our IT department was prompted by the audit results to independently look at COBIT as the framework for a new set of Cedel Group Policy Statements. The director of processing and communications, who chaired this review, stated, "COBIT presented its control objectives in a new and logical manner which is practical to implement."

The results of a complete COBIT review of the Cedel policies have been encouraging. The new policies being generated apply to all technical platforms. Plus senior management is becoming more risk and control conscious. The traditional conflict between meeting business objectives and managing control requirements is becoming less of an issue as managers frequently acknowledge the business benefits of controls.

CONCLUSION

A new, strong focus on practical business and efficiency priorities was the most notable difference when we implemented COBIT. Following its principles, we now establish audits based on the auditees' own business and operating objectives. Audits are now approached from the top, rather than from the middle downwards. The introduction of COBIT has proved to be an extremely effective audit method and senior management has found that audits add value to the business.

Based on our organisation's success with implementing COBIT, I encourage colleagues to take a close look at COBIT with their respective IT management. COBIT is a highly flexible and credible approach to maintaining and improving a controlled environment for the benefit of all involved in the industry.

John Beveridge, CISA
Office of the State Auditor of Massachusetts
United States

ABSTRACT
The Office of the State Auditor is the principal governmental audit entity for state government in Massachusetts. We have used CobiT extensively in audit selection, on individual engagements and for substantiating results. CobiT assists our teams in identifying IT audits and framing them to one or more domains or sets of control objectives.

BACKGROUND
Our audits provide the governor, legislature, auditees, oversight entities and the public with an independent evaluation of state functions and activities. The IT audit division performs integrated, financial-related, operational and IT audits in a multi-platform environment which includes 20 large data centers and more than 150 small to medium facilities in more than 600 audit entities.

PROCESS
Our IT audit management team used a phased approach where some members of our IT audit staff were introduced to the *Framework*, *Control Objectives* and *Audit Guidelines* for use on their audits. The team selected audits where IT facility examinations would be included in the scope and for a system under development audit of a particular application system.

Once the management team and selected senior auditors were familiar enough with CobiT to assist other staff, the entire IT audit staff was given a two-day training session on the control model and related products. Using CobiT on a pilot basis provided an excellent insight into its application and appropriate experiences upon which to develop the training.

In pre-audit work CobiT helps identify high risk IT processes and assess the IT control environment. By reviewing organisational and IT policies against CobiT's high-level and detailed control objectives, the team quickly focuses on areas to be included in the audit scope or potential management advisory services work. During pre-audits, our team uses the CobiT framework and control objectives to facilitate interview discussions. Identification of data and information requirements and sources are referenced to CobiT's business requirements for information. This assists audit teams and auditees in discussions on control objectives and control policy, procedures and standards.

CobiT's focus on control objectives and their related purpose to the business organisation has supported audit management's efforts to move away from checklist auditing. We continue to strengthen our audit planning process and understanding of fundamental control objectives for IT by implementing CobiT's principles.

CONCLUSION
At the start of the engagement, the audit team references CobiT during entrance conferences as one of their primary audit criteria. It is an authoritative source that lends credibility to the review criteria, and when shared with the auditee, provides excellent opportunities for constructive audit work. This has helped auditees understand the basis of the review from the start. Furthermore, our team found that CobiT's use dovetails with the Committee of Sponsoring Organisations (COSO) and current changes to auditing standards (e.g., implementation of SAS 70 and 78). CobiT's audit guidelines also can be used to develop audit work programs.

CobiT also is useful in helping auditees evaluate and strengthen internal controls. There is a tremendous benefit for them to be better prepared for upcoming audits. Being aware of the review criteria means that auditees are aware of the control practices recommended for the IT processes. CobiT's organisation makes it easy for the auditee to relate to and interpret auditors' requests for information and subsequent recommendations.

Our experience with CobiT also has assisted entry level auditors gain an understanding of IT processes and detailed control objectives, and to frame that to the auditee organisation and IT environment. By implementing CobiT we identified the need to enhance and amend generic audit guidelines, audit procedure manuals and quality assurance reviews.

Across the board we have achieved increased consistency of discussions regarding IT domains, control objectives and IT controls.

AD VAN NIJNATTEN, PARTNER, EDP AUDIT, THE NETHERLANDS
EDDY SCHUERMANS, CISA, PARTNER, ASSURANCE SERVICES, BELGIUM
RENE BARLAGE, EDP AUDITOR
PRICEWATERHOUSECOOPERS

ABSTRACT

PricewaterhouseCoopers in the Netherlands has 100 EDP auditors in computer assurance services, many who already have in depth knowledge of COBIT and are putting it to use for clients. For many clients we use the following phased approach:

- Focus. Identify business drivers for IT and assess the level of business risks involved with the deployment of IT.
- Evaluate. Assess threats and vulnerabilities, identify lacking or inadequate control measures and determine root causes.
- Address control deficiencies. Agree upon action plans and apply internal control improvements.
- Monitor. Ensure continuous improvement through the implementation of adequate monitoring of the internal control measures put in place.

BACKGROUND

We have implemented COBIT for several PricewaterhouseCoopers clients and are strong supporters of the framework. Our staff use it to develop improvement programs for client IT departments. The detailed control objectives help us better assess client systems management processes.

PROCESS

Examples of how COBIT was successfully used in business situations include:

Airline company. The client asked us to measure effectiveness and efficiency of their IT department. We first measured user satisfaction and, after analysing the findings, performed a detailed review of IT processes based on COBIT guidance. As a result, procedures in the IT department were significantly improved.

Network services supplier. A network provider implemented systems management based on ITIL. We were asked to perform a third party review and report the results to clients of the provider. Our staff used the COBIT framework to perform the audit.

Not-for-Profit. Based on COBIT's principles and ITIL we conducted an improvement program for the IT department.

Chamber of Commerce. Several mergers and significant business changes had affected the organisation's IT environment. We used the COBIT framework to implement an appropriate improvement program.

Bank. A Dutch bank asked us to document baseline controls for several platforms. We described baseline controls for RS/6000, Windows NT servers and several network components. For the systems management part of the baseline controls we consulted the detailed control objectives from COBIT.

CONCLUSION

A unique benefit of COBIT is that Information Technology Infrastructure Library (ITIL) is one of the global standards on which COBIT is based. Developed in the UK, ITIL is popular in many countries. In the Netherlands, auditors who are members of ITIMF.EDP, an ITIL user group, frequently are asked to audit IT processes created using ITIL publications. COBIT provides an excellent framework to perform these audits.

Pratap Oak, Senior Information Technology Auditor
Jay Stott, Vice President, Information Technology Audit
Fidelity Investments
Boston, Massachusetts, USA

ABSTRACT
Since Fidelity Investments, an investment management organisation based in Boston, MA, adopted CobiT, audit work has become extremely consistent and control self-assessments are now feasible.

BACKGROUND
Fidelity has 24,000 employees in 70 cities in the US, Canada, Europe, Australia and Asia. Customer assets total approximately US $905 billion.

