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 IT Governance Institute, which conducts research and authors COBIT.

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 in and support of COBIT!

For additional information about the IT Governance Institute, visit *www.itgi.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* 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

The *Implementation Tool Set* 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 is available. It is 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.*

ITGI Contribution Form

Contributor: _____

Address: _____

_____

City _____ State/Province _____

Zip/Postal Code _____ Country _____

Remitted by: _____

Phone: _____

E-mail: _____

For information on the institute and contribution benefits see *www.itgi.org*

Contribution amount (US $):

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

☐ $500 (Platinum) ☐ Other US $_____

☐ Check enclosed payable in US dollars to ITGI

☐ **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 ITGI at +1.847.253.1443, or mail your contribution to: ITGI, 135 S. LaSalle Street, Department 1055, Chicago, IL 60674-1055 USA

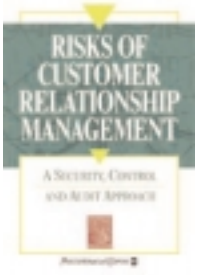
Direct any questions to Scott Artman at +1.847.253.1545, ext. 459, or *finance@isaca.org*.

Thank you for supporting CobiT!

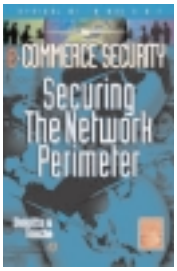
Recent ITGI Research Projects

Security Provisioning:
Managing Access in Extended Enterprises, ISSP
Member - $20 Nonmember - $30

e-Commerce Security
Public Key Infrastructure: Good Practices for Secure Communications, TRS-2
Member - $35 Nonmember - $50



Risks of Customer Relationship Management
A Security, control and Audit Approach, ISCR
Member - $75 Nonmember - $85



e-Commerce Security
Securing the Network Perimeter, TRS-3
Member - $35 Nonmember - $50

e-Commerce Security
Business Continuity Planning, IBCP
Member - $35 Nonmember - $50

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

Pricing and Order Form

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

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)

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/bookstore*

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

☐ MR. ☐ MS. ☐ MRS. ☐ MISS ☐ OTHER _____ Date _____
MONTH/DAY/YEAR

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/Coworker
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 ☐ CISM
2 ☐ CPA
3 ☐ CA
4 ☐ CIA
5 ☐ CBA
6 ☐ CCP
7 ☐ CSP
8 ☐ FCA
9 ☐ CFE
10 ☐ MA
11 ☐ FCPA
12 ☐ CFSA
13 ☐ 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 †	$ 120.00	(US)
• Chapter dues *(see following page)*	$ _____	(US)
• New member processing fee	$ 30.00	(US)*
PLEASE PAY THIS TOTAL	$ _____	(US)

† For student membership information please visit *www.isaca.org/student*

* Membership dues consist of association dues, chapter dues and new member processing fee.

Method of payment
☐ Check payable in US dollars, drawn on US bank
☐ Send invoice (Applications cannot be processed until dues payment is received.)
☐ MasterCard ☐ VISA ☐ American Express ☐ Diners Club

All payments by credit card will be processed in US dollars

ACCT # _____

Print name of cardholder _____

Expiration date _____
MONTH/YEAR

Signature _____

Cardholder billing address if different than address provided above:

_____

_____

By applying for membership in the Information Systems Audit and Control Association, members agree to hold the association and the IT Governance Institute, their officers, directors, agents, trustees, and employees and members, harmless for all acts or failures to act while carrying out the purpose of the association and the institute as set forth in their respective bylaws, and they certify that they will abide by the association's *Code of Professional Ethics (www.isaca.org/ethics).*

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, dues or gifts to the Information Systems Audit and 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 US members, $60 for non-US members. This amount is not 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
Fax: +1.847.253.1443

U.S. dollar amounts listed below are for local chapter dues. While correct at the time of printing, chapter dues are subject to change without notice. Please include the appropriate chapter dues amount with your remittance.

For current chapter dues, or if the amount is not listed below, please visit the web site *www.isaca.org/chapdues* or contact your local chapter at *www.isaca.org/chapters*.

Chapter Name	Chapter Number	Dues
ASIA		
Hong Kong	64	$40
Bangalore, India	138	$15
Cochin, India	176	$10
Coimbatore, India	155	$10
Hyderabad, India	164	$17
Kolkata, India	165	⁕
Madras, India (Chennai)	99	$10
Mumbai, India	145	⁕
New Delhi, India	140	$10
Pune, India	159	$17
Indonesia	123	⁕
Nagoya, Japan	118	$130
Osaka, Japan	103	$10
Tokyo, Japan	89	$120
Korea	107	$30
Lebanon	181	$35
Malaysia	93	$10
Muscat, Oman	168	$40
Karachi, Pakistan	148	$15
Manila, Philippines	136	$0
Jeddah, Saudi Arabia	163	$0
Riyadh, Saudi Arabia	154	$0
Singapore	70	$10
Sri Lanka	141	$15
Taiwan	142	$50
Bangkok, Thailand	109	$10
UAE	150	$10
CENTRAL/SOUTH AMERICA		
Buenos Aires, Argentina	124	$35
Mendoza, Argentina	144	⁕
São Paulo, Brazil	166	$25
LaPaz, Bolivia	173	$25
Santiago de Chile	135	$40
Bogotá, Colombia	126	$50
San José, Costa Rica	31	$33
Quito, Ecuador	179	$15
Mérida, Yucatán, México	101	$50
Mexico City, México	14	$65
Monterrey, México	80	$65
Panamá	94	$25
Lima, Perú	146	$15
Puerto Rico	86	$30
Montevideo, Uruguay	133	$100
Venezuela	113	$25
EUROPE/AFRICA		
Austria	157	$45
Belux (Belgium and Luxembourg)	143	$48
Croatia	170	$50
Czech Republic	153	$110
Denmark	96	⁕
Estonian	162	$10
Finland	115	$70
Paris, France	75	⁕
German	104	$80
Athens, Greece	134	$20
Budapest, Hungary	125	$60
Irish	156	$40
Tel-Aviv, Israel	40	⁕
Milano, Italy	43	$53
Rome, Italy	178	$26
Kenya	158	$40
Latvia	139	$10
Lithuania	180	$20
Netherlands	97	$50
Lagos, Nigeria	149	$20
Oslo, Norway	74	$50
Warsaw, Poland	151	$30
Moscow, Russia	167	$0
Romania	172	$50
Slovenia	137	$50
Slovensko	160	$40
South Africa	130	$35
Barcelona, Spain	171	$110
Valencia, Spain	182	$25
Sweden	88	$45
Switzerland	116	$35
Tanzania	174	$40
London, UK	60	$80
Central UK	132	$55
Northern England	111	$50
Scottish, UK	175	$45
NORTH AMERICA		
Canada		
Calgary, AB	121	$0
Edmonton, AB	131	$25
Vancouver, BC	25	$20
Victoria, BC	100	$0
Winnipeg, MB	72	$15
Nova Scotia	105	$0
Ottawa Valley, ON	32	$10
Toronto, ON	21	$25
Montreal, PQ	36	$20
Quebec City, PQ	91	$35
Islands		
Bermuda	147	$0
Trinidad & Tobago	106	$25
Midwestern United States		
Chicago, IL	02	$50
Illini (Springfield, IL)	77	$30
Central Indiana (Indianapolis)	56	$30
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
Quad Cities	169	$0
Northeastern United States		
Greater Hartford, CT (Southern New England)	28	$40
Central Maryland (Baltimore)	24	$25
New England (Boston, MA)	18	$30
New Jersey (Newark)	30	$40
Central New York (Syracuse)	29	$0
Hudson Valley, NY (Albany)	120	$0
New York Metropolitan	10	$50
Western New York (Buffalo)	46	$30
Harrisburg, PA	45	$25
Lehigh Valley (Allentown, PA)	122	$35
Philadelphia, PA	06	$40
Pittsburgh, PA	13	$20
National Capital Area, DC	05	$40
Southeastern United States		
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	$35
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		
Central Arkansas (Little Rock)	82	$60
Central Mississippi (Jackson)	161	$0
Denver, CO	16	$40
Greater Kansas City, KS	87	$0
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		
Anchorage, AK	177	$20
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	$25
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	$25
OCEANIA		
Adelaide, Australia	68	$0
Brisbane, Australia	44	$16
Canberra, Australia	92	$15
Melbourne, Australia	47	$25
Perth, Australia	63	$5
Sydney, Australia	17	$30
Auckland, New Zealand	84	$30
Wellington, New Zealand	73	$22
Papua New Guinea	152	$0

⁕Call chapter for information

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

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_____

One of the most important assets of an enterprise is its information. The integrity and reliability of that information and the systems that generate it are crucial to an enterprise's success. Faced with complex and correspondingly ingenious cyberthreats, organizations are looking for individuals who have the proven experience and knowledge to identify, evaluate and recommend solutions to mitigate IT system vulnerabilities. ISACA offers two certifications to meet these needs.

