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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ISACF Contribution Form

Contributor: _____

Address: _____

_____

City _____ State/Province _____

Zip/Postal Code _____ Country _____

Remitted by: _____

Phone: _____

e-mail: _____

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

Contribution amount (US $):

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

☐ $500 (Platinum) ☐ Other US $_____

☐ Check enclosed payable in US $ to ISACF

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

Card number _____ Exp. Date _____

Name of cardholder: _____

Signature of cardholder: _____

Complete card billing address if different from address on left

_____

_____

_____

U.S. Tax ID number: 95-3080691

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

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

Thank you for supporting CobiT!

Recent ISACF Research Projects

Control Objectives for Net Centric Technology, NCC

Member - $90 Non-member - $130

Digital Signatures

Security & Controls, ISDS

Member - $35 Non-member - $50

In Partnership with

Deloitte & Touche

e-Commerce Security

A Global Status Report, ISEC

Member - $35 Non-member - $50

e-Commerce Security

Enterprise Best Practices, 2-EC

Member - $30 Non-member - $40

e-Commerce Security

Trading Partner Identification, Registration and Enrollment, TRS-1

Member - $35 Non-member - $50

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

Pricing and Order Form

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

GOVERNANCE INSTITUTE™

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

COBIT 2nd Edition purchasers - see *www.isaca.org/3upgrade.htm* for special upgrade pricing.

Individual components are also available for purchase:

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

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

Name _____ Date _____

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

Company Name _____

Address: ❑ Home ❑ Company _____

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

Phone Number ( ) _____ Fax Number ( ) _____

E-mail Address _____ Special Shipping Instructions or Remarks _____

_____

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

PAYMENT INFORMATION – PREPAYMENT REQUIRED

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

Account # _____ Exp. Date _____

Print Cardholder Name _____ Signature of Cardholder _____

Cardholder Billing Address if different than above _____

_____

Shipping and Handling Rates

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

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

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

PDF

Information Systems Audit and Control Association

MEMBERSHIP APPLICATION

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

Date _____
MONTH/DAY/YEAR

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

Name _____
FIRST MIDDLE LAST/FAMILY

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

Residence address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

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

Company name _____

Business address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

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

E-mail _____

Send mail to
☐ Home
☐ Business

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

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

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

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

Date of Birth _____
MONTH/DAY/YEAR

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

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

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

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

Payment due

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

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

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

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

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

ACCT # _____

Print Name of Cardholder _____

Expiration Date _____
MONTH/DAY/YEAR

Signature _____

Cardholder billing address if different than address provided above:

_____

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

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

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

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

Make checks payable to:
Information Systems Audit and Control Association

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

PDF

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

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

Chapter Name	Chapter Number	Dues
ASIA		
Hong Kong	64	$35
Bangalore, India	138	$15
Calcutta	165	⁕
Coimbatore, India	155	⁕
Delhi, India	140	$10
Hyderabad, India	164	$17
Madras, India (Chennai)	99	$5
Mumbai, India	145	$20
Pune, India	159	$17
Indonesia	123	⁕
Nagoya, Japan	118	⁕
Osaka, Japan	103	⁕
Tokyo, Japan	89	$180
Korea	107	$30
Malaysia	93	$10
Muscat, Oman	167	⁕
Karachi, Pakistan	148	$12.50
Manila, Philippines	136	$25
Jeddah, Saudi Arabia	163	$0
Riyadh, Saudi Arabia	154	$0
Singapore	70	$10
Sri Lanka	141	$15
Taiwan	142	$35
Bangkok, Thailand	109	$9
UAE	150	$10
CENTRAL/SOUTH AMERICA		
Buenos Aires, Argentina	124	$150
Mendoza, Argentina	144	$120
São Paulo, Brazil	166	$25
Santiago de Chile	135	$40
Bogota, Colombia	126	$50
San Jose, Costa Rica	31	$33
Merida, Yucatan, Mexico	101	$50
Mexico City, Mexico	14	$65
Monterrey, Mexico	80	$0
Panama	94	$20
Lima, Peru	146	$0
Puerto Rico	86	$30
Montevideo, Uruguay	133	⁕
Venezuela	113	⁕
EUROPE/AFRICA		
Austria	157	$50
Belux (Belgium and Luxembourg)	143	$40
Czech Republic	153	$110
Denmark	96	⁕
Estonian	162	$10
Finland	115	$70
Paris, France	75	⁕
German	104	$80
Athens, Greece	134	$10
Budapest, Hungary	125	$50
Irish	156	$35
Tel-Aviv, Israel	40	⁕
Milano, Italy	43	$72
Kenya	158	$40
Latvia	139	$10
Netherlands	97	$30
Lagos, Nigeria	149	$20
Oslo, Norway	74	$40
Warsaw, Poland	151	$0
Slovenia	137	$50
Slovensko	160	$40
South Africa	130	$50
Madrid, Spain	112	⁕
Sweden	88	$45
Switzerland	116	$35
London, UK	60	$88
Central UK	132	$35
Northern UK	111	$50
NORTH AMERICA		
Canada		
Calgary, AB	121	$0
Edmonton, AB	131	$25
Vancouver, BC	25	$15
Victoria, BC	100	$0
Winnipeg, MB	72	$15
Nova Scotia	105	$0
Ottawa Valley, ON	32	$10
Toronto, ON	21	$25
Montreal, PQ	36	$15
Quebec City, PQ	91	$35
Islands		
Bermuda	147	$0
Trinidad & Tobago	106	$25
Midwestern United States		
Chicago, IL	02	$50
Illini (Springfield, IL)	77	$30
Central Indiana (Indianapolis)	56	$25
Michiana (South Bend, IN)	127	$25
Iowa (Des Moines)	110	$25
Kentuckiana (Louisville, KY)	37	$30
Detroit, MI	08	$35
Western Michigan (Grand Rapids)	38	$25
Minnesota (Minneapolis)	07	$30
Omaha, NE	23	$30
Central Ohio (Columbus)	27	$25
Greater Cincinnati, OH	03	$20
Northeast Ohio (Cleveland)	26	$30
Kettle Moraine, WI (Milwaukee)	57	$25
Northeastern United States		
Greater Hartford, CT (Southern New England)	28	$35
Central Maryland (Baltimore)	24	$25
New England (Boston, MA)	18	$30
New Jersey (Newark)	30	$40
Central New York (Syracuse)	29	$30
Hudson Valley, NY (Albany)	120	$0
New York Metropolitan	10	$50
Western New York (Buffalo)	46	$30
Harrisburg, PA	45	$30
Lehigh Valley (Allentown, PA)	122	$35
Philadelphia, PA	06	$40
Pittsburgh, PA	13	$20
National Capital Area, DC	05	$30
Southeastern United States		
North Alabama (Birmingham)	65	$30
Jacksonville, FL	58	$30
Central Florida (Orlando)	67	$30
South Florida (Miami)	33	$40
West Florida (Tampa)	41	$35
Atlanta, GA	39	$30
Charlotte, NC	51	$35
Research Triangle (Raleigh, NC)	59	$25
Piedmont/Triad (Winston-Salem, NC)	128	$30
Greenville, SC	54	$30
Memphis, TN	48	$45
Middle Tennessee (Nashville)	102	$45
Virginia (Richmond)	22	$30
Southwestern United States		
Central Arkansas (Little Rock)	82	$60
Central Mississippi (Jackson)	161	$25
Denver, CO	16	$35
Greater Kansas City, KS	87	$25
Baton Rouge, LA	85	$25
Greater New Orleans, LA	61	$20
St. Louis, MO	11	$25
New Mexico (Albuquerque)	83	$25
Central Oklahoma (OK City)	49	$30
Tulsa, OK	34	$25
Austin, TX	20	$25
Greater Houston Area, TX	09	$40
North Texas (Dallas)	12	$30
San Antonio/So. Texas	81	$25
Western United States		
Phoenix, AZ	53	$30
Los Angeles, CA	01	$25
Orange County, CA (Anaheim)	79	$30
Sacramento, CA	76	$20
San Francisco, CA	15	$45
San Diego, CA	19	$30
Silicon Valley, CA (Sunnyvale)	62	$25
Hawaii (Honolulu)	71	$30
Boise, ID	42	$30
Willamette Valley, OR (Portland)	50	$30
Utah (Salt Lake City)	04	$30
Mt. Rainier, WA (Olympia)	129	$20
Puget Sound, WA (Seattle)	35	$35
OCEANIA		
Adelaide, Australia	68	$0
Brisbane, Australia	44	$16
Canberra, Australia	92	$30
Melbourne, Australia	47	$30
Perth, Australia	63	$5
Sydney, Australia	17	$30
Auckland, New Zealand	84	$24
Wellington, New Zealand	73	$22
Papua New Guinea	152	$0