The CobiT framework can proactively improve the control environment and provide value-added services. It directly addresses the challenge faced by our CIO and other executives in support of the overall business objectives by continually improving IT systems. As a result of senior management's support and encouragement for continuous improvement, we have 'CobiT-ised' the audit process in a relatively short period of time.

We have accomplished more audits with fewer resources and have improved coordination with other audit groups, risk evaluations, audit planning, audit scoping and communication of audit issues. One of the most important benefits we obtained by using CobiT is the satisfaction of performing quality work.

PROCESS
Previously the challenge to mitigate IT risks was handled with best practices and related methodologies. Our managers strongly support continual improvements and quickly recognised that CobiT provided a generally applicable and accepted standard for IT governance control. CobiT has moved the process forward by offering a baseline of IT controls that relate directly to Fidelity's business objectives.

In 1996 we conducted a review using the CobiT framework and confirmed its usefulness. In 1997 we created a database of CobiT domains, processes and control objectives/elements. Then we mapped the CobiT database to the various types of audits we perform.

Many positive changes resulted from this effort. Audit programs and work paper documentation were updated based on the framework. CobiT was incorporated into our mission statement. Engagement memos now explain how the framework is used, and copies of the framework are made available to auditees to help them better prepare for and understand the benefits of the audit.

CONCLUSION
By implementing CobiT, we have incorporated a comprehensive body of knowledge about controls into our audits. CobiT provides the authoritative baseline of IT controls and helps ensure complete, efficient and consistent coverage of the IT control environment.

Going forward, we plan to use CobiT for control self-assessment reviews and for further tightening the control environment. It provides a basis for better metrics on the state of the IT control environment and is flexible enough to support our objectives through the many changes ahead.

CHRISTIAN HENDRICKS
DEPARTMENT OF DEFENSE
UNITED STATES

ABSTRACT

The Office of the Inspector General (OIG) of the US Department of Defense uses COBIT as a standard to define the IT auditable area. COBIT is written in a way the IT community can understand and adhere to. As a result, strategic plans can be prepared that ensure effective audit coverage. This case study details how COBIT was implemented to perform strategic planning of IT, establish a basis to evaluate its auditors' skills and select the best IT training courses.

BACKGROUND

COBIT's domain and process framework presents control activities in a manageable and definable structure. For each of the four domains, control objectives are assessed based on the timing presented in the OIG strategic plan. Our long range goal is to cover each control objective in the domains.

PROCESS

Audits are planned using the control objectives as criteria. Detailed audit procedures are developed based on several areas including government requirements and use of computer assisted audit techniques. Because auditors working in IT need specialised expertise, we use COBIT to perform skills assessments and ensure that the audit can be accomplished successfully. Auditors rate their ability to work in the four COBIT domains and evaluate their ability to audit using the high-level control objectives. Each auditor's education, training and experience in IT is characterised based on these three skill sets:

Basic Understanding: Broad knowledge of an IT process, purpose, objectives and goals.

Working Knowledge: Demonstrated ability to identify internal control strengths and weaknesses within an IT process.

Expert Knowledge: Ability to design and use computer assisted audit techniques to identify, evaluate and correct internal control weaknesses.

To evaluate training opportunities, we maintain a database of courses based on their ability to provide a skill set that supports a COBIT domain and control objective. Other factors such as course cost, schedule and performance are considered also. Based on the COBIT course assessment, we can select the best course at the right time.

CONCLUSION

COBIT provides a framework, which the IT community can understand and adhere to. As a result, strategic audit plans can be prepared that ensure effective audit coverage. Furthermore, using the control objectives as a basis for assessing IT audit and auditor skill requirements, effective and timely training can be provided to ensure that the audit can be performed successfully.

John Beveridge, CISA
for
Boston Gas Company
USA

ABSTRACT
CobiT was carefully studied to learn its benefits and determine how it would most benefit Boston Gas. Consistent with the Internal Audit department's strategy to provide value-added auditing services, CobiT has served as a benchmark for best practices of control and criteria for review.

BACKGROUND
Boston Gas Company, a public utility, employs 1,400 and generates US $700 million per year. It serves 74 cities and towns in the greater Boston, MA, USA, area. Its IT environment is primarily driven by IBM mainframe, UNIX, Novell and NT platforms and networks.

PROCESS
The Internal Audit Manager and an IS auditor obtained CobiT when it was published in 1996 and soon after participated in a CobiT presentation sponsored by the New England Chapter of ISACA.

Convinced that CobiT could benefit Boston Gas in developing IT related policies and procedures and performing IT audits, the managers introduced CobiT's principles to the Vice President of IS and members of the IS staff. As a result of this presentation, several customised, successful uses of CobiT were identified, including:

- The Director of Internal Audit indicated that the department would adopt CobiT as a review standard so goal posts for review would be clearly communicated.
- The IS department adopted CobiT as a benchmark and set of control objectives and guidelines against which to measure current and future IS functions and projects.

CONCLUSION
The success of introducing CobiT and having Internal Audit and the IT departments adopt it rested on their becoming familiar with the control framework, obtaining training and focusing their time on implementing its principles. CobiT has provided added value to the utility by focusing on the overall business objective while strengthening IT controls.

DAVID ABTS, EXECUTIVE VICE PRESIDENT, DIRECTOR OF MIS AND OPERATIONS
SANTA BARBARA BANK AND TRUST
SANTA BARBARA, CALIFORNIA, USA

ABSTRACT
The Santa Barbara Bank and Trust implemented COBIT to support our overall business objectives with effective IT governance.

BACKGROUND
We embraced the COBIT approach because it focuses on business needs. And first and foremost we are running a business. By implementing COBIT's principles, we have been able to keep our business objectives on track as we take the steps needed to ensure a controlled information systems environment.

PROCESS
Our IS auditors previously focused on auditing computer systems or code. After implementing COBIT's principles, they audit according to the business processes, with audit scopes that are easily understood and supported by business managers. For example, where an audit formerly may have focused on 'control over NT,' now it will target 'loan application front-end processing.'

Instead of looking at IS audits as a business disruption, department managers now use the auditors' knowledge to add value and protection.

In one instance, managers assured auditors that unwanted outsiders could not gain access to internal computers through a corporate world wide web site. But the audit staff noticed there was e-mail capability and alerted managers that the e-mail system needed controls to reduce the chance of spam mail, which could jam the server.

CONCLUSION
As a result of COBIT implementation, cooperation between business managers and IS auditors increased and communication improved. The COBIT framework and its other components helped managers clearly comprehend how controls and security issues benefit their departments.

When department managers and IS auditors speak in the same business language, the audit process becomes a cooperative effort that benefits the whole bank.

Peter De Koninck, Senior Auditor, Brussels, Belgium
Erik Guldentops, Director, Global Information Security
Society for Worldwide Interbank Financial Telecommunication (S.W.I.F.T.) sc

ABSTRACT
The Society for Worldwide Interbank Financial Telecommunication (S.W.I.F.T.) used CobiT in an audit of its customer support centers located in the Netherlands, Singapore and United States. This was a 16 person-week audit effort.