Certified Information Systems Auditor (CISA)

The CISA program is designed to assess and certify individuals in the IS audit, control and security profession who demonstrate exceptional skill and judgment.

The CISA examination content areas include:

- The IS audit process
- Management, planning and organization of IS
- Technical infrastructure and operational practices
- Protection of information assets
- Disaster recovery and business continuity
- Business application system development, acquisition, implementation and maintenance
- Business process evaluation and risk management

To earn the CISA designation, candidates are required to:

- Successfully complete the CISA examination
- Adhere to the Information Systems Audit and Control Association (ISACA) Code of Professional Ethics
- Submit verified evidence of a minimum number of years of professional information systems auditing, control or security work experience
- Comply with the CISA continuing education program (after becoming certified)

Certified Information Security Manager (CISM)

CISM is a newly created credential for security managers that provides executive management with the assurance that those certified have the expertise to provide effective security management and consulting. It is business-oriented and focused on information risk management while addressing management, design and technical security issues at a conceptual level.

The CISM credential measures expertise in the areas of:

- Information security governance
- Risk management
- Information security program(me) development
- Information security management
- Response management

To earn the CISM designation, information security professionals are required to:

- Successfully complete the CISM examination
- Adhere to the Information Systems Audit and Control Association (ISACA) Code of Professional Ethics
- Submit verified evidence of a minimum number of years of information security experience, with a number of those years in the job analysis domains
- Comply with the CISM continuing education program (after becoming certified)

A grandfathering opportunity, available through 31 December 2003, allows information security professionals with the necessary experience to apply for certification without taking the CISM exam.

CISA®
CERTIFIED INFORMATION SYSTEMS AUDITOR™

CISM
CERTIFIED INFORMATION SECURITY MANAGER™

Being a CISA or a CISM is more than passing an examination. It demonstrates the commitment, dedication and proficiency required to excel in your profession. These certifications identify their holders as consummate professionals who maintain a competitive advantage among their peers. Earning these designations helps assure a positive reputation and distinguishes you among other candidates seeking positions in both the private and public sectors. As a member of ISACA, you have the opportunity to sit for the exams, purchase review materials and attend ISACA conferences to maintain your certifications at a substantially reduced cost.

For more information on becoming a CISA or a CISM, visit the ISACA web site at *www.isaca.org/certification.*

COBIT®

3rd Edition

Framework

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

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.

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 1-893209-14-8 (*Framework*)
ISBN 1-893209-13-X (Complete 6 book set with CD-ROM)

Printed in the United States of America.

ACKNOWLEDGMENTS

COBIT STEERING COMMITTEE

Erik Guldentops, S.W.I.F.T. sc, Belgium

John Lainhart, PricewaterhouseCoopers, USA

Eddy Schuermans, PricewaterhouseCoopers, Belgium

John Beveridge, State Auditor's Office, Massachusetts, USA

Michael Donahue, PricewaterhouseCoopers, USA

Gary Hardy, Arthur Andersen, United Kingdom

Ronald Saull, Great-West Life Assurance, London Life and Investors Group, Canada

Mark Stanley, Sun America Inc., USA

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.

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.

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.

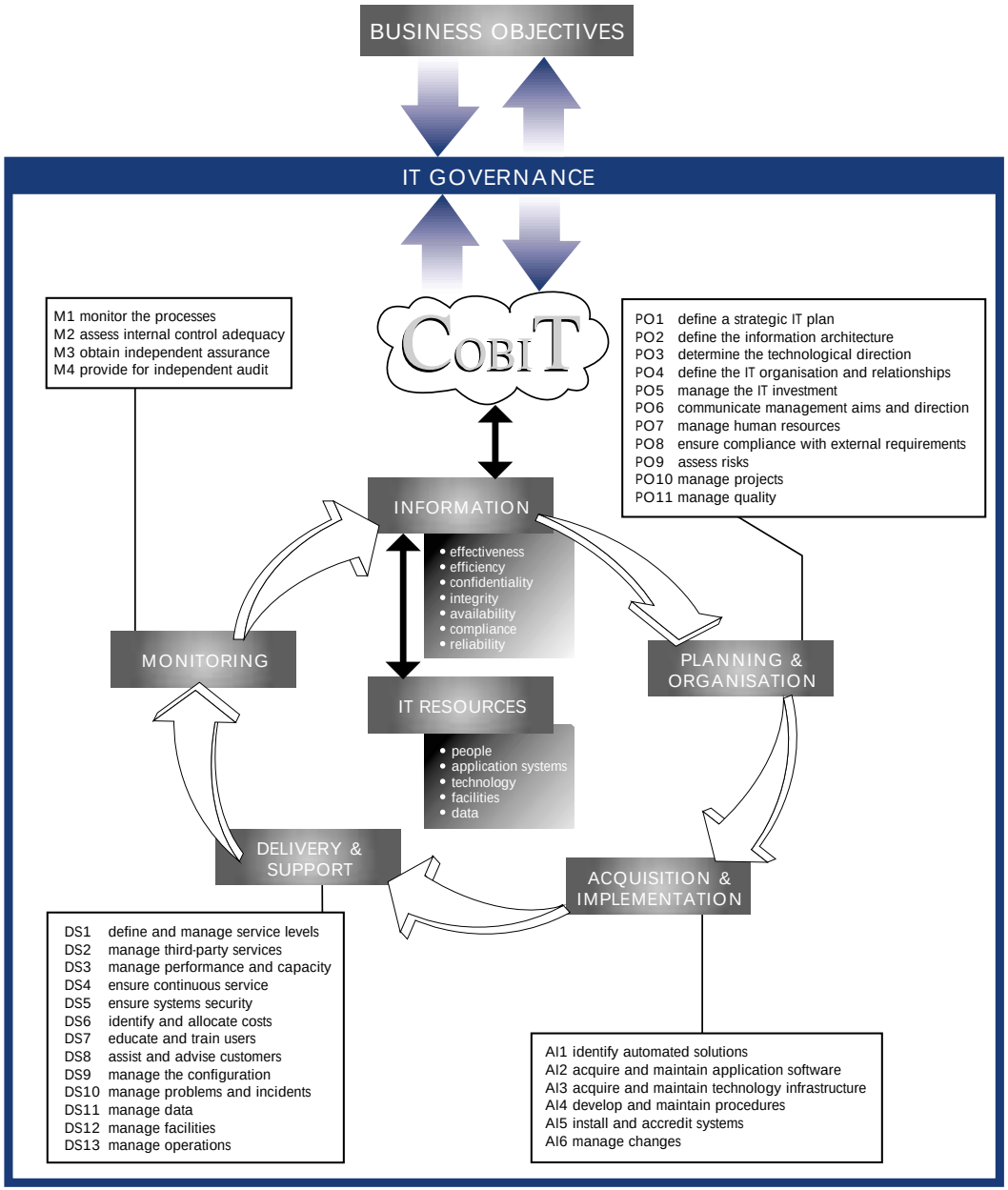
Specifically, COBIT provides **Maturity Models** for control over IT processes, so that management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be; **Critical Success Factors**, 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.

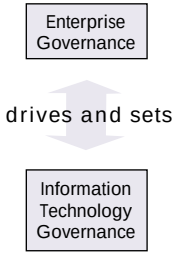
EMERGENCE OF ENTERPRISE AND IT GOVERNANCE

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

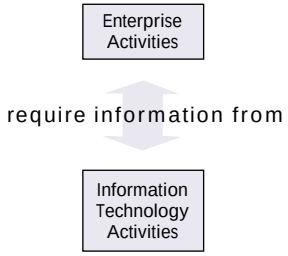
enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy.

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.