⁕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

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

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

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

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

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

Information Systems Audit and Control Association®

proud sponsor of the

CISA®

CERTIFIED INFORMATION SYSTEMS AUDITOR

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

As an Employer

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

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

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

As an IT Professional

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

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

Requirements for CISA certification

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

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

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

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

GOVERNANCE INSTITUTE™

COBIT®

3rd Edition

Audit Guidelines

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

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 1-893209-18-0 (*Audit Guidelines*)
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.

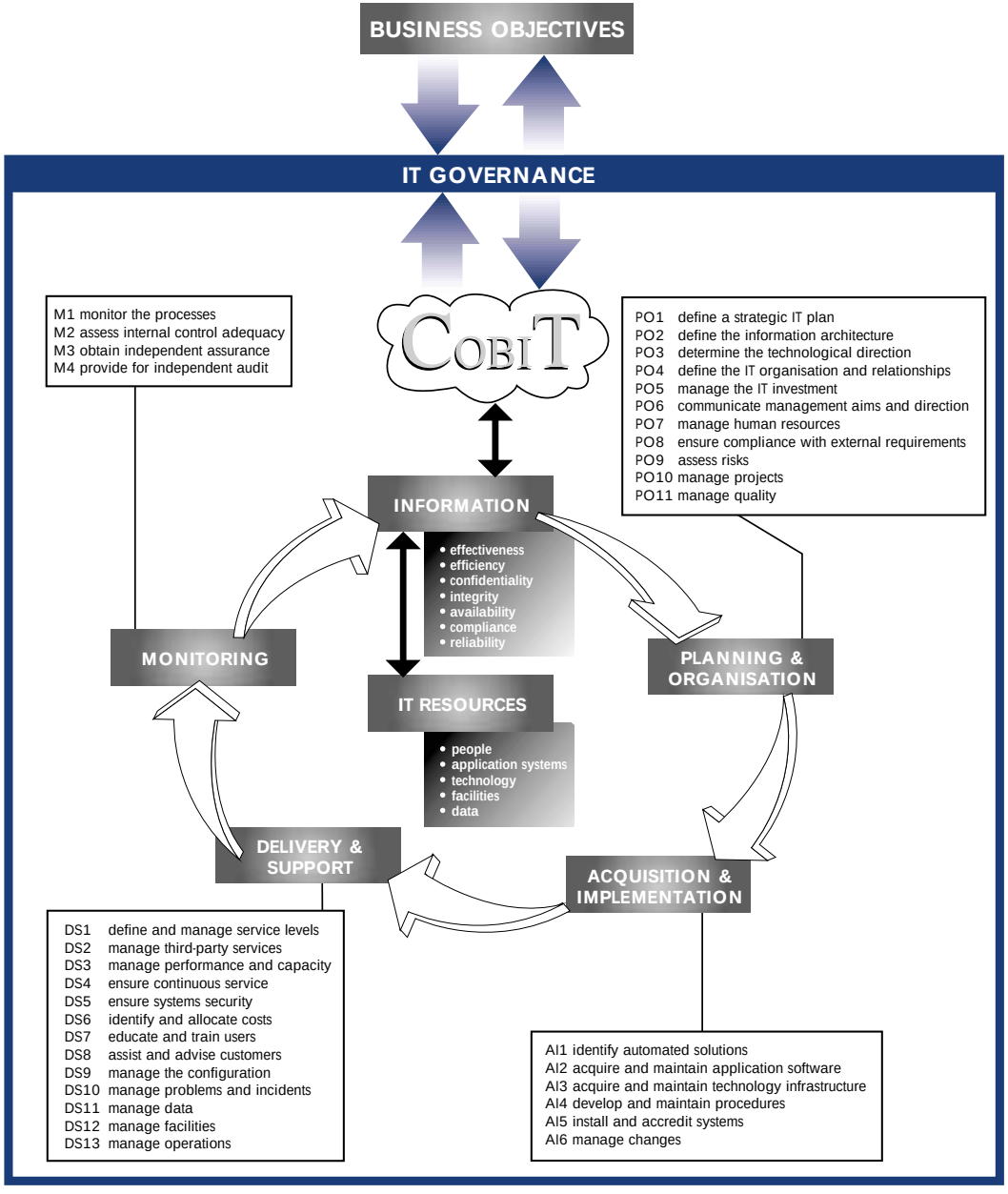
Specifically, COBIT provides **Maturity Models** for control over IT processes, so that management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be; **Critical Success Factors**,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

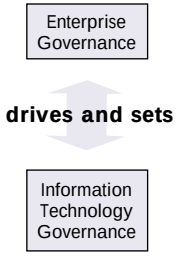
EMERGENCE OF ENTERPRISE AND IT GOVERNANCE

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

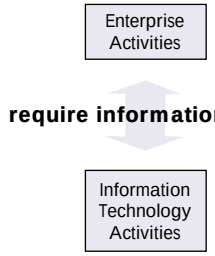
enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy.