BACKGROUND
S.W.I.F.T. is a Belgium-based cooperative owned by 2,465 banks for secure interbank financial messaging services and interface software. S.W.I.F.T.'s global network handles approximately 2.5 million messages daily with an average daily transaction total of US $2.3 trillion.

The S.W.I.F.T. customer support function had recently been re-engineered and new tools and processes were put in place. The audit plan provided room for auditing tools and processes. CobiT had been used to audit the processes, but not the tools.

PROCESS
At first management's reaction to the CobiT IT governance and control model was rather negative because of timing. But auditees often think that audits come at a bad time. During the audit, though, this attitude was reversed and the approach became well-accepted. This change was confirmed by senior management after they received the draft audit report.

Managers were particularly impressed by the process orientation which was used instead of the traditional way of focusing on confidentiality/integrity/availability. The most apparent outcome of the CobiT approach is the logical set-up and sequence of interviews which make the process more efficient because auditors build their knowledge in an appropriate order.

It had taken lengthy discussions to obtain senior and line management approval of the audit scope because the CobiT framework was leading an investigation into previously untapped areas. Managers questioned the audit team's ability to perform an objective audit in these new fields. The department previously only looked at IT security issues, with security broadly defined. The CobiT approach focused on management of the process and process control issues.

We constructed a matrix using the CobiT control objectives. A risk assessment helped us determine which objectives would be verified during the audit. We then cross-checked the objectives withheld for the audit with (a) scopes from previous audits, (b) industry standards and (c) checklists provided by external auditors.

Based on the matrix, we constructed the audit program. The CobiT framework enabled us to prioritise audit activities and areas under review, using the primary/secondary ratings provided by CobiT.

CONCLUSION
Implementing the CobiT framework in this comprehensive audit was a major change for auditors and management. While change often creates adversity and criticism, the process orientation was quickly appreciated by management, and the auditors are planning to use it again.

CobiT will be used more and more in future audits, certainly now that the Audit Committee has ratified it as the IT audit reference. It is certainly being regarded as a good basis for SAS70-type reviews. In parallel, CobiT has also found its way into the IT organisation of the enterprise. After the CIO, upon coming across the *Framework* by accident, ordered it for all the Service IT Managers. It lifted his ideas and plans for moving the IT organisation towards increased measurability and process excellence.

CobiT is also finding immediate and practical use. When looking for input on defining the mission and objectives for a new systems planning group, the CIO came to me and said, "Give me your CobiT Detailed Objectives to help do this!" I only had to point him to the PO1 through PO5 sections. He had asked me for input on this mission and objectives previously, so why hadn't I thought of this myself?

COBIT FAQS

1. WHAT IS THE PURPOSE OF COBIT?

The purpose of COBIT is to provide management and business process owners with an Information Technology (IT) governance model that helps in understanding and managing the risks associated with IT. COBIT helps bridge the gaps between business risks, control needs and technical issues. It is a control model to meet the needs of IT governance and ensure the integrity of information and information systems.

2. WHO IS USING COBIT?

COBIT is being used by those who have the primary responsibilities for business processes and technology, those who depend on technology for relevant and reliable information, and those providing quality, reliability and control of information technology.

3. WHO ARE THE PROCESS OWNERS?

COBIT is business process oriented and therefore addresses itself in the first place to the owners of these processes. Referring to Porter's Generic Business Model we are talking about core processes (procurement, operations, marketing, sales, etc.) as well as support processes (human resources, administration, information technology, etc.). As a consequence, COBIT is not only to be applied by the IT department, but by the business as a whole.

The above approach stems from the fact that in today's enterprises, the process owners are responsible for the performance of their processes, of which IT has become an integral part. In other words, they are empowered but also accountable. As a consequence, the business process owners bear the final responsibility for the information technology as deployed within the confines of their business process. Of course, they will make use of services provided by specialised parties like the traditional IT department or the third party service provider.

COBIT provides the business process owners with a framework, which should enable them to control all the different activities underlying IT deployment. As a result, on this basis they can gain reasonable assurance that IT will contribute to the achievement of their business objectives. Moreover, COBIT provides the business process owners with a generic communication framework to facilitate understanding and clarity among the different parties involved in the delivery of IT services.

Furthermore, the addition of the *Management Guidelines* in the 3rd Edition provides management with a set of tools that allow self-assessment in order to make choices for control implementation and improvements over IT, and measure the achievement of goals and the proper performance of IT processes. The *Management Guidelines* include maturity models, critical success factors, key goal indicators and key performance indicators to support managerial decision making.

4. WHY WAS THE ORIENTATION OF COBIT FOCUSSED ON THE PROCESS RATHER THAN FUNCTIONS OR APPLICATIONS?

The COBIT framework has been structured into 34 IT processes clustering interrelated life-cycle activities or interrelated discrete tasks. The process model was preferred for several reasons. Firstly, a process by its nature is result oriented in the way that it focuses on the final outcome while optimising the use of resources. The way these resources are physically structured, e.g., people/skills in departments, is less relevant in this perspective. Secondly, a process, and especially its objectives, is more permanent in nature and doesn't risk change as often as an organisational entity. Thirdly, the deployment of IT cannot be confined to a particular department and involves users and management as well as IT specialists. In this context, the IT process remains nevertheless the common denominator. As far as applications are concerned, they are treated within the COBIT framework as one of the five resource categories. Hence they are to be managed and controlled in such a way as to bring about the required information at the business process level. This way, application systems are an integral part of the COBIT framework and can be addressed specifically through the resource vantage point. In other words, focusing strictly on the resources only, one would automatically get an applications view of the COBIT objectives.

CobiT FAQs, *continued*

5. HOW ROBUST ARE THE BUSINESS REQUIREMENTS?

During the review process of CobiT, senior managers and CIO's liked the definition of the business requirements for information, and supported the choices about which requirements were most important in what process. Choices were difficult and entailed considerable debate among the experts during the project. The guiding principle has always been: What really is fundamental for this Control Objective in this process? Which resource needs special control? Which information requirement needs special attention?

6. WHAT IS THE OVERALL QUALITY OF CobiT, AND WERE THERE ANY PROCESS OWNERS/EXECUTIVES THAT WERE PART OF THE EXPERT REVIEW?

In order to assure the final quality of CobiT, several measures have been taken. The most important are:

i. The whole research process has been governed by the CobiT Steering Committee (CSC). Besides preconceiving the deliverables, the CSC has also been responsible for the final quality of these deliverables.

ii. The detailed research results have been quality controlled throughout.

iii. The preliminary research results, as well as the framework, have been exposed to two groups of experts including business managers.

iv. Before issuing the final texts they have been distributed to a number of specialists for comments.