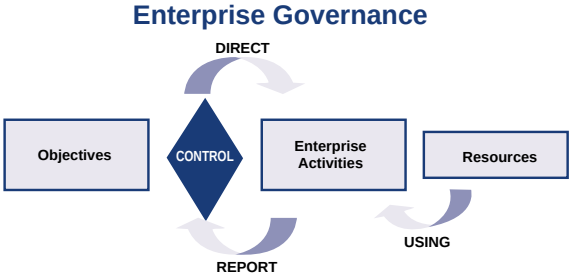
Looking at the interplay of enterprise and IT governance processes in more detail, enterprise governance, the system by which entities are directed and controlled, drives and sets IT governance. At the same time, IT should provide critical input to, and constitute an important component of, strategic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

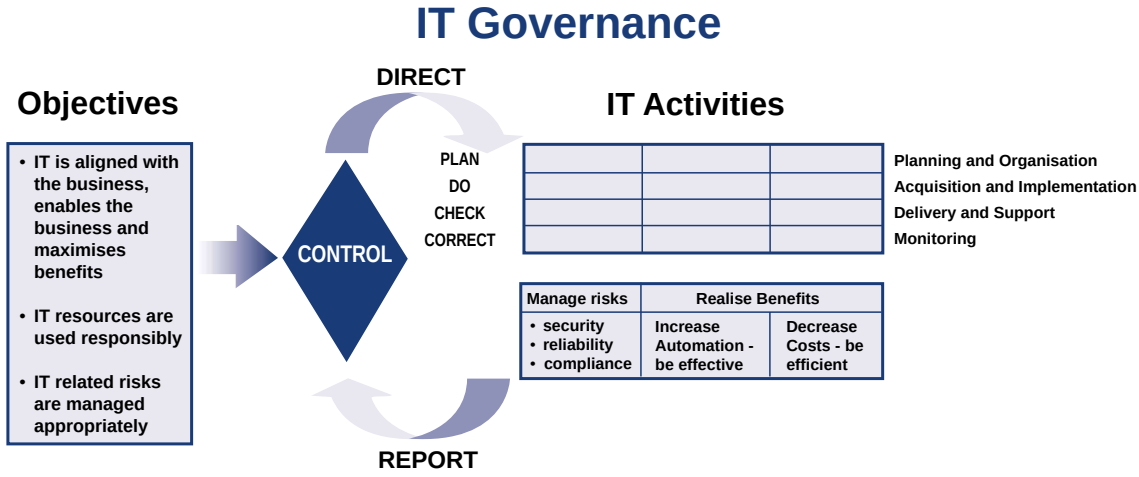


Enterprises are governed by generally accepted good (or best) practices, to ensure that the enterprise is achieving its goals-the assurance of which is guaranteed by certain controls. From these objectives flows the organisation's direction, which dictates certain enterprise activities, using the enterprise's 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.



THE COBIT FRAMEWORK, *continued*

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.**

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.

THE COBIT FRAMEWORK, *continued*

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

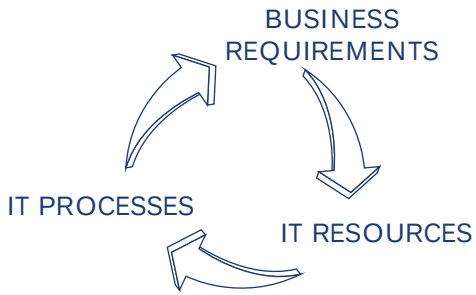
For the purpose of this project, the following definitions are provided. "Control" is adapted from the COSO Report (*Internal Control—Integrated Framework*, Committee of Sponsoring Organisations of the Treadway Commission, 1992) and "IT Control Objective" is adapted from the SAC Report (*Systems Auditability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

THE FRAMEWORK'S PRINCIPLES, *continued*

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:

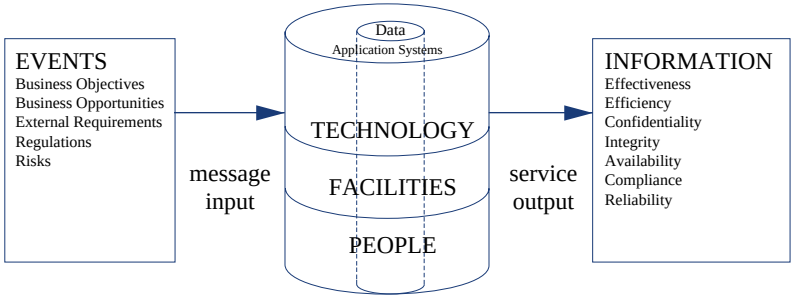
Effectiveness	deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
Efficiency	concerns the provision of information through the optimal (most productive and economical) use of resources.
Confidentiality	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.

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.

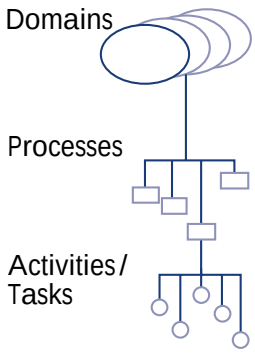
Another way of looking at the relationship of IT resources to the delivery of services is depicted below.



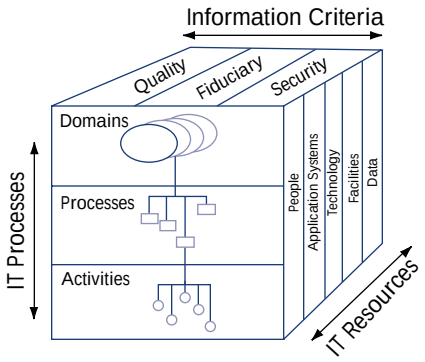
In order to ensure that the business requirements for information are met, adequate control measures need to be defined, implemented and monitored over these resources. How then can organisations satisfy themselves that the information they get exhibits the characteristics they need? This is where a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

THE FRAMEWORK'S PRINCIPLES, *continued*

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.

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.

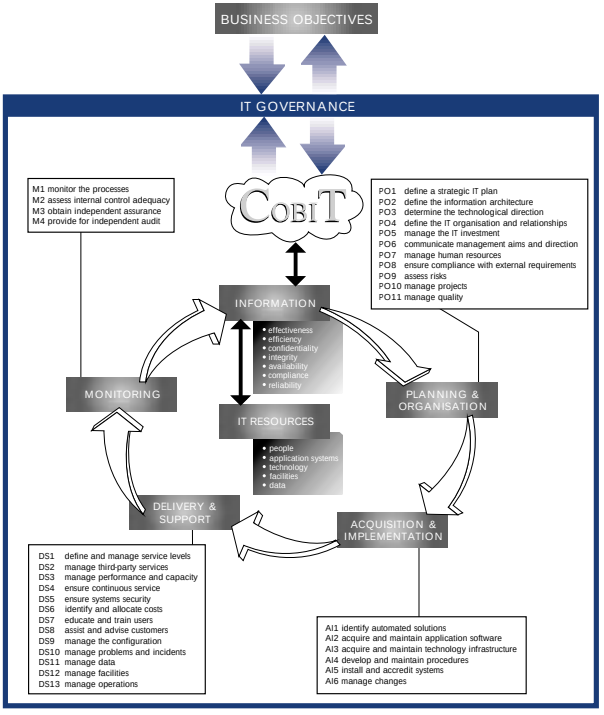
It is clear that all control measures will not necessarily satisfy the different business requirements for information to the same degree.

- **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.

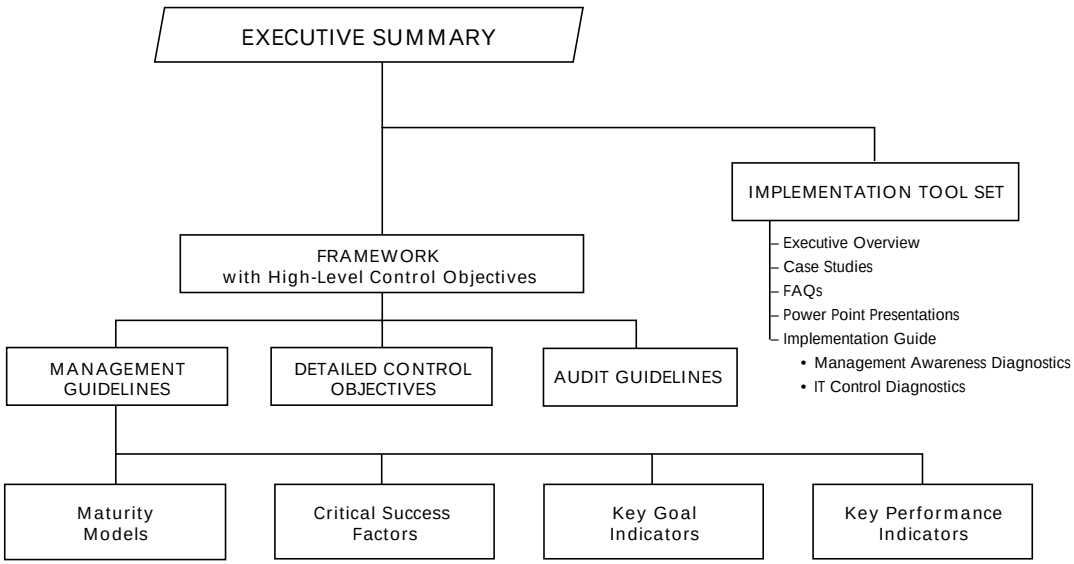
Refer to Appendix II, COBIT Project Description; Appendix III, COBIT Primary Reference Material; and Appendix IV, Glossary of Terms.