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.

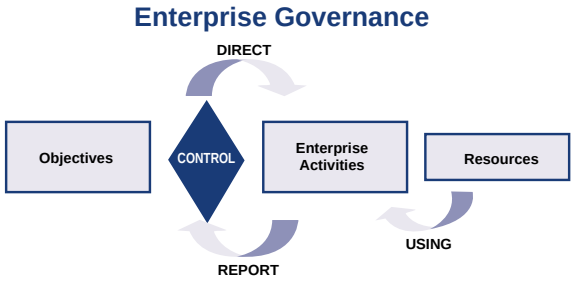
Looking at the interplay of enterprise and IT governance processes in more detail, enterprise governance, the system by which entities are directed and controlled, drives and sets IT governance. At the same time, IT should provide critical input to, and constitute an important component of, strategic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

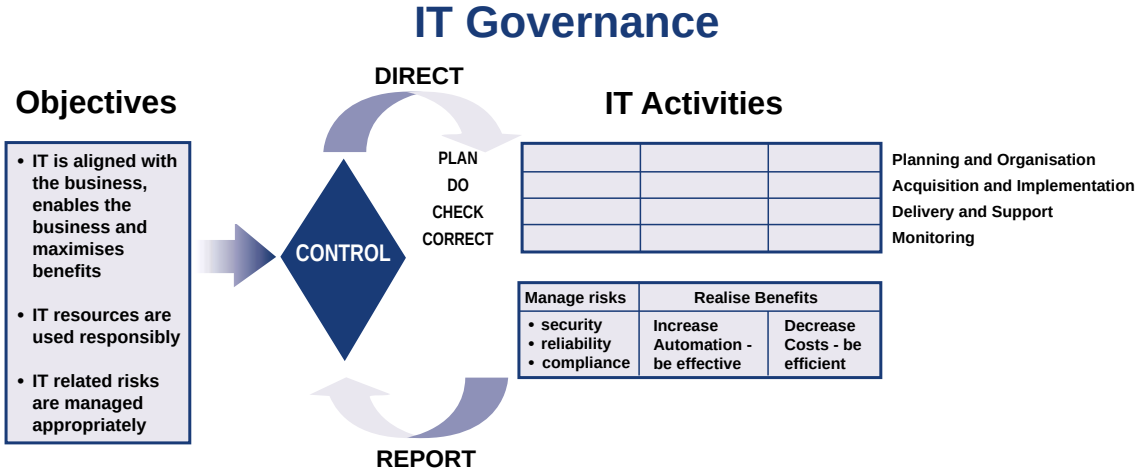


Enterprises are governed by generally accepted good (or best) practices, to ensure that the enterprise is achieving its goals-the assurance of which is guaranteed by certain controls. From these objectives flows the organisation's direction, which dictates certain enterprise activities, using the enterprise's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

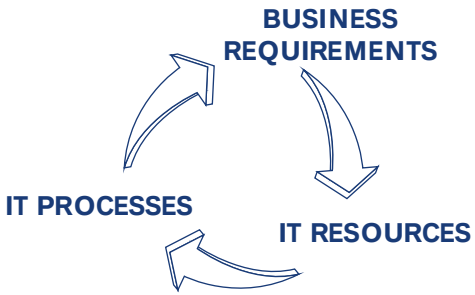
IT Control Objective is defined as a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

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.

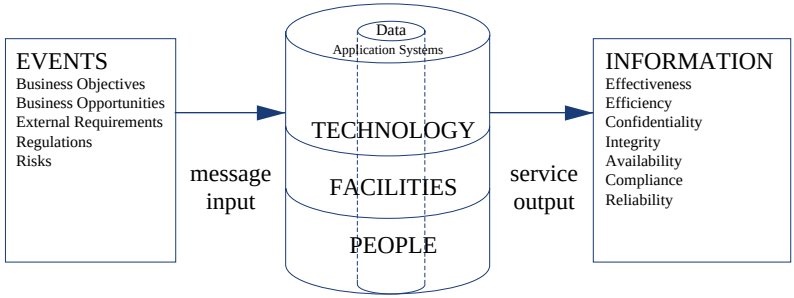
Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.

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

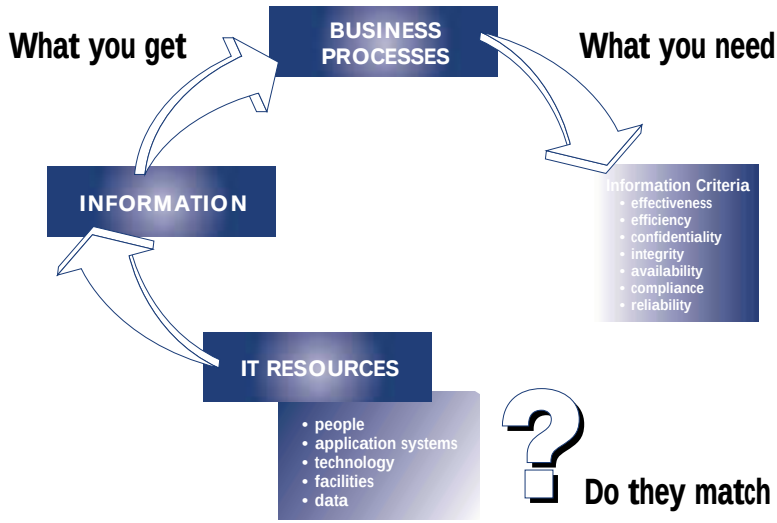
People include staff skills, awareness and productivity to plan, organise, acquire, deliver, support and monitor information systems and services.

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.

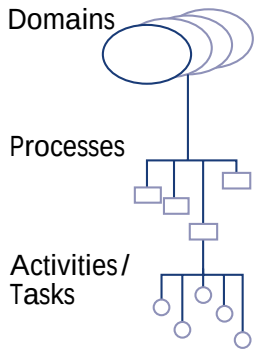


In order to ensure that the business requirements for information are met, adequate control measures need to be defined, implemented and monitored over these resources. How then can organisations satisfy themselves that the information they get exhibits the characteristics they need? This is where a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

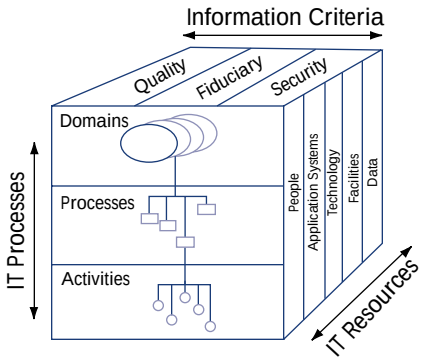


THE FRAMEWORK'S PRINCIPLES, *continued*

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.