The *Management Guidelines* were developed by a world-wide panel consisting of 40 security and control experts, IT management and performance management professionals, industry analysts and academics who participated in a residential workshop conducted by professional facilitators. The workshop deliverables went through a quality assurance process and were exposed for review. However, it needs to be emphasized that these guidelines remain generic, generally applicable and do not provide industry specific norms. Organisations will in many cases need to customise this general set of directions to their own environment.

Overall, experience shows that the CobiT model appeals to business management as a whole and that they appreciate the added value of it in view of improving their control over IT. In this regard, we are confident that the required quality level, beyond customer satisfaction, has been achieved.

7. WHAT IS THE FUTURE DIRECTION OF CobiT?

As with any comprehensive and groundbreaking research, CobiT will be updated every 3 years. This will ensure that the model and the framework remain comprehensive and valid. The validation will also entail ensuring that the 41 primary reference materials have not changed, and, if they have, to reflect that in the document.

8. HOW DID ISACF/A DECIDE ON THE LIST OF PRIMARY REFERENCES?

The list of primary references was developed as a collective consensus based on the experience of the professionals who participated in the CobiT Steering Committee's research, expert review and quality assurance efforts.

9. CAN I USE CobiT AS A STATEMENT OF CRITERIA FOR SPECIFIC AUDIT CONCLUSIONS?

Yes, basing the Audit Guidelines firmly on the Control Objectives takes the auditor's opinion out of the audit conclusion, replacing it with authoritative criteria. CobiT is based on 41 standards and best practices documents for Information Technology from standards setting bodies (both public and private) world-wide. These include documents from Europe, Canada, Australia, Japan and the United States. Because CobiT contains all pertinent worldwide standards identifiable at the time, it is all-inclusive with respect to IT controls standards. As a result, CobiT can be used as an authoritative source reference document, providing IT controls criteria on audits.

10. ARE THE CONTROL OBJECTIVES MEANT TO BE A MINIMUM LEVEL OF CONTROL OR BEST PRACTICE?

They are both minimum levels of control and best practice, because we are still at the level of control objectives, not yet at the control guidelines or control practices level. This will be addressed by further phases of the CobiT project, where the environment of the enterprise, the specific business objectives, the level of security at which one wants to achieve, the degree of risk one wants to accept, etc., will all determine how the control objectives for a process will be translated into the right level of control.

Because all of these choices are not self-evident, and because the control selection process can be onerous and time consuming, standard minimum security and control levels certainly should be developed and promoted.

11. WHAT ABOUT THE ABSENCE OF PLATFORM SPECIFIC CONTROLS?

The CobiT control objectives are generic in nature and are addressing activities or tasks within IT processes. This way they are platform independent on the one hand. On the other hand, however, they are the overall structure wherein more specific platform related controls are to be defined. In fact, the general control objectives should remain valid regardless of whether one is con-trolling for example a mainframe platform or an office automation platform. It is obvious that certain aspects will require more emphasis in a given environment.

12. WHERE ARE THE APPLICATION CONTROLS?

The application controls have been fully integrated in the CobiT model. This option has been taken considering that CobiT is business process oriented and that at this level application controls are merely part of the overall controls to be exercised over information systems and related technology. In most cases however this part cannot be outsourced. Hence the question “Where are the application controls?” is of prime importance.

Application systems and data are treated within the CobiT framework as two of the five resource categories. They are to deliver the required information at the business process level. This way application systems and data are an integral part of the CobiT framework and can be addressed specifically through the resource vantage point. In doing this, one will notice that many CobiT processes address the application controls and continue this through the entire whole lifecycle, from conception to operations.

Besides the overall resource view, there is one process “Manage data” where the traditional transactions and file controls can be found. Nevertheless one should consider that these controls on their own do not suffice anymore to effectively control application systems and data.

When integrating CobiT in one’s organisation, the above elements have to be taken into account. In this regard, it is required to add platform specific controls to the generic control objectives. Platforms should be interpreted widely in this sense, (e.g., office automation, telecommunications, data warehouse, etc.). The CobiT processes which are to be revisited in this regard, are those related to the “technology” resource category.

13. WHY IS THERE OVERLAP WITHIN THE CONTROL OBJECTIVES?

Overlap in the Control Objectives, although not occurring very often, was intentional. Some control objectives transcend domains and processes and therefore must be repeated to ensure that they exist in each domain or process. Some control objectives are meant to be crosschecks of one another and therefore must be repeated to ensure consistent application in more than one domain or process. Thus, although perceived as overlapping, CobiT intentionally repeats some control objectives in order to ensure appropriate coverage of these IT controls.

CobiT FAQs, *continued*

14. ARE THE CONTROL OBJECTIVES LINKED TO THE AUDIT GUIDELINES AND TO WHAT DEGREE?

Objectives have been developed from a process orientation because management is looking for pro-active advice on how to address the issue of keeping IT under control. Balancing cost and risk is the next issue to address (i.e., making a conscious choice of how and whether to implement each control objective). Future CobiT products will thoroughly address this choice, even though the pro-active principle remains - control objectives should be applied in the first place to achieve an information control criteria (effectiveness, efficiency, confidentiality, availability, integrity, compliance and reliability). The link is the process. The control objectives help management establish control over the process, the audit guidelines assist the auditor or assessor by providing assurance that the process is actually under control such that the information requirements necessary to achieve business objectives will be satisfied. In reference to the control framework represented by the waterfall model, the audit guidelines can be seen as providing the feedback from the control processes back to the business objectives. The control objectives are the guide going down the waterfall to get the IT process under control. The audit guidelines are the guide for going back up the waterfall with the question: "Is there assurance that the business objective will be achieved? Sometimes audit guidelines are straight translations from the control objectives; more often the guidelines look for evidence that the process is under control.

15. WHY ARE THERE NOT ANY RISK STATEMENTS WITH THE CONTROL OBJECTIVES?

The provision of risk statements was seriously considered and investigated during the research and review phase of the initial CobiT project, but not retained because management preferred the pro-active approach (objects are to be achieved) over the reactive approach (risks are to be mitigated). The risk approach comes in at the end of the audit guidelines when the risk of not implementing the controls is substantiated. In the application of CobiT, the risk approach is certainly useful when management decides which controls to implement or when auditors decide which control objectives to review. Both of these decisions depend entirely on the risk environment.

16. WHAT TRAINING IS AVAILABLE FOR THE USE OF CobiT?

Through the International Headquarters of ISACA, there are one- to two-day training sessions in the fundamentals of CobiT and its use by management and auditors or evaluators. The training covers the CobiT framework, definitions, control objectives, audit guidelines, case studies, and successful implementation approaches. Training can be tailored as the executive management, users or evaluators would like. Furthermore, ISACA has prepared slide presentations for providing awareness of CobiT, its framework, definitions, control objectives and audit guidelines (included in this package). ISACA also provides one-day and two-day CobiT courses throughout the year. ISACA can tailor presentations to the requirements of any organisation and the level of detail required.