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

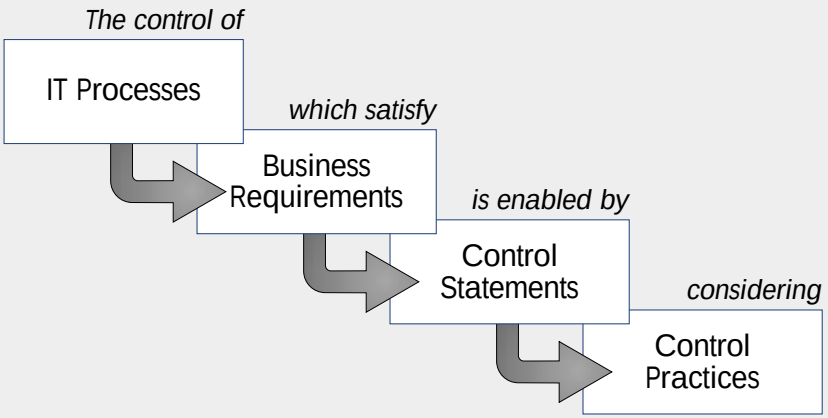
FRAMEWORK NAVIGATION OVERVIEW

The High-Level Control Objectives section presents control statements, business requirements, enablers and considerations for all of COBIT's 34 IT processes. The domain indicator ("PO" for Planning & Organisation, "AI" for Acquisition & Implementation, "DS" for Delivery & Support and "M" for Monitoring) is shown at top left. The applicable information criteria and IT resources managed are shown via mini-matrix, as described on the following page.

The COBIT *Framework* has been limited to high-level control objectives in the form of a business need within a particular IT process, the achievement of which is enabled by a control statement, for which consideration should be given to potentially applicable controls.

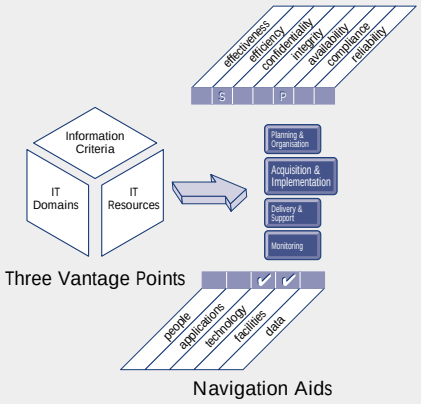
The Control Objectives have been organised by process/activity, but navigation aids have been provided not only to facilitate entry from any one vantage point, but also to facilitate combined or global approaches, such as installation/implementation of a process, global management responsibilities for a process and the use of IT resources by a process.

It should also be noted that the Control Objectives have been defined in a generic way; i.e., not depending on the technical platform, while accepting the fact that some special technology environments may need separate coverage for Control Objectives.



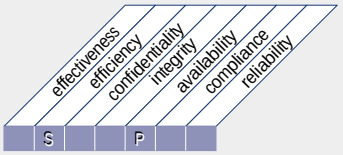
FRAMEWORK NAVIGATION OVERVIEW, *continued*

To facilitate efficient use of the Control Objectives in support of the different vantage points, some navigation aids are provided as part of the presentation of the high-level Control Objectives. For each of the three dimensions along which the COBIT *Framework* can be approached—processes, IT resources and information criteria—a navigation aid is provided.

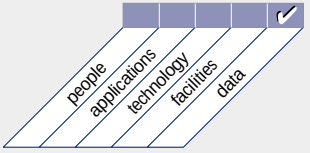


IT domains are identified by this icon in the UPPER RIGHT CORNER of each page in the Control Objectives section, with the domain under review highlighted and enlarged.

The cue to information criteria will be provided in the UPPER LEFT CORNER in the Control Objectives section by means of this mini-matrix, which will identify which criteria are applicable to each high-level control objective and to which degree (primary or secondary).

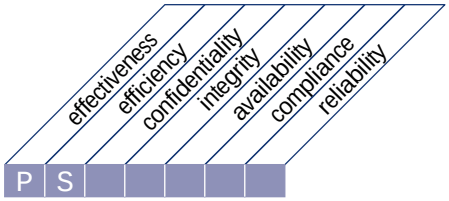


A second mini-matrix in the LOWER RIGHT CORNER in the Control Objectives section identifies the IT resources that are specifically managed by the process under consideration—not those that merely take part in the process. For example, the "manage data" process concentrates particularly on Integrity and Reliability of the data resource.



HIGH-LEVEL CONTROL OBJECTIVES

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining a strategic IT plan

that satisfies the business requirement

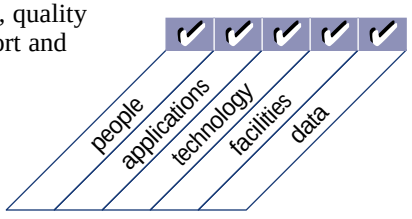
to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

is enabled by

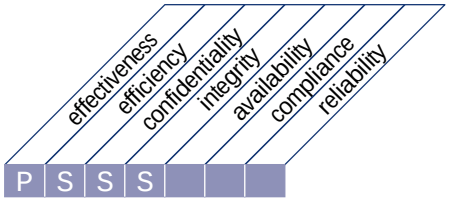
a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals

and takes into consideration

- enterprise business strategy
- definition of how IT supports the business objectives
- inventory of technological solutions and current infrastructure
- monitoring the technology markets
- timely feasibility studies and reality checks
- existing systems assessments
- enterprise position on risk, time-to-market, quality
- need for senior management buy-in, support and critical review



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining the information architecture

that satisfies the business requirement

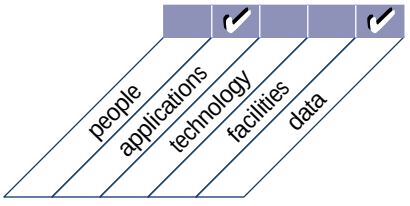
of optimising the organisation of the information systems

is enabled by

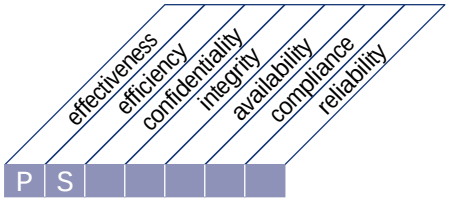
creating and maintaining a business information model and ensuring appropriate systems are defined to optimise the use of this information

and takes into consideration

- automated data repository and dictionary
- data syntax rules
- data ownership and criticality/security classification
- an information model representing the business
- enterprise information architectural standards



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

determining technological direction

that satisfies the business requirement

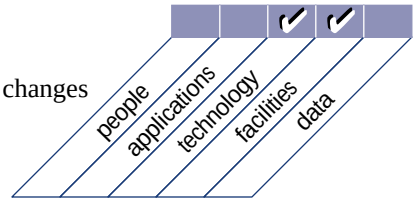
to take advantage of available and emerging technology to drive and make possible the business strategy

is enabled by

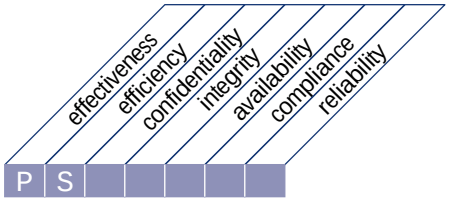
creation and maintenance of a technological infrastructure plan that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms

and takes into consideration

- capability of current infrastructure
- monitoring technology developments via reliable sources
- conducting proof-of-concepts
- risk, constraints and opportunities
- acquisition plans
- migration strategy and roadmaps
- vendor relationships
- independent technology reassessment
- hardware and software price/performance changes