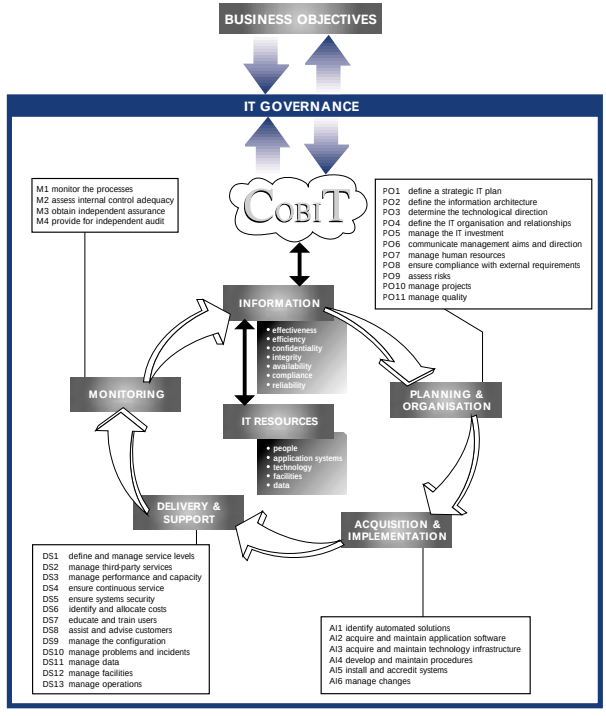
It is clear that all control measures will not necessarily satisfy the different business requirements for information to the same degree.

- **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 Objective*s, 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.

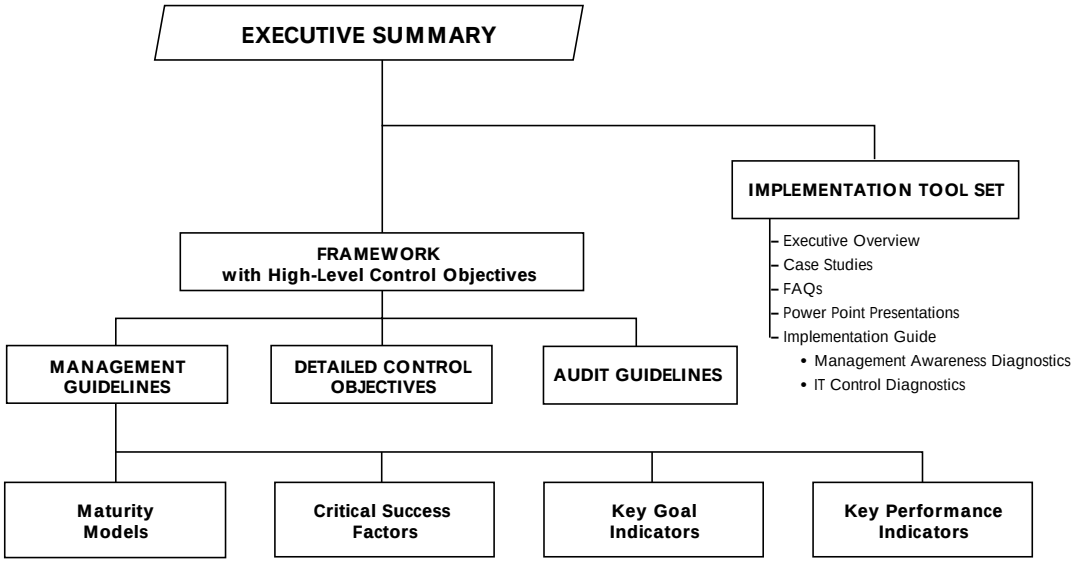
Refer to Appendix II, COBIT Project Description; Appendix III, COBIT Primary Reference Material; and Appendix IV, Glossary of Terms.

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



INTRODUCTION TO AUDIT GUIDELINES

COBIT & THE *AUDIT GUIDELINES*

The *Audit Guidelines* provide a complementary tool to enable the easy application of the COBIT *Framework* and *Control Objectives* within audit and assessment activities. The purpose of the *Audit Guidelines* is to provide a simple structure for auditing and assessing controls based upon generally accepted audit practices that fits within the overall COBIT scheme.

Individual audit objectives and practices vary considerably from organisation to organisation and there are many kinds of practitioners involved in audit-related activity, e.g., external auditors, internal auditors, evaluators, quality reviewers and technical assessors. For these reasons, the *Audit Guidelines* are generic and high level in their structure.

Auditors have a general requirement to provide management and the business process owners with assurance and advice regarding controls in an organisation; to provide reasonable assurance that relevant control objectives are being met; to identify where there are significant weaknesses in those controls; to substantiate the risk that may be associated with such weaknesses; and, finally, to advise these executives on the corrective actions that should be taken. COBIT provides clear policies and good practices for security and control of information and related technology. Therefore, basing the *Audit Guidelines* firmly on the *Control Objectives* takes the auditor's opinion out of the audit conclusion, replacing it with authoritative criteria (41 standards and best practice statements from private and public standards setting bodies worldwide).

These *Audit Guidelines* provide guidance for preparing audit plans that are integrated with the COBIT *Framework* and detailed *Control Objectives*. They should be used in conjunction with the COBIT *Framework* and *Control Objectives*, and can be developed into specific audit programmes. They are, however, neither exhaustive nor definitive. They cannot be everything to everyone and will have to be tailored for the specific environment.

There are, however, four things the *Guidelines* are not:

1. The *Audit Guidelines* are not intended as a tool for creating the overall audit plan and coverage which considers a range of factors including past weaknesses, risks to the organisation, known incidents, new developments and strategic choices. Although the *Framework* and *Control Objectives* provide direction, guidance for the exact activity is outside the scope of the *Audit Guidelines*.
2. The *Audit Guidelines* are not intended as a tool to teach the basics of auditing even though they incorporate the generally accepted basics of general and IT auditing.
3. The *Audit Guidelines* do not attempt to explain in detail how computerised planning, assessment, analysis and documentation tools (which include but extend beyond Computer Assisted Audit Techniques) can be used to support and automate the audit of IT processes. There is enormous potential for information technology to be used to enhance the efficiency and effectiveness of audits, but guidance on this topic is also outside the scope of the *Audit Guidelines*.
4. The *Audit Guidelines* are not exhaustive nor definitive, but will evolve together with COBIT and its detailed *Control Objectives*.

The COBIT *Audit Guidelines* enable the auditor to review specific IT processes against COBIT's recommended *Control Objectives* to help assure management where controls are sufficient, or to advise management where processes need to be improved.

From a management perspective, process owners will ask the questions: "Is what I am doing all right? And if not, how do I fix it?" COBIT's *Framework* and *Audit Guidelines* will help answer these questions. The approach provides a "reactive" perspective, whereas auditors also need to support management in a "proactive" manner. The *Framework* and *Audit Guidelines* are equally applicable proactively in the early stages of processes and project development — answering the question, "What do I need so it will not need to be fixed?"