17. WHO IN MY ORGANISATION SHOULD GO TO THE TRAINING?

CobiT training should be attended by management, IS and audit managers, IT professionals, business process managers, and quality assurance and audit professionals.

18. WHAT IS THE LEVEL OF TRAINING REQUIRED?

The amount and level of training necessary is a function of how comfortable one feels with the product. For those entities that are more proactive, and that have a well-defined relationship with their IT department, the training could simply be fulfilled by utilising the CobiT Implementation Tool Set. However, for those entities where things are not as well defined, it is strongly encouraged that those from Management, IT and Audit attend an ISACA one-day session. These are available through the International Office or local chapters throughout the world.

19. WHY ARE THERE DIFFERENCES BETWEEN THE DETAILED CONTROL OBJECTIVES AND CONTROL CONSIDERATIONS?

Control objectives focus on specific detailed control objectives associated with each IT process. They are defined based on a number of sources, comprising de facto and de jure international standards relating to control over IT that provide the view of the control specialist. The control considerations, as updated in the 3rd Edition of CobiT, provide management's view and are aligned with the critical success factors for control included in the *Management Guidelines*.

20. IN WHAT WAY CAN I SUGGEST TO IT MANAGEMENT THAT THEY USE CobiT?

Because CobiT is business oriented, using it to understand IT control objectives in order to manage IT related business risks is straightforward:

1. Start with your business objectives in the *Framework*
2. Select the IT processes and control objectives appropriate to your enterprise from the *Control Objectives*
3. Operate from your business plan
4. Assess your procedures and results with the *Audit Guidelines*
5. Assess the status of your organisation, identify critical activities leading to success and measure performance in reaching enterprise goals with the *Management Guidelines*.

21. IS THE CobiT FRAMEWORK SUPERIOR TO THE OTHER ACCEPTED CONTROL MODELS?

Most senior managers are aware of the importance of the general control frameworks with respect to their fiduciary responsibility, such as COSO, Cadbury, COCO or King; however they may not necessarily be aware of the details of each. In addition, management is increasingly aware of the more technical security guidance such as, OECD and IFAC IT statements at the high level, and DTI Code of Practices at the detailed level. Although the aforementioned models emphasise business control and IT security issues, only CobiT attempts to deal with IT specific control issues from a business perspective. It should be noted that COSO was used as source material for the business model. Lastly, CobiT is not meant to replace any of these control models. It is intended to provide more detail in the IT environment while building on the strengths of these control models.

22. WHAT IS THE QUICKEST AND BEST WAY TO SELL CobiT TO IT MANAGERS?

As we all know, there is no cavalry to come to the rescue. As the rest of the Implementation Tools point out, the organisational culture is vitally important. A proactive culture will be more receptive than one that is not. However, consider emphasising the business aspects and the fact that CobiT does not get lost in technical terminology. Furthermore, point out that CobiT was designed the way an IT manager thinks, and that one of its greatest benefits is that everything is documented in one place.

Furthermore, with the addition of the *Management Guidelines*, CobiT provides management with new capabilities to support self-assessment of organizational status, comparison with industry best practices, alignment with enterprise objectives, implementation decision making and performance monitoring. The maturity models, critical success factors, key goal indicators and key performance indicators provided in these guidelines can assist management in better aligning IT with the overall enterprise strategy by ensuring that IT is an enabler of the enterprise goals.

CobiT FAQs, *continued*

23. SINCE CobiT CURRENTLY DOES NOT ADDRESS ASSOCIATED BUSINESS RISKS, BUT RATHER THE MORE PROACTIVE CONTROL STATEMENTS TO BE ACHIEVED, IS THERE ANY CONSIDERATION BEING GIVEN TO ADDRESS THE PERCEIVED NEED OF RISK IDENTIFICATION?

Risk is addressed in a pervasive manner throughout CobiT and even more so with the advent of the *Management Guidelines* in the 3rd Edition. A major driver of the control and assurance processes is the IT Governance model that is now covered extensively in CobiT and the *Management Guidelines* framework. IT governance refers to the generic enterprise objectives of measuring benefits and managing risk. The same idea, risk management as an enterprise objective, was nevertheless already captured by CobiT earlier, because CobiT states that IT needs to provide information to the enterprise that must have the required characteristics in order to enable the achievement of enterprise objectives. While the security related criteria of availability, integrity and confidentiality may be more readily associated with risk, not achieving enterprise objectives or not providing the required criteria is a risk that the enterprise needs to control.

Specific examples have been provided in the 'substantiating' section of the *Audit Guidelines*. The objective of that section is to document for management what can or has happened as a result of not having effective control in place. More practically, one entire process was defined to cover the assessment of risk. (See PO9 - Assess Risk.)

In conclusion, risk is addressed in the *Framework* in a proactive manner, i.e., by focussing on objectives, because the primary risk that needs to be managed is that of not achieving the objectives. Second, the 'substantiating' section of the *Audit Guidelines* provides examples of these risks for each process. This provides for the risk information that the control and assurance professional is looking for. Finally, a whole IT process is dedicated to the assessment of risk in the overall set of IT objectives.

24. HAS CobiT AND ITS FRAMEWORK BEEN ACCEPTED BY CIO'S?

Yes, it has been accepted in many organisations globally, and new cases continue to be documented. However, it should not surprise anyone that in those entities where the CIO has embraced CobiT as a usable IT framework, this has come as a direct consequence of one or more CobiT Champions within the Audit and/or IT Department(s).

The addition of the *Management Guidelines* should also increase the acceptance of CobiT by both enterprise and IT management. The emphasis on alignment of IT with enterprise goals, self-assessment and performance measurement will ensure that CobiT is seen not only as a control framework, but also as providing a set of tools for improving the effectiveness of information and IT resources. The integration of the *Management Guidelines* with the CobiT *Framework* and *Control Objectives* will provide additional emphasis for management to use CobiT as the authoritative, up-to-date and established model for IT control and governance.

25. HOW ARE THE NEW MANAGEMENT GUIDELINES INTEGRATED INTO THE CobiT FRAMEWORK?

Starting with the CobiT *Framework*, the application of international standards and guidelines, and research into best practices led to the development of the *Control Objectives*. *Audit Guidelines* were then developed to assess whether these *Control Objectives* are appropriately implemented. However, management needs a similar application of the *Framework* to allow self-assessment and choices to be made for control implementation and improvements over its information and related technology.

The *Management Guidelines* provide the tools to accomplish this. They were developed for each of the 34 high-level control objectives, with a process management and performance measurement perspective. Maturity models, critical success factors, key goal indicators and key performance indicators are provided by the guidelines to support management decision-making processes. The control considerations of the high-level

control objectives have been updated to reflect, without mapping one-to-one, the critical success factors of the control objective.

The development of the *Management Guidelines* took into consideration the need to support the requirements of:

- Enterprise and IT management, with a set of new process management tools, while realising the benefit of utilising an established, authoritative and up-to-date control framework, as represented by CobiT.
- The security and control professional, with a basis for leveraging and evolving existing control oriented processes to provide additional services and value in support of enterprise objectives.