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining the IT organisation and relationships

that satisfies the business requirement

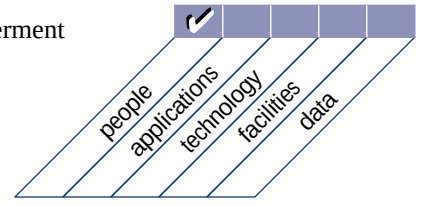
to deliver the right IT services

is enabled by

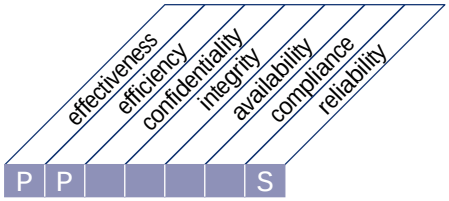
an organisation suitable in numbers and skills with roles and responsibilities defined and communicated, aligned with the business and that facilitates the strategy and provides for effective direction and adequate control

and takes into consideration

- board level responsibility for IT
- management's direction and supervision of IT
- IT's alignment with the business
- IT's involvement in key decision processes
- organisational flexibility
- clear roles and responsibilities
- balance between supervision and empowerment
- job descriptions
- staffing levels and key personnel
- organisational positioning of security, quality and internal control functions
- segregation of duties



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing the IT investment

that satisfies the business requirement

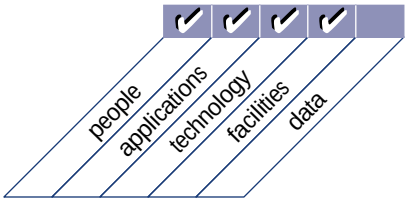
to ensure funding and to control disbursement of financial resources

is enabled by

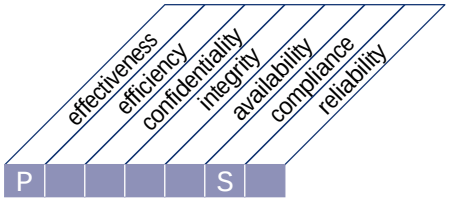
a periodic investment and operational budget established and approved by the business

and takes into consideration

- funding alternatives
- clear budget ownership
- control of actual spending
- cost justification and awareness of total cost of ownership
- benefit justification and accountability for benefit fulfillment
- technology and application software life cycles
- alignment with enterprise business strategy
- impact assessment
- asset management



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

communicating management aims and direction

that satisfies the business requirement

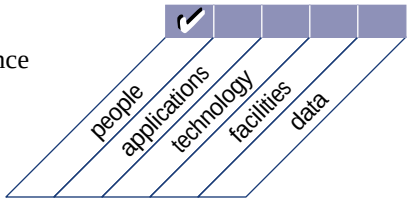
to ensure user awareness and understanding of those aims

is enabled by

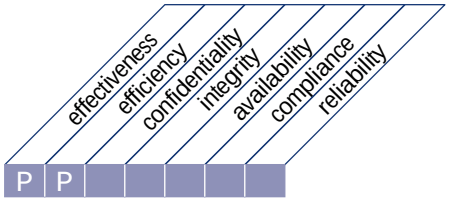
policies established and communicated to the user community; furthermore, standards need to be established to translate the strategic options into practical and usable user rules

and takes into consideration

- clearly articulated mission
- technology directives linked to business aims
- code of conduct/ethics
- quality commitment
- security and internal control policies
- security and internal control practices
- lead-by-example
- continuous communications programme
- providing guidance and checking compliance



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing human resources

that satisfies the business requirement

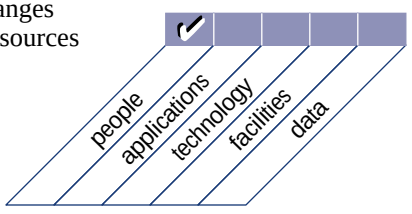
to acquire and maintain a motivated and competent workforce and maximise personnel contributions to the IT processes

is enabled by

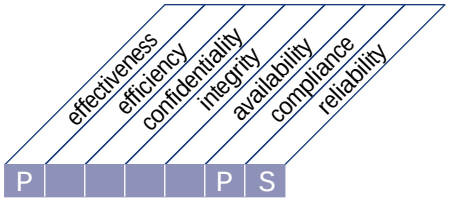
sound, fair and transparent personnel management practices to recruit, line, vet, compensate, train, appraise, promote and dismiss

and takes into consideration

- recruitment and promotion
- training and qualification requirements
- awareness building
- cross-training and job rotation
- hiring, vetting and dismissal procedures
- objective and measurable performance evaluation
- responsiveness to technical and market changes
- properly balancing internal and external resources
- succession plan for key positions



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring compliance with external requirements

that satisfies the business requirement

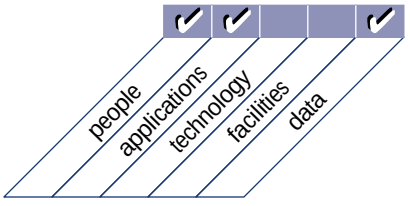
to meet legal, regulatory and contractual obligations

is enabled by

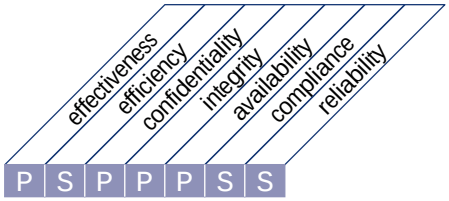
identifying and analysing external requirements for their IT impact, and taking appropriate measures to comply with them

and takes into consideration

- laws, regulations and contracts
- monitoring legal and regulatory developments
- regular monitoring for compliance
- safety and ergonomics
- privacy
- intellectual property



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing risks

that satisfies the business requirement

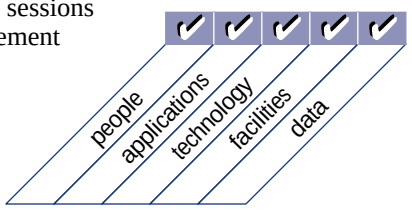
of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

is enabled by

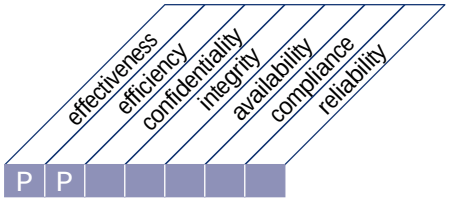
the organisation engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks

and takes into consideration

- risk management ownership and accountability
- different kinds of IT risks (technology, security, continuity, regulatory, etc.)
- defined and communicated risk tolerance profile
- root cause analyses and risk brainstorming sessions
- quantitative and/or qualitative risk measurement
- risk assessment methodology
- risk action plan
- timely reassessment



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing projects

that satisfies the business requirement

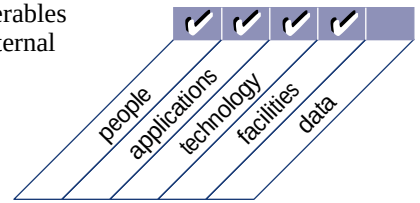
to set priorities and to deliver on time and within budget

is enabled by

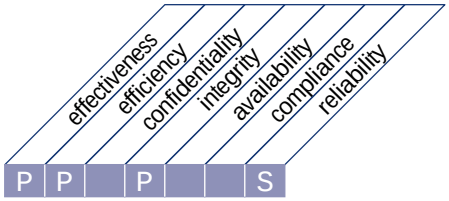
the organisation identifying and prioritising projects in line with the operational plan and the adoption and application of sound project management techniques for each project undertaken

and takes into consideration

- business management sponsorship for projects
- program management
- project management capabilities
- user involvement
- task breakdown, milestone definition and phase approvals
- allocation of responsibilities
- rigorous tracking of milestones and deliverables
- cost and manpower budgets, balancing internal and external resources
- quality assurance plans and methods
- program and project risk assessments
- transition from development to operations