GENERAL STRUCTURE OF THE *AUDIT GUIDELINES*

The most common model for assessing control is the audit model. Another increasingly adopted approach is the risk analysis model which will be covered towards the end of this introduction. All those involved in assessing control can leverage either model.

The objectives of auditing are to:

- provide management with reasonable assurance that control objectives are being met,
- where there are significant control weaknesses, to substantiate the resulting risks, and
- advise management on corrective actions

The generally accepted structure of the audit process is:

- identification and documentation
- evaluation
- compliance testing
- substantive testing

The IT process is therefore audited by:

- **Obtaining** an understanding of business requirements related risks, and relevant control measures
  - **Evaluating** the appropriateness of stated controls
    - **Assessing** compliance by testing whether the stated controls are working as prescribed, consistently and continuously
      - **Substantiating** the risk of control objectives not being met by using analytical techniques and/or consulting alternative sources.

With the aim of providing assistance to management in the form of assurance advice, we have developed this structure into an audit framework that builds on COBIT requirements:

- presentation in a tiered approach (levels)
- business objective orientation
- process driven
- focusing on
  - resources that need to be managed
  - information criteria that are required

At the highest level this general audit approach is supported by:

- the COBIT *Framework*, especially the summary with the IT process classification, the applicable information criteria and IT resources (see page 29)
- requirements for the audit process itself (see section Audit Process Requirements page 22)
- generic requirements for IT process auditing (see section Generic IT Audit Guideline, page 23)
- general principles of control (see section Control Process Observations, pages 23-24)

The second level is comprised of the detailed audit guidelines for each IT process as provided in the main body of this publication.

The guidelines have been presented in a standard template following the general structure of Obtaining, Evaluating, Assessing and Substantiating. This template has been applied to the Generic IT *Audit Guidelines* as well as to the detailed *Audit Guidelines*.

At the third and lowest level the auditor can complement the *Audit Guidelines* to meet local conditions, driving the audit planning phase with audit attention points that influence detailed control objectives by:

- sector specific criteria
- industry standards
- platform specific elements
- detailed control techniques employed

Of importance for this level, is the fact that control objectives are not necessarily applicable always and everywhere. It is therefore suggested that a high level risk assessment, be conducted to determine which objectives need to be specifically focussed on and which may be ignored.

All these elements are offered to support the planning and performance of IT audits, and a better integrated application of the detailed audit guidelines. The guidelines are not exhaustive and not universally applicable. The high level of support information (generic guidelines, audit process requirements and control observations) will help auditors develop the audit programme they need.

DETAILED STRUCTURE FOR AUDIT GUIDELINES APPLICATION

Level 1 General IT audit approach	J COBIT *Framework* J Audit Process Requirements J Control Observations J Generic Audit Guideline
Level 2 Process audit guidelines	J Detailed *Audit Guidelines*
Level 3 Audit attention points to complement detailed control objectives	J Local Conditions • sector specific criteria • industry standards • platform specific elements • detailed control techniques used

AUDIT PROCESS REQUIREMENTS

Having defined what we are going to audit and provide assurance on, we have to determine the most appropriate approach or strategy for carrying out our audit work. First we need to *determine the correct scope of our audit*. To achieve this we need to investigate, analyse and define:

- the business processes concerned
- the platforms and information systems which are supporting the business process as well as interconnectivity with other platforms or systems
- the IT roles and responsibilities defined, including what has been in- or out-sourced
- associated business risks and strategic choices

The next step is to *identify the information requirements* which are of particular relevance with respect to the business processes. Then we will need to *identify the inherent IT risks as well as overall level of control* which can be associated with the business process. To achieve this we identify:

- recent changes in the business environment having an IT impact
- recent changes to the IT environment, new developments, etc.
- recent incidents relevant to the controls and business environment
- IT monitoring controls applied by management
- recent audit and/or certification reports
- recent results of self assessments

On the basis of the information obtained, we can now select the relevant COBIT processes as well as the resources that apply to them. This could require that certain COBIT processes will need to be audited several times, each time for a different platform or system.

One should determine an audit strategy on the basis of which detailed audit plan should be further elaborated, e.g., is one going for a controls based approach or a substantive approach.

Finally, all the steps, tasks and decision points to perform the audit need to be considered. An example of a generic audit process (with steps, tasks and decision points), following the standard template, is provided in Appendix V.

AUDIT PROCESS REQUIREMENTS

• **define audit scope**	J business process concerned J platforms, systems and their interconnectivity, supporting the process J roles, responsibilities and organisational structure
• **identify information requirements relevant for the business process**	J relevance to the business process
• **identify inherent IT risks and overall level of control**	J recent changes and incidents in business and technology environment J results of audits, self-assessments and certification J monitoring controls applied by management
• **select processes and platforms to audit**	J processes J resources
• **set audit strategy**	J controls X risk J steps and tasks J decision points

GENERIC IT AUDIT GUIDELINE

The template on page 25 (and also provided as a foldout at the end of this document) presents the generic requirements for auditing IT processes to provide the first level of audit guidelines, generally applicable to all processes. It is primarily oriented towards process understanding and determining ownership and should be a foundation and reference framework for any detailed audit guidelines.

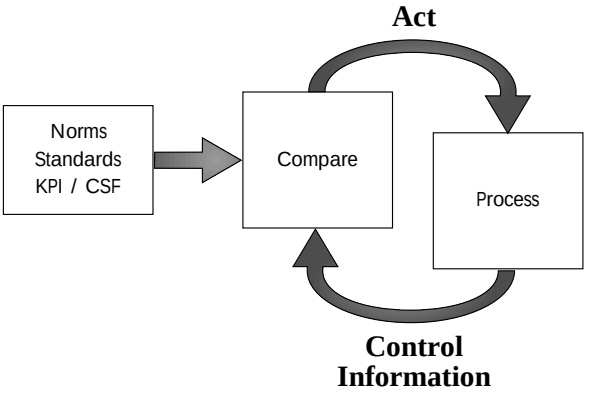
This same template is then applied to the 34 processes as identified in the COBIT *Framework.*

CONTROL PROCESS OBSERVATIONS

The general principles of control can also supply additional insight on how to further complement the *Audit Guidelines*. These principles are primarily focused on process and control responsibilities, control standards and control information flows.

Control, from a management point-of-view, is defined as determining what is being accomplished; that is, evaluating the performance and if necessary applying corrective measures so that the performance takes place according to plan.

The control process consists of four steps. First, a standard of desired performance is specified for a process. Second, there is a means of sensing what is happening in the process, i.e., the process delivers control information to a control unit. Third, the control unit compares the information with the standard. Fourth, if what is actually happening does not conform to the standard, the control unit directs that corrective action be taken, conveyed as information back to the process.