The *Management Guidelines* assume little knowledge of control frameworks, in general, and CobiT, in particular, by enterprise and IT management. Yet, they use the same structure as the *Control Objectives* and the *Audit Guidelines* to support the needs of the security and control professional. Through both content and presentation format, there is appropriate differentiation, yet also integration and synergy in the CobiT 3rd Edition in order to support the needs of both the above audiences.

This page intentionally left blank

APPENDICES

This page intentionally left blank

IT GOVERNANCE MANAGEMENT GUIDELINE

The following Management Guideline and Maturity Model identify the Critical Success Factors (CSFs), Key Goal Indicators (KGIs), Key Performance Indicators (KPIs) and Maturity Model for **IT governance.** First, IT governance is defined, articulating the business need. Next, the information criteria related to IT governance are identified. The business need is measured by the KGIs and enabled by a control statement, leveraged by all the IT resources. The achievement of the enabling control statement is measured by the KPIs, which consider the CSFs. The Maturity Model is used to evaluate an organisation's level of achievement of IT governance—from Non-existent (the lowest level) to Initial/Ad Hoc, to Repeatable but Intuitive, to Defined Process, to Managed and Measurable, to Optimised (the highest level). To achieve the Optimised maturity level for IT governance, an organisation must be at least at the Optimised level for the Monitoring domain and at least at the Managed and Measurable level for all other domains.

(See the COBIT *Management Guidelines* for a thorough discussion of the use of these tools.)

IT Governance Management Guideline

Governance over information technology and its processes with the business goal of adding value, while balancing risk versus return

ensures delivery of information to the business that addresses the required Information Criteria and is measured by Key Goal Indicators

is enabled by *creating and maintaining a system of process and control excellence appropriate for the business that directs and monitors the business value delivery of IT*

considers Critical Success Factors that leverage all IT Resources and is measured by Key Performance Indicators

Critical Success Factors

- IT governance activities are integrated into the enterprise governance process and leadership behaviours
- IT governance focuses on the enterprise goals, strategic initiatives, the use of technology to enhance the business and on the availability of sufficient resources and capabilities to keep up with the business demands
- IT governance activities are defined with a clear purpose, documented and implemented, based on enterprise needs and with unambiguous accountabilities
- Management practices are implemented to increase efficient and optimal use of resources and increase the effectiveness of IT processes
- Organisational practices are established to enable: sound oversight; a control environment/culture; risk assessment as standard practice; degree of adherence to established standards; monitoring and follow up of control deficiencies and risks
- Control practices are defined to avoid breakdowns in internal control and oversight
- There is integration and smooth interoperability of the more complex IT processes such as problem, change and configuration management
- An audit committee is established to appoint and oversee an independent auditor, focusing on IT when driving audit plans, and review the results of audits and third-party reviews.

Information Criteria
effectiveness
efficiency
confidentiality
integrity
availability
compliance
reliability

IT Resources
people
applications
technology
facilities
data

Key Goal Indicators

- Enhanced performance and cost management
- Improved return on major IT investments
- Improved time to market
- Increased quality, innovation and risk management
- Appropriately integrated and standardised business processes
- Reaching new and satisfying existing customers
- Availability of appropriate bandwidth, computing power and IT delivery mechanisms
- Meeting requirements and expectations of the customer of the process on budget and on time
- Adherence to laws, regulations, industry standards and contractual commitments
- Transparency on risk taking and adherence to the agreed organisational risk profile
- Benchmarking comparisons of IT governance maturity
- Creation of new service delivery channels

Key Performance Indicators

- Improved cost-efficiency of IT processes (costs vs. deliverables)
- Increased number of IT action plans for process improvement initiatives
- Increased utilisation of IT infrastructure
- Increased satisfaction of stakeholders (survey and number of complaints)
- Improved staff productivity (number of deliverables) and morale (survey)
- Increased availability of knowledge and information for managing the enterprise
- Increased linkage between IT and enterprise governance
- Improved performance as measured by IT balanced scorecards

IT Governance Maturity Model

Governance over information technology and its processes with the business goal of adding value, while balancing risk versus return

0 Non-existent There is a complete lack of any recognisable IT governance process. The organisation has not even recognised that there is an issue to be addressed and hence there is no communication about the issue.

1 Initial / Ad Hoc There is evidence that the organisation has recognised that IT governance issues exist and need to be addressed. There are, however, no standardised processes, but instead there are ad hoc approaches applied on an individual or case-by-case basis. Management's approach is chaotic and there is only sporadic, non-consistent communication on issues and approaches to address them. There may be some acknowledgement of capturing the value of IT in outcome-oriented performance of related enterprise processes. There is no standard assessment process. IT monitoring is only implemented reactively to an incident that has caused some loss or embarrassment to the organisation.

2 Repeatable but Intuitive There is global awareness of IT governance issues. IT governance activities and performance indicators are under development, which include IT planning, delivery and monitoring processes. As part of this effort, IT governance activities are formally established into the organisation's change management process, with active senior management involvement and oversight. Selected IT processes are identified for improving and/or controlling core enterprise processes and are effectively planned and monitored as investments, and are derived within the context of a defined IT architectural framework. Management has identified basic IT governance measurements and assessment methods and techniques, however, the process has not been adopted across the organisation. There is no formal training and communication on governance standards and responsibilities are left to the individual. Individuals drive the governance processes within various IT projects and processes. Limited governance tools are chosen and implemented for gathering governance metrics, but may not be used to their full capacity due to a lack of expertise in their functionality.

3 Defined Process The need to act with respect to IT governance is understood and accepted. A baseline set of IT governance indicators is developed, where linkages between outcome measures and performance drivers are defined, documented and integrated into strategic and operational planning and monitoring processes. Procedures have been standardised, documented and implemented. Management has communicated standardised procedures and informal training is established. Performance indicators over all IT governance activities are being recorded and tracked, leading to enterprise-wide improvements. Although measurable, procedures are not sophisticated, but are the formalisation of existing practices. Tools are standardised, using currently available techniques. IT Balanced Business Scorecard ideas are being adopted by the organization. It is, however, left to the individual to get training, to follow the standards and to apply them. Root cause analysis is only occasionally applied. Most processes are monitored against some (baseline) metrics, but any deviation, while mostly being acted upon by individual initiative, would unlikely be detected by management. Nevertheless, overall accountability of key process performance is clear and management is rewarded based on key performance measures.

4 Managed and Measurable There is full understanding of IT governance issues at all levels, supported by formal training. There is a clear understanding of who the customer is and responsibilities are defined and monitored through service level agreements. Responsibilities are clear and process ownership is established. IT processes are aligned with the business and with the IT strategy. Improvement in IT processes is based primarily upon a quantitative understanding and it is possible to monitor and measure compliance with procedures and process metrics. All process stakeholders are aware of risks, the importance of IT and the opportunities it can offer. Management has defined tolerances under which processes must operate. Action is taken in many, but not all cases where processes appear not to be working effectively or

efficiently. Processes are occasionally improved and best internal practices are enforced. Root cause analysis is being standardised. Continuous improvement is beginning to be addressed. There is limited, primarily tactical, use of technology, based on mature techniques and enforced standard tools. There is involvement of all required internal domain experts. IT governance evolves into an enterprise-wide process. IT governance activities are becoming integrated with the enterprise governance process.