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing quality

that satisfies the business requirement

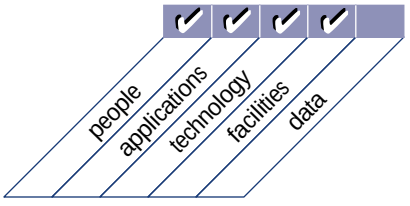
to meet the IT customer requirements

is enabled by

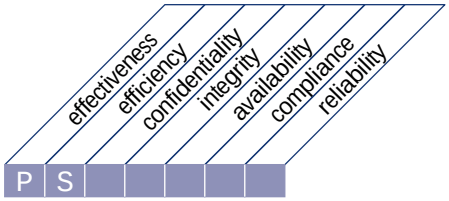
the planning, implementing and maintaining of quality management standards and systems providing for distinct development phases, clear deliverables and explicit responsibilities

and takes into consideration

- establishment of a quality culture
- quality plans
- quality assurance responsibilities
- quality control practices
- system development life cycle methodology
- programme and system testing and documentation
- quality assurance reviews and reporting
- training and involvement of end user and quality assurance personnel
- development of a quality assurance knowledge base
- benchmarking against industry norms



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

identifying automated solutions

that satisfies the business requirement

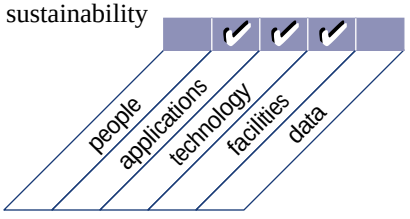
of ensuring an effective and efficient approach to satisfy the user requirements

is enabled by

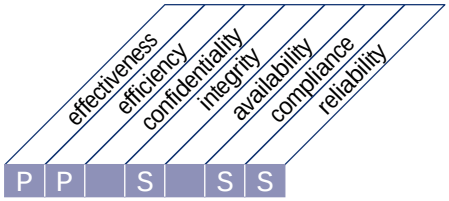
an objective and clear identification and analysis of the alternative opportunities measured against user requirements

and takes into consideration

- knowledge of solutions available in the market
- acquisition and implementation methodologies
- user involvement and buy in
- alignment with enterprise and IT strategies
- information requirements definition
- feasibility studies (costs, benefits, alternatives, etc.)
- functionality, operability, acceptability and sustainability requirements
- compliance with information architecture
- cost-effective security and control
- supplier responsibilities



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

acquiring and maintaining application software

that satisfies the business requirement

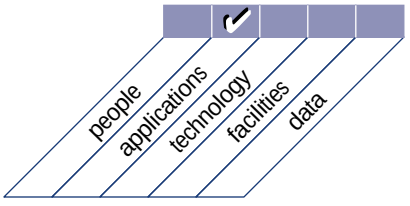
to provide automated functions which effectively support the business process

is enabled by

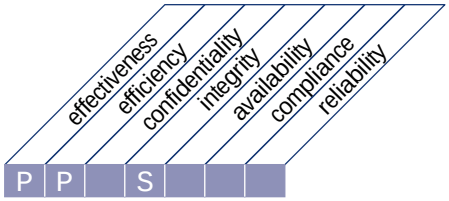
the definition of specific statements of functional and operational requirements, and a phased implementation with clear deliverables

and takes into consideration

- functional testing and acceptance
- application controls and security requirements
- documentation requirements
- application software life cycle
- enterprise information architecture
- system development life cycle methodology
- user-machine interface
- package customisation



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

acquiring and maintaining technology infrastructure

that satisfies the business requirement

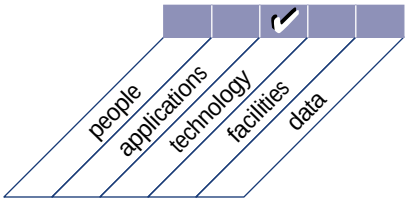
to provide the appropriate platforms for supporting business applications

is enabled by

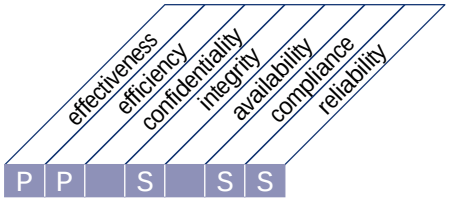
judicious hardware and software acquisition, standardising of software, assessment of hardware and software performance, and consistent system administration

and takes into consideration

- compliance with technology infrastructure directions and standards
- technology assessment
- installation, maintenance and change controls
- upgrade, conversion and migration plans
- use of internal and external infrastructures and/or resources
- supplier responsibilities and relationships
- change management
- total cost of ownership
- system software security



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

developing and maintaining procedures

that satisfies the business requirement

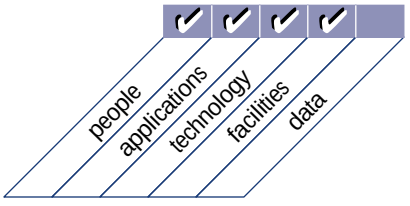
to ensure the proper use of the applications and the technological solutions put in place

is enabled by

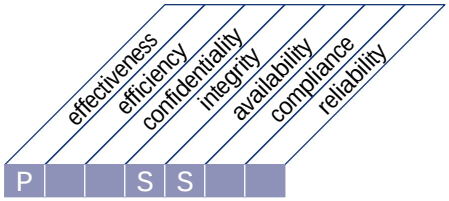
a structured approach to the development of user and operations procedure manuals, service requirements and training materials

and takes into consideration

- business process re-design
- treating procedures as any other technology deliverable
- timely development
- user procedures and controls
- operational procedures and controls
- training materials
- managing change



High-Level Control Objective



Control over the IT process of

installing and accrediting systems

that satisfies the business requirement

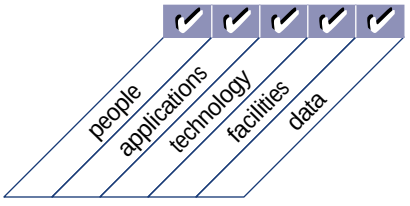
to verify and confirm that the solution is fit for the intended purpose

is enabled by

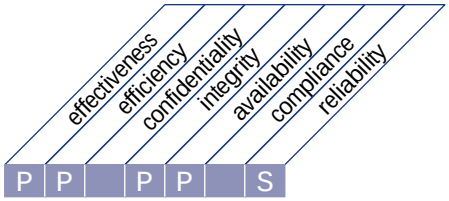
the realisation of a well-formalised installation migration, conversion and acceptance plan

and takes into consideration

- training of user and IT operations personnel
- data conversion
- a test environment reflecting the live environment
- accreditation
- post-implementation reviews and feedback
- end user involvement in testing
- continuous quality improvement plans
- business continuity requirements
- capacity and throughput measurement
- agreed upon acceptance criteria



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing changes

that satisfies the business requirement

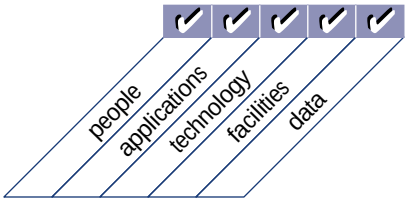
to minimise the likelihood of disruption, unauthorised alterations and errors

is enabled by

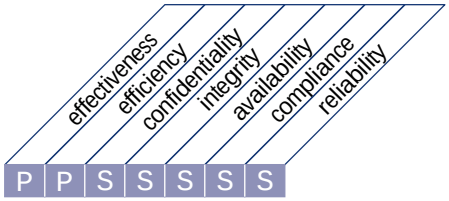
a management system which provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure

and takes into consideration

- identification of changes
- categorisation, prioritisation and emergency procedures
- impact assessment
- change authorisation
- release management
- software distribution
- use of automated tools
- configuration management
- business process re-design



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining and managing service levels

that satisfies the business requirement

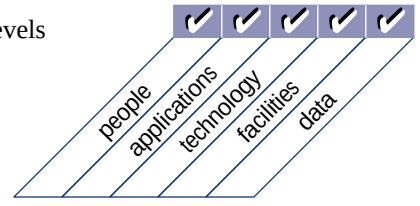
to establish a common understanding of the level of service required

is enabled by

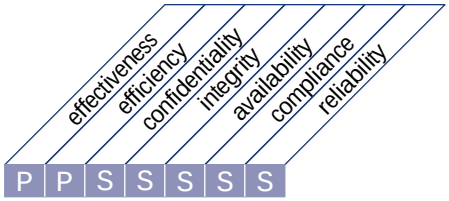
the establishment of service-level agreements which formalise the performance criteria against which the quantity and quality of service will be measured

and takes into consideration

- formal agreements
- definition of responsibilities
- response times and volumes
- charging
- integrity guarantees
- non-disclosure agreements
- customer satisfaction criteria
- cost/benefit analysis of required service levels
- monitoring and reporting