From this model, the following control observations may bear relevance to audit:

1. For this model to work, the *responsibility* for the business (or in this case IT) process must be clear and that accountability must be unambiguous. If not, control information will not flow and corrective action will not be acted upon.
2. *Standards* can be of a very wide variety, from high-level plans and strategies to detailed measurable key performance indicators (KPI) and critical success factors (CSF). Clearly documented, maintained and communicated standards are a must for a good control process. Clear responsibility for custodianship of these standards also is a requirement for good control.
3. The *control process* has the same requirements: well documented as to how it works with clear responsibilities. An important aspect is the clear definition of what constitutes a deviation, i.e., what are the limits of deviation.
4. The timeliness, integrity and appropriateness of *control information*, as well as other information, is basic to the good functioning of the control system and is something the auditor must address.
5. Both control information and corrective action information will have requirements as to *evidence* in order to establish *accountability* after the fact.

GENERIC AUDIT GUIDELINE

OBTAINING AN UNDERSTANDING

The audit steps to be performed to document the activities underlying the control objectives as well as to identify the stated control measures/procedures in place.

Interview appropriate management and staff to gain an understanding of:

- Business requirements and associated risks
- Organisation structure
- Roles and responsibilities
- Policies and procedures
- Laws and regulations
- Control measures in place
- Management reporting (status, performance, action items)

Document the process-related IT resources particularly affected by the process under review. Confirm the understanding of the process under review, the Key Performance Indicators (KPI) of the process, the control implications, e.g., by a process walk through.

EVALUATING THE CONTROLS

The audit steps to be performed in assessing the effectiveness of control measures in place or the degree to which the control objective is achieved. Basically deciding what, whether and how to test.

Evaluate the appropriateness of control measures for the process under review by considering identified criteria and industry standard practices, the Critical Success Factors (CSF) of the control measures and applying auditor professional judgment.

- Documented processes exist
- Appropriate deliverables exist
- Responsibility and accountability are clear and effective
- Compensating controls exist, where necessary

Conclude the degree to which the control objective is met.

ASSESSING COMPLIANCE

The audit steps to be performed to ensure that the control measures established are working as prescribed, consistently and continuously and to conclude on the appropriateness of the control environment.

Obtain direct or indirect evidence for selected items/periods to ensure that the procedures have been complied with for the period under review using both direct and indirect evidence.

Perform a limited review of the adequacy of the process deliverables.

Determine the level of substantive testing and additional work needed to provide assurance that the IT process is adequate.

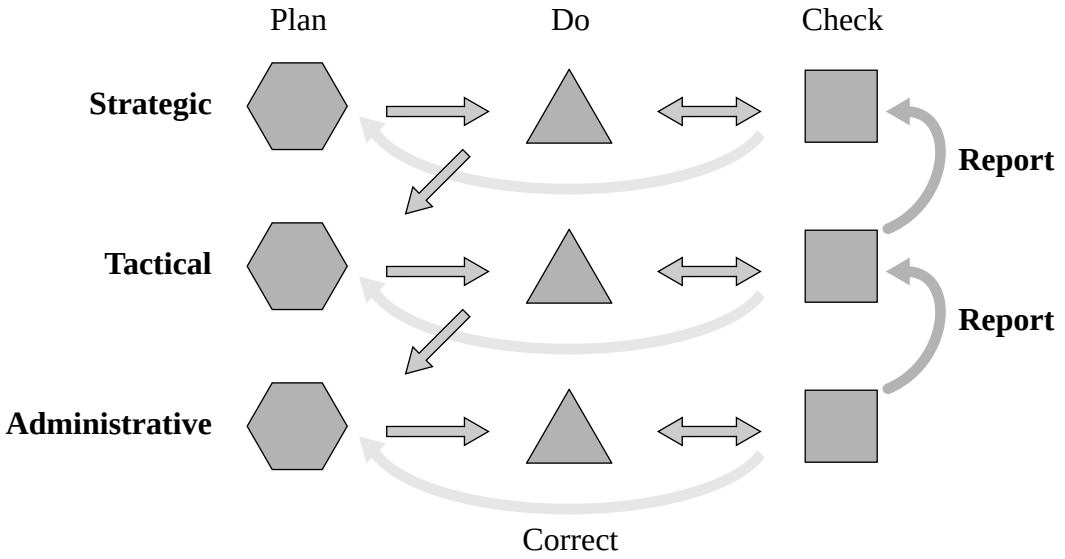
SUBSTANTIATING THE RISK

The audit steps to be performed to substantiate the risk of the control objective not being met by using analytical techniques and/or consulting alternative sources. The objective is to support the opinion and to 'shock' management into action. Auditors have to be creative in finding and presenting this often sensitive and confidential information.

Document the control weaknesses, and resulting threats and vulnerabilities.

Identify and document the actual and potential impact; e.g., through root-cause analysis.

Provide comparative information, e.g., through benchmarks.



Controls also operate at different levels in the traditional Plan-Do-Check-Correct cycle that management is comfortable with. This model illustrates

- the logical sequence of plan-do-check and correct the plan if necessary
- how this happens at strategic, tactical and administrative levels
- several lateral and horizontal relationships
  - strategic 'doing' results in tactical planning
  - tactical 'doing' results in administrative planning
  - the 'checking' and 'doing' activities continually cooperate and influence each other
  - the administrative 'checking' activity reports up to tactical 'checking' which in its turn reports up to strategic checking

When assessing control mechanisms, reviewers should be aware that controls operate at these different levels and that they have intricate relationships. COBIT's process orientation provides some indication as to different control processes, levels and interrelationships, but actual implementation or assessment of control systems needs to take this added complex dimension into account.

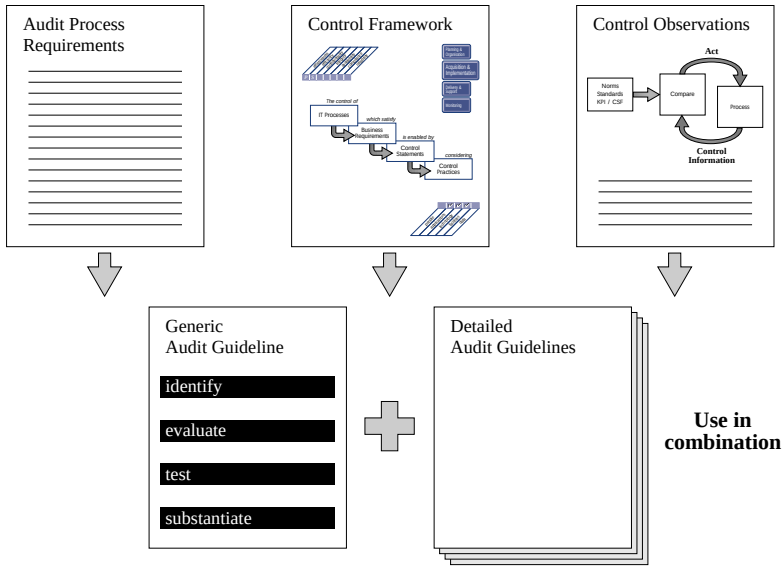
PUTTING IT ALL TOGETHER

In summary, the detailed *Audit Guidelines* can always be complemented by considering the Generic Guideline and the process under review, and obtain further audit tasks to achieve the audit objective. The audit programme development itself can benefit from considering the IT audit process requirements, the COBIT *Framework* and High-Level *Control Objectives*, and the Control Considerations stated above.