5 **Optimised** There is advanced and forward-looking understanding of IT governance issues and solutions. Training and communication is supported by leading-edge concepts and techniques. Processes have been refined to a level of external best practice, based on results of continuous improvement and maturity modeling with other organisations. The implementation of these policies has led to an organisation, people and processes that are quick to adapt and fully support IT governance requirements. All problems and deviations are root cause analysed and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimised manner to automate the workflow and provide tools to improve quality and effectiveness. The risks and returns of the IT processes are defined, balanced and communicated across the enterprise. External experts are leveraged and benchmarks are used for guidance. Monitoring, self-assessment and communication about governance expectations are pervasive within the organisation and there is optimal use of technology to support measurement, analysis, communication and training. Enterprise governance and IT governance are strategically linked, leveraging technology and human and financial resources to increase the competitive advantage of the enterprise.

COBIT PROJECT DESCRIPTION

The COBIT project continues to be supervised by a Project Steering Committee formed by international representatives from industry, academia, government and the security and control profession. The Project Steering Committee has been instrumental in the development of the COBIT *Framework* and in the application of the research results. International working groups were established for the purpose of quality assurance and expert review of the project's interim research and development deliverables. Overall project guidance is provided by the IT Governance Institute.

RESEARCH AND APPROACH FOR EARLIER DEVELOPMENT

Starting with the COBIT *Framework* defined in the 1st edition, the application of international standards and guidelines and research into best practices have led to the development of the control objectives. Audit guidelines were next developed to assess whether these control objectives are appropriately implemented.

Research for the 1st and 2nd editions included the collection and analysis of identified international sources and was carried out by teams in Europe (Free University of Amsterdam), the US (California Polytechnic University) and Australia (University of New South Wales). The researchers were charged with the compilation, review, assessment and appropriate incorporation of international technical standards, codes of conduct, quality standards, professional standards in auditing and industry practices and requirements, as they relate to the *Framework* and to individual control objectives. After collection and analysis, the researchers were challenged to examine each domain and process in depth and suggest new or modified control objectives applicable to that particular IT process. Consolidation of the results was performed by the COBIT Steering Committee and the Director of Research of ISACF.

RESEARCH AND APPROACH FOR THE 3RD EDITION

The COBIT 3rd Edition project consisted of developing the *Management Guidelines* and updating COBIT 2nd Edition based on new and revised international references.

Furthermore, the COBIT *Framework* was revised and enhanced to support increased management control, to introduce performance management and to further develop IT governance. In order to provide management with an application of the *Framework* so that it can assess and make choices for control implementation and improvements over its information and related technology, as well as measure performance, the *Management Guidelines* include Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators related to the *Control Objectives*.

Management Guidelines was developed by using a worldwide panel of 40 experts from industry, academia, government and the IT security and control profession. These experts participated in a residential workshop guided by professional facilitators and using development guidelines defined by the COBIT Steering Committee. The workshop was strongly supported by the Gartner Group and PricewaterhouseCoopers, who not only provided thought leadership but also sent several of their experts on control, performance management and information security. The results of the workshop were draft Maturity Models, Critical Success Factors, Key Goal Indicators and Key Performance Indicators for each of COBIT's 34 high-level control objectives. Quality assurance of the initial deliverables was conducted by the COBIT Steering Committee and the results were posted for exposure on the ISACA web site. The *Management Guidelines* document was finally prepared to offer a new management-oriented set of tools, while providing integration and consistency with the COBIT *Framework*.

The update to the *Control Objectives*, based on new and revised international references, was conducted by members of ISACA chapters, under the guidance of COBIT Steering Committee members. The intention was not to perform a global analysis of all material or a redevelopment of the *Control Objectives*, but to provide an incremental update process.

The results of the development of the *Management Guidelines* were then used to revise the COBIT *Framework*, especially the considerations, goals and enabler statements of the high-level control objectives.

COBIT PRIMARY REFERENCE MATERIAL

COSO: Committee of Sponsoring Organisations of the Treadway Commission. *Internal Control — Integrated Framework.* 2 Vols. American Institute of Certified Accountants, New Jersey, 1994.

OECD Guidelines: Organisation for Economic Co-operation and Development. *Guidelines for the Security of Information,* Paris, 1992.

DTI Code of Practice for Information Security Management: Department of Trade and Industry and British Standard Institute. *A Code of Practice for Information Security Management,* London, 1993, 1995.

ISO 9000-3: International Organisation for Standardisation. *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.

An Introduction to Computer Security: The NIST Handbook: NIST Special Publication 800-12, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1995.

ITIL IT Management Practices: Information Technology Infrastructure Library. Practices and guidelines developed by the Central Computer and Telecommunications Agency (CCTA), London, 1989.

IBAG Framework: Draft Framework from the Infosec Business Advisory Group to SOGIS (Senior Officials Group on Information Security, advising the European Commission), Brussels, 1994.

NSW Premier's Office Statements of Best Practices and Planning Information Management and Techniques: *Statements of Best Practice #1 through #6.* Premier's Department New South Wales, Government of New South Wales, Australia, 1990 through 1994.

Memorandum Dutch Central Bank: *Memorandum on the Reliability and Continuity of Electronic Data Processing in Banking.* De Nederlandsche Bank, Reprint from Quarterly Bulletin #3, Netherlands, 1998.

EDPAF Monograph #7, EDI: An Audit Approach: Jamison, Rodger. *EDI: An Audit Approach,* Monograph Series #7, Information Systems Audit and Control Foundation, Inc., Rolling Meadows, IL, April 1994.

PCIE (President's Council on Integrity and Efficiency) Model Framework: *A Model Framework for Management Over Automated Information Systems.* Prepared jointly by the President's Council on Management Improvement and the President's Council on Integrity and Efficiency, Washington, DC, 1987.

Japan Information Systems Auditing Standards: *Information System Auditing Standard of Japan.* Provided by the Chuo Audit Corporation, Tokyo, August 1994.

CONTROL OBJECTIVES Controls in an Information Systems Environment: Control Guidelines and Audit Procedures: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Fourth Edition, Rolling Meadows, IL, 1992.

CISA Job Analysis: Information Systems Audit and Control Association Certification Board. "Certified Information Systems Auditor Job Analysis Study," Rolling Meadows, IL, 1994.

IFAC International Information Technology Guidelines—Managing Security of Information: International Federation of Accountants, New York, 1998.

IFAC International Guidelines on Information Technology Management—Managing Information Technology Planning for Business Impact: International Federation of Accountants, New York, 1999.