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing third-party services

that satisfies the business requirement

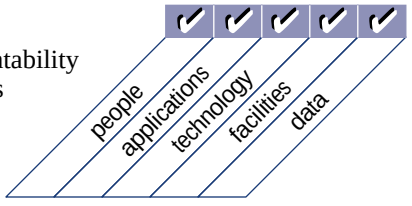
to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements

is enabled by

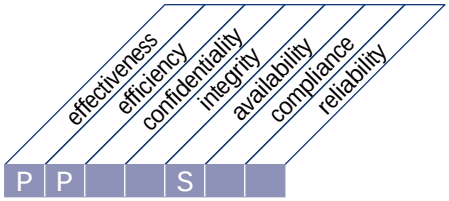
control measures aimed at the review and monitoring of existing agreements and procedures for their effectiveness and compliance with organisation policy

and takes into consideration

- third-party service agreements
- contract management
- non-disclosure agreements
- legal and regulatory requirements
- service delivery monitoring and reporting
- enterprise and IT risk assessments
- performance rewards and penalties
- internal and external organisational accountability
- analysis of cost and service level variances



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing performance and capacity

that satisfies the business requirement

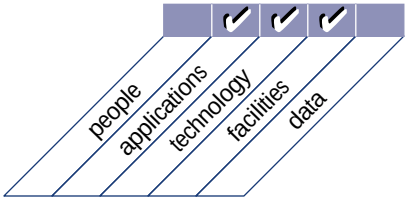
to ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs

is enabled by

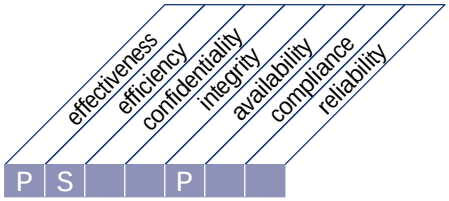
data collection, analysis and reporting on resource performance, application sizing and workload demand

and takes into consideration

- availability and performance requirements
- automated monitoring and reporting
- modeling tools
- capacity management
- resource availability
- hardware and software price/performance changes



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring continuous service

that satisfies the business requirement

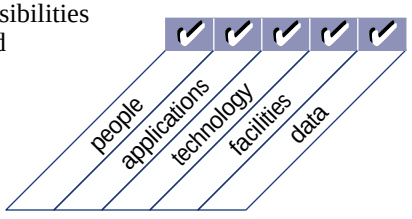
to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption

is enabled by

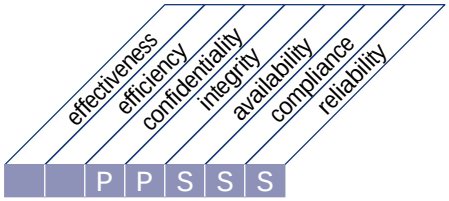
having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements

and takes into consideration

- criticality classification
- alternative procedures
- back-up and recovery
- systematic and regular testing and training
- monitoring and escalation processes
- internal and external organisational responsibilities
- business continuity activation, fallback and resumption plans
- risk management activities
- assessment of single points of failure
- problem management



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring systems security

that satisfies the business requirement

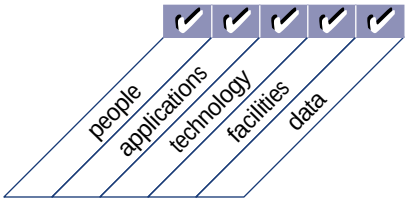
to safeguard information against unauthorised use, disclosure or modification, damage or loss

is enabled by

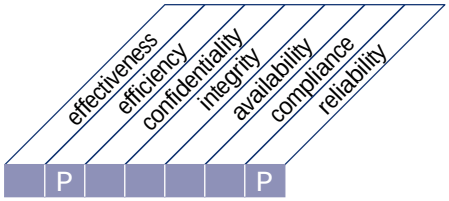
logical access controls which ensure that access to systems, data and programmes is restricted to authorised users

and takes into consideration

- confidentiality and privacy requirements
- authorisation, authentication and access control
- user identification and authorisation profiles
- need-to-have and need-to-know
- cryptographic key management
- incident handling, reporting and follow-up
- virus prevention and detection
- firewalls
- centralised security administration
- user training
- tools for monitoring compliance, intrusion testing and reporting



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

identifying and allocating costs

that satisfies the business requirement

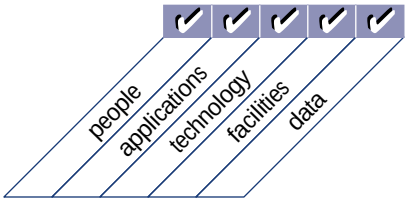
to ensure a correct awareness of the costs attributable to IT services

is enabled by

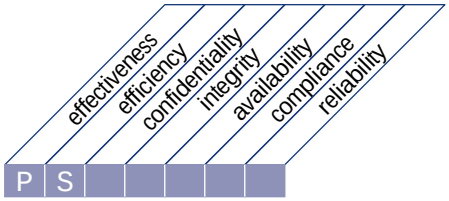
a cost accounting system which ensures that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering

and takes into consideration

- resources identifiable and measurable
- charging policies and procedures
- charge rates and charge-back process
- linkage to service level agreement
- automated reporting
- verification of benefit realisation
- external benchmarking



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

educating and training users

that satisfies the business requirement

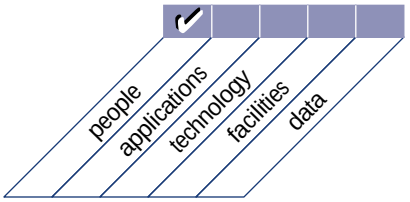
to ensure that users are making effective use of technology and are aware of the risks and responsibilities involved

is enabled by

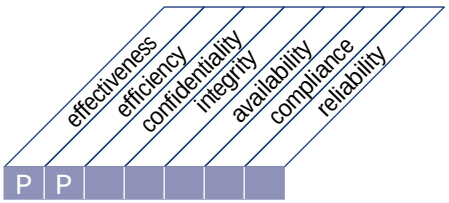
a comprehensive training and development plan

and takes into consideration

- training curriculum
- skills inventory
- awareness campaigns
- awareness techniques
- use of new training technologies and methods
- personnel productivity
- development of knowledge base



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assisting and advising customers

that satisfies the business requirement

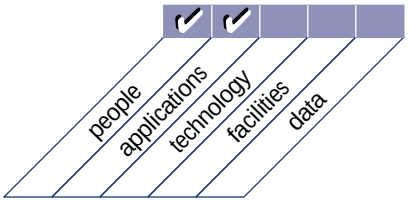
to ensure that any problem experienced by the user is appropriately resolved

is enabled by

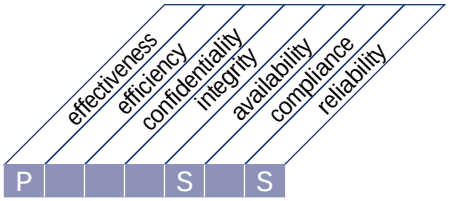
a help desk facility which provides first-line support and advice

and takes into consideration

- customer query and problem response
- query monitoring and clearance
- trend analysis and reporting
- development of knowledge base
- root cause analysis
- problem tracking and escalation



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing the configuration

that satisfies the business requirement

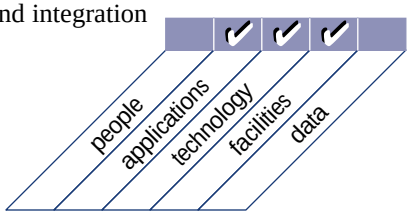
to account for all IT components, prevent unauthorised alterations, verify physical existence and provide a basis for sound change management

is enabled by

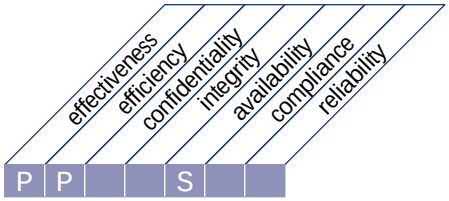
controls which identify and record all IT assets and their physical location, and a regular verification programme which confirms their existence

and takes into consideration

- asset tracking
- configuration change management
- checking for unauthorised software
- software storage controls
- software and hardware interrelationships and integration
- use of automated tools