LINK BETWEEN *CONTROL OBJECTIVES* AND *AUDIT GUIDELINES*

Objectives have been developed from a process orientation because management is looking for pro-active advice on how to address the issue of keeping IT under control. The *Control Objectives* help management establish control over the process, the *Audit Guidelines* assist the auditor or assessor to provide assurance that the process is actually under control so that the information requirements necessary to achieve business objectives will be satisfied.

The link between the two is the process, hence the *Audit Guidelines* have been developed for each process as opposed to for each control objective.



In reference to the control framework represented by the waterfall model, the *Audit Guidelines* can be seen as providing the feedback from the control processes back to the business objectives. The control objectives are the guide going down the waterfall to get the IT process under control. The *Audit Guidelines* are the guide for going back-up the waterfall with the question: "Is there assurance that the business objective will be achieved?" Sometimes *Audit Guidelines* are straight translations from the *Control Objectives;* more often the guidelines look for evidence that the process is under control.

OPPORTUNITIES AND CHALLENGES FOR THE ASSESSMENT TASKS

Using the *Framework*, *Control Objectives* and the *Audit Guidelines* as the basis for the audit/assessment task present some definite advantages:

- allows for prioritising audit activities and areas under review, using the Primary and Secondary rating of the information criteria
- leads to investigation of areas that normally — without a framework or model — would not have been addressed
- a more logical set up and sequence of interviews can be developed as auditors step their way through the process
- investigations can be focussed using the indicator of which resource is more important in which process
- as a standard to define auditable IT areas for the strategic audit plan to ensure
  - effective audit coverage
  - timely acquisition/building of necessary audit skills

However, there are also some challenges in integrating framework and objectives into the audit work:

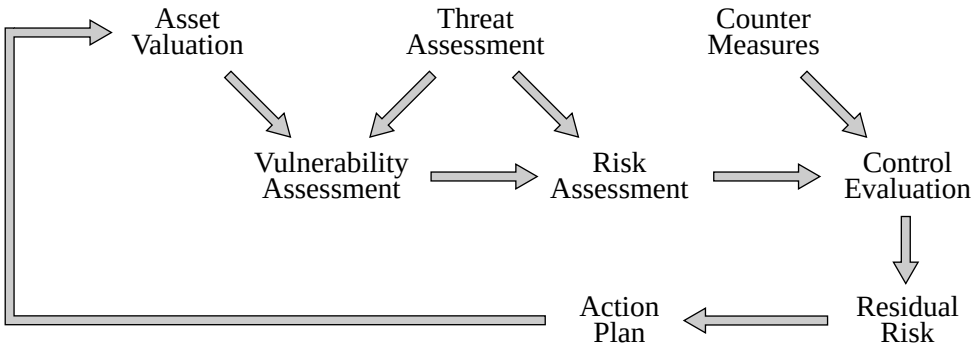
- change never comes easy (attitude, toolset, skill set, etc.)
- the detailed nature makes the initial application cumbersome especially when checking completeness and applicability of the control objectives for the area under review
- there is a necessary degree of repetition in the *Audit Guidelines* because there is rarely a one-to-one relationship between the control objective and the control mechanisms, one mechanism contributing in varying ways to several objectives, one objective needing several mechanisms to be achieved
- enforces some formalism (e.g., recording background information) that may seem unnecessary

RISK ANALYSIS AS AN ALTERNATIVE ASSESSMENT APPROACH

Balancing cost and risk is the next issue to address, i.e., making a conscious choice of how and whether to implement each control objective. Risk analysis approaches address this choice, even though the pro-active principle remains; control objectives should be applied in the first place to achieve an information control criteria (effectiveness, efficiency, confidentiality, availability, integrity, compliance and reliability). It is self-evident that some form of business risk assessment needs to be used by management to define the measures to implement (see CO PO9). Auditors also will do some form of risk assessment when choosing process domains and control objectives for review.

A commonly accepted approach for risk analysis in IT is as follows:

Risk Analysis Framework



The model starts from the valuation of assets which in the COBIT *Framework* consists of the information that has the required criteria to help achieve the business objectives (including all the resources necessary to produce that information). The next step is the vulnerability analysis† which looks at the importance of the information criteria in the process under review, i.e., if a business process is vulnerable to integrity loss, then specific measures are required. Next one looks at threats, i.e., that which can exploit a vulnerability. The probability of the threat, the degree of vulnerability and the severity of the impact are combined to conclude on the risk assessment. This is followed by the selection of countermeasures (controls) and an evaluation of their effectiveness, which also identifies residual risk. The conclusion is an action plan after which the cycle can start again.

† the result of a vulnerability analysis is the identification of relevant threats and the result of a threat analysis is the identification of relevant vulnerabilites.

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							IT Resources				
			effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	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

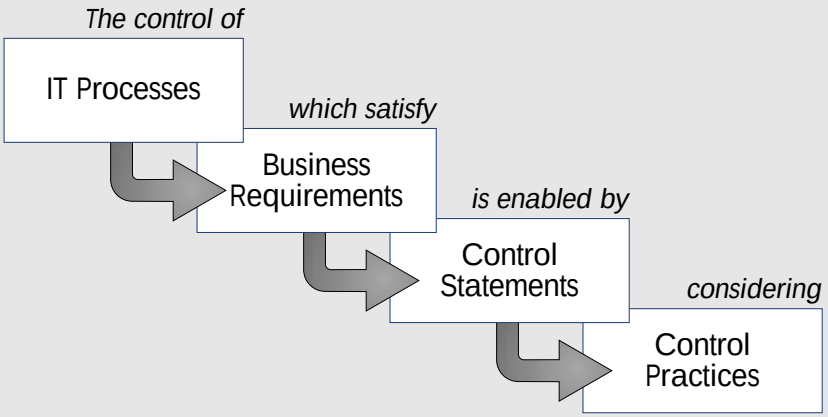
AUDIT GUIDELINES NAVIGATION OVERVIEW

The Audit Guidelines section contains detailed audit guidelines for each of the 34 IT processes. On the left page is the high-level control objective. 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. Beginning on the right page, are the descriptions of the audit guidelines for the IT process.