Guide for Auditing for Controls and Security, A System Development Life Cycle Approach: *NIST Special Publication 500-153:* National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, 1988.

Government Auditing Standards: US General Accounting Office, Washington, DC, 1999.

SPICE: Software Process Improvement and Capability Determination. A standard on software process improvement, British Standards Institution, London, 1995.

Denmark Generally Accepted IT Management Practices: The Institute of State Authorized Accountants, Denmark, 1994.

DRI International, Professional Practices for Business Continuity Planners: Disaster Recovery Institute International. *Guideline for Business Continuity Planners*, St. Louis, MO, 1997.

IIA, SAC Systems Audibility and Control: Institute of Internal Auditors Research Foundation, *Systems Audibility and Control Report*, Altamonte Springs, FL, 1991, 1994.

IIA, Professional Practices Pamphlet 97-1, Electronic Commerce: Institute of Internal Auditors Research Foundation, Altamonte Springs, FL, 1997.

E & Y Technical Reference Series: Ernst & Young, *SAP R/3 Audit Guide*, Cleveland, OH, 1996.

C & L Audit Guide SAP R/3: Coopers & Lybrand, *SAP R/3: Its Use, Control and Audit*, New York, 1997.

ISO IEC JTC1/SC27 Information Technology — Security: International Organisation for Standardisation (ISO) Technical Committee on Information Technology Security, Switzerland, 1998.

ISO IEC JTC1/SC7 Software Engineering: International Organisation for Standardisation (ISO) Technical Committee on Software Process Assessment. *An Assessment Model and Guidance Indicator,* Switzerland, 1992.

ISO TC68/SC2/WG4, Information Security Guidelines for Banking and Related Financial Services: International Organisation for Standardisation (ISO) Technical Committee on Banking and Financial Services, Draft, Switzerland, 1997.

Common Criteria and Methodology for Information Technology Security Evaluation: CSE (Canada), SCSSI (France), BSI (Germany), NLNCSA (Netherlands), CESG (United Kingdom), NIST (USA) and NSA (USA), 1999.

Recommended Practice for EDI: EDIFACT (EDI for Administration Commerce and Trade), Paris, 1987.

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

ESF Baseline Control—Communications: European Security Forum, London. *Communications Network Security*, September 1991; *Baseline Controls for Local Area Networks*, September, 1994.

ESF Baseline Control—Microcomputers: European Security Forum, London. *Baseline Controls Microcomputers Attached to Network*, June 1990.

Computerized Information Systems (CIS) Audit Manual: EDP Auditors Foundation (now the Information Systems Audit and Control Foundation), Rolling Meadows, IL, 1992.

Standards for Internal Control in the Federal Government (GAO/AIMD-00-21.3.1): US General Accounting Office, Washington, DC 1999.

Guide for Developing Security Plans for Information Technology: NIST Special Publication 800-18, National Institute for Standards and Technology, US Department of Commerce, Washington, DC, 1998.

Financial Information Systems Control Audit Manual (FISCAM): US General Accounting Office, Washington, DC, 1999.

BS7799-Information Security Management: British Standards Institute, London, 1999.

CICA Information Technology Control Guidelines, 3rd Edition: Canadian Institute of Chartered Accountants, Toronto, 1998.

ISO/IEC TR 1335-n Guidelines for the Management of IT Security (GMITS), Parts 1-5: International Organisation for Standardisation, Switzerland, 1998.

AICPA/CICA SysTrust™ Principles and Criteria for Systems Reliability, Version 1.0: American Institute of Certified Public Accountants, New York, and Canadian Institute of Chartered Accountants, Toronto, 1999.

Glossary of Terms

AICPA	American Institute of Certified Public Accountants
CICA	Canadian Institute of Chartered Accountants
CISA	Certified Information Systems Auditor
CCEB	Common Criteria for Information Technology Security
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
COSO	Committee of Sponsoring Organisations of the Treadway Commission
DRI	Disaster Recovery Institute International
DTI	Department of Trade and Industry of the United Kingdom
EDIFACT	Electronic Data Interchange for Administration, Commerce and Trade
EDPAF	Electronic Data Processing Auditors Foundation (now ISACF)
ESF	European Security Forum, a cooperation of 70+ primarily European multi-nationals with the goal of researching common security and control issues in IT
GAO	US General Accounting Office
I4	International Information Integrity Institute, similar association as the ESF, with similar goals but primarily US-based and run by Stanford Research Institute
IBAG	Infosec Business Advisory Group, industry representatives who advise the Infosec Committee. This Committee is composed of government officials of the European Community and itself advises the European Commission on IT security matters.
IFAC	International Federation of Accountants
IIA	Institute of Internal Auditors
INFOSEC	Advisory Committee for IT Security Matters to the European Commission
ISACA	Information Systems Audit and Control Association
ISACF	Information Systems Audit and Control Foundation
ISO	International Organisation for Standardisation (with offices in Geneva, Switzerland)
ISO9000	Quality management and quality assurance standards as defined by ISO
IT Control Objective	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria. The harmonised criteria of France, Germany, the Netherlands and the United Kingdom, since then also supported by the European Commission (see also TCSEC, the US equivalent).
NBS	National Bureau of Standards of the US
NIST (formerly NBS)	National Institute of Standards and Technology, based in Washington, DC
NSW	New South Wales, Australia
OECD	Organisation for Economic Cooperation and Development
OSF	Open Software Foundation
PCIE	President's Council on Integrity and Efficiency
SPICE	Software Process Improvement and Capability Determination—a standard on software process improvement
TCSEC	Trusted Computer System Evaluation Criteria, also known as The Orange Book: security evaluation criteria for computer systems as originally defined by the US Department of Defense. See also ITSEC, the European equivalent.
TickIT	Guide to Software Quality Management System Construction and Certification

GOVERNANCE INSTITUTE™

3701 ALGONQUIN ROAD, SUITE 1010
ROLLING MEADOWS, ILLINOIS 60008, USA

TELEPHONE: +1.847.253.1545
FACSIMILE: +1.847.253.1443
E-MAIL: research@isaca.org
WEB SITES: *www.ITgovernance.org*
www.isaca.org

TELL US WHAT YOU THINK ABOUT COBIT

We are interested in knowing your reaction to *COBIT: Control Objectives for Information and related Technology*. Please provide your comments below.

_____
_____
_____
_____
_____
_____
_____
_____

Name _____
Company _____
Address _____
City _____ State/Province _____
Country _____ ZIP/Postal Code _____
FAX Number _____
E-mail Address _____

☐ I am interested in learning more about how COBIT can be used in my organisation. Please ask a representative to contact me.

☐ Please send me more information about:

- ☐ Purchasing other COBIT products
- ☐ COBIT Training Courses (in-house or general session)
- ☐ Certified Information Systems Auditor™ (CISA®) Certification
- ☐ *Information Systems Control Journal*
- ☐ Information Systems Audit and Control Association (ISACA)

Thank you!

All respondents will be acknowledged.