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing problems and incidents

that satisfies the business requirement

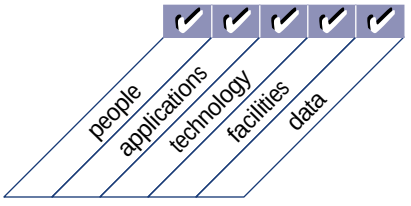
to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence

is enabled by

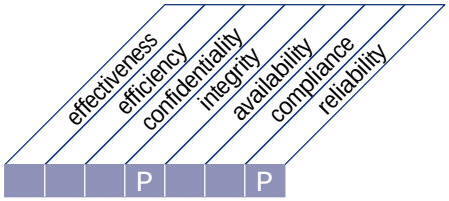
a problem management system which records and progresses all incidents

and takes into consideration

- audit trails of problems and solutions
- timely resolution of reported problems
- escalation procedures
- incident reports
- accessibility of configuration information
- supplier responsibilities
- coordination with change management



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing data

that satisfies the business requirement

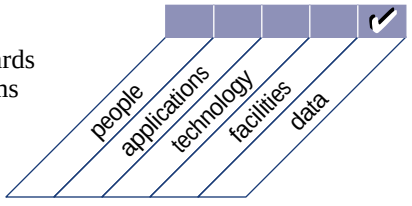
to ensure that data remains complete, accurate and valid during its input, update and storage

is enabled by

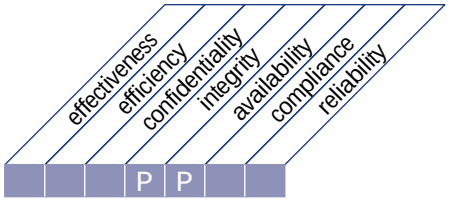
an effective combination of application and general controls over the IT operations

and takes into consideration

- form design
- source document controls
- input, processing and output controls
- media identification, movement and library management
- data back-up and recovery
- authentication and integrity
- data ownership
- data administration policies
- data models and data representation standards
- integration and consistency across platforms
- legal and regulatory requirements



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing facilities

that satisfies the business requirement

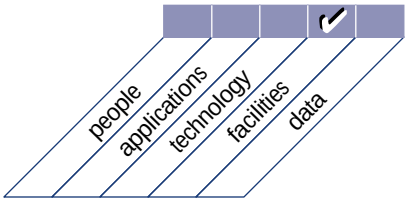
to provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards

is enabled by

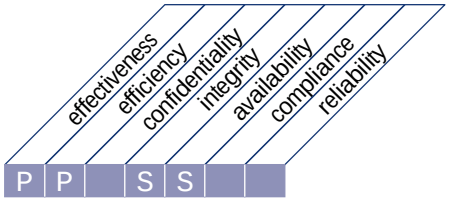
the installation of suitable environmental and physical controls which are regularly reviewed for their proper functioning

and takes into consideration

- access to facilities
- site identification
- physical security
- inspection and escalation policies
- business continuity planning and crisis management
- personnel health and safety
- preventive maintenance policies
- environmental threat protection
- automated monitoring



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing operations

that satisfies the business requirement

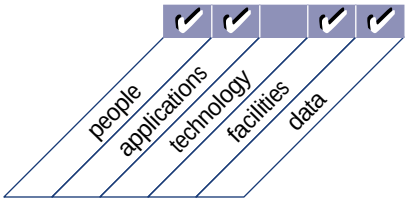
to ensure that important IT support functions are performed regularly and in an orderly fashion

is enabled by

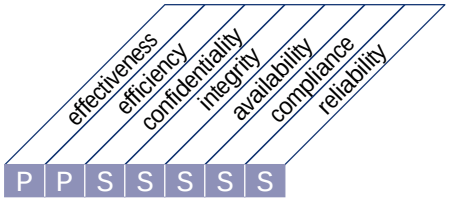
a schedule of support activities which is recorded and cleared for the accomplishment of all activities

and takes into consideration

- operations procedure manual
- start-up process documentation
- network services management
- workload and personnel scheduling
- shift hand-over process
- system event logging
- coordination with change, availability and business continuity management
- preventive maintenance
- service level agreements
- automated operations
- incident logging, tracking and escalation



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

monitoring the processes

that satisfies the business requirement

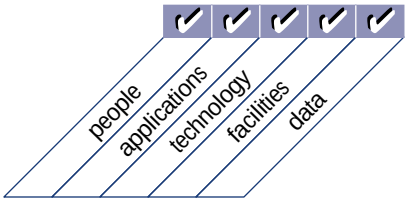
to ensure the achievement of the performance objectives set for the IT processes

is enabled by

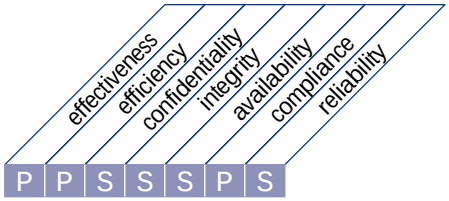
the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations

and takes into consideration

- scorecards with performance drivers and outcome measures
- customer satisfaction assessments
- management reporting
- knowledge base of historical performance
- external benchmarking



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing internal control adequacy

that satisfies the business requirement

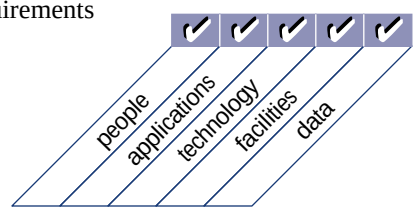
to ensure the achievement of the internal control objectives set for the IT processes

is enabled by

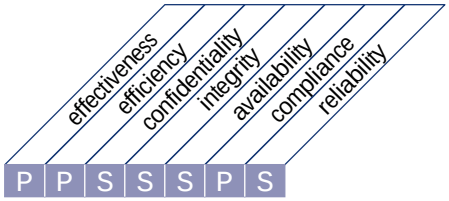
the commitment to monitoring internal controls, assessing their effectiveness, and reporting on them on a regular basis

and takes into consideration

- responsibilities for internal control
- ongoing internal control monitoring
- benchmarks
- error and exception reporting
- self-assessments
- management reporting
- compliance with legal and regulatory requirements



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

obtaining independent assurance

that satisfies the business requirement

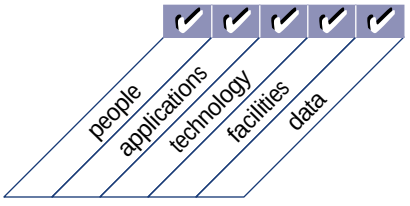
to increase confidence and trust among the organisation, customers, and third-party providers

is enabled by

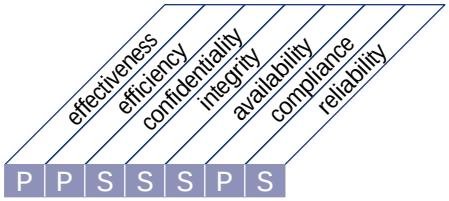
independent assurance reviews carried out at regular intervals

and takes into consideration

- independent certifications and accreditation
- independent effectiveness evaluations
- independent assurance of compliance with laws and regulatory requirements
- independent assurance of compliance with contractual commitments
- third-party service provider reviews and benchmarking
- performance of assurance reviews by qualified personnel
- proactive audit involvement



HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

providing for independent audit

that satisfies the business requirement

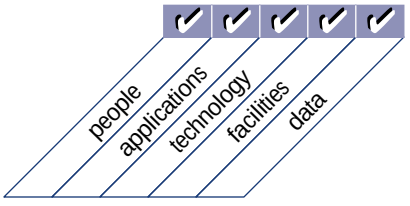
to increase confidence levels and benefit from best practice advice

is enabled by

independent audits carried out at regular intervals

and takes into consideration

- audit independence
- proactive audit involvement
- performance of audits by qualified personnel
- clearance of findings and recommendations
- follow-up activities
- impact assessments of audit recommendations (costs, benefits and risks)



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

Information Criteria
effectiveness
efficiency
confidentiality
integrity
availability
compliance
reliability

IT Resources
people
applications
technology
facilities
data

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.

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.