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.

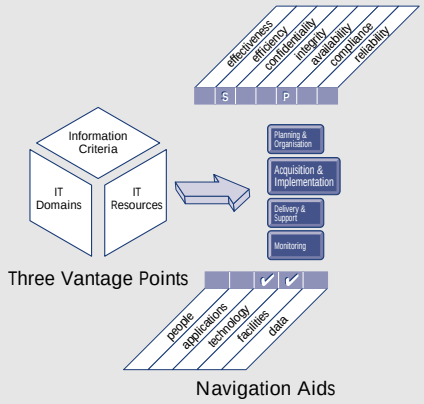
The control objectives have been organised by process/activity, but navigation aids have been provided not only to facilitate entry from any one vantage point, but also to facilitate combined or global approaches, such as installation/implementation of a process, global management responsibilities for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



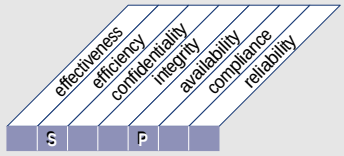
AUDIT GUIDELINES NAVIGATION OVERVIEW, *continued*

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.

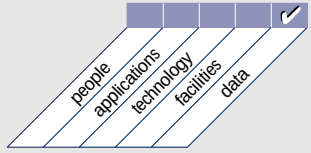


IT domains are identified by this icon in the UPPER RIGHT CORNER of each page in the Audit Guidelines section, with the domain under review highlighted and enlarged.

The cue to information criteria will be provided in the UPPER LEFT CORNER in the Audit Guidelines 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 Audit Guidelines 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.



CONTROL OBJECTIVE RELATIONSHIPS
DOMAINS, PROCESSES AND CONTROL OBJECTIVES

PLANNING & ORGANISATION

1.0 Define a Strategic IT Plan
- 1.1 IT as Part of the Organisation's Long- and Short-Range Plan
- 1.2 IT Long-Range Plan
- 1.3 IT Long-Range Planning—Approach and Structure
- 1.4 IT Long-Range Plan Changes
- 1.5 Short-Range Planning for the IT Function
- 1.6 Communication of IT Plans
- 1.7 Monitoring and Evaluating of IT Plans
- 1.8 Assessment of Existing Systems

2.0 Define the Information Architecture
- 2.1 Information Architecture Model
- 2.2 Corporate Data Dictionary and Data Syntax Rules
- 2.3 Data Classification Scheme
- 2.4 Security Levels

3.0 Determine Technological Direction
- 3.1 Technological Infrastructure Planning
- 3.2 Monitor Future Trends and Regulations
- 3.3 Technological Infrastructure Contingency
- 3.4 Hardware and Software Acquisition Plans
- 3.5 Technology Standards

4.0 Define the IT Organisation and Relationships
- 4.1 IT Planning or Steering Committee
- 4.2 Organisational Placement of the IT Function
- 4.3 Review of Organisational Achievements
- 4.4 Roles and Responsibilities
- 4.5 Responsibility for Quality Assurance
- 4.6 Responsibility for Logical and Physical Security
- 4.7 Ownership and Custodianship
- 4.8 Data and System Ownership
- 4.9 Supervision
- 4.10 Segregation of Duties
- 4.11 IT Staffing
- 4.12 Job or Position Descriptions for IT Staff
- 4.13 Key IT Personnel
- 4.14 Contracted Staff Policies and Procedures
- 4.15 Relationships

5.0 Manage the IT Investment
- 5.1 Annual IT Operating Budget
- 5.2 Cost and Benefit Monitoring
- 5.3 Cost and Benefit Justification

6.0 Communicate Management Aims and Direction
- 6.1 Positive Information Control Environment
- 6.2 Management's Responsibility for Policies
- 6.3 Communication of Organisation Policies
- 6.4 Policy Implementation Resources
- 6.5 Maintenance of Policies
- 6.6 Compliance with Policies, Procedures and Standards
- 6.7 Quality Commitment
- 6.8 Security and Internal Control Framework Policy
- 6.9 Intellectual Property Rights
- 6.10 Issue-Specific Policies
- 6.11 Communication of IT Security Awareness

7.0 Manage Human Resources
- 7.1 Personnel Recruitment and Promotion
- 7.2 Personnel Qualifications
- 7.3 Roles and Responsibilities
- 7.4 Personnel Training
- 7.5 Cross-Training or Staff Back-up
- 7.6 Personnel Clearance Procedures
- 7.7 Employee Job Performance Evaluation
- 7.8 Job Change and Termination

8.0 Ensure Compliance with External Requirements
- 8.1 External Requirements Review
- 8.2 Practices and Procedures for Complying with External Requirements
- 8.3 Safety and Ergonomic Compliance
- 8.4 Privacy, Intellectual Property and Data Flow
- 8.5 Electronic Commerce
- 8.6 Compliance with Insurance Contracts

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

9.0 Assess Risks
- 9.1 Business Risk Assessment
- 9.2 Risk Assessment Approach
- 9.3 Risk Identification
- 9.4 Risk Measurement
- 9.5 Risk Action Plan
- 9.6 Risk Acceptance
- 9.7 Safeguard Selection
- 9.8 Risk Assessment Commitment

10.0 Manage Projects
- 10.1 Project Management Framework
- 10.2 User Department Participation in Project Initiation
- 10.3 Project Team Membership and Responsibilities
- 10.4 Project Definition
- 10.5 Project Approval
- 10.6 Project Phase Approval
- 10.7 Project Master Plan
- 10.8 System Quality Assurance Plan
- 10.9 Planning of Assurance Methods
- 10.10 Formal Project Risk Management
- 10.11 Test Plan
- 10.12 Training Plan
- 10.13 Post-Implementation Review Plan

11.0 Manage Quality
- 11.1 General Quality Plan
- 11.2 Quality Assurance Approach
- 11.3 Quality Assurance Planning
- 11.4 Quality Assurance Review of Adherence to IT Standards and Procedures
- 11.5 System Development Life Cycle Methodology
- 11.6 System Development Life Cycle Methodology for Major Changes to Existing Technology
- 11.7 Updating of the System Development Life Cycle Methodology
- 11.8 Coordination and Communication
- 11.9 Acquisition and Maintenance Framework for the Technology Infrastructure
- 11.10 Third-Party Implementor Relationships
- 11.11 Programme Documentation Standards
- 11.12 Programme Testing Standards
- 11.13 System Testing Standards
- 11.14 Parallel/Pilot Testing
- 11.15 System Testing Documentation
- 11.16 Quality Assurance Evaluation of Adherence to Development Standards
- 11.17 Quality Assurance Review of the Achievement of IT Objectives
- 11.18 Quality Metrics
- 11.19 Reports of Quality Assurance Reviews

ACQUISITION & IMPLEMENTATION

1.0 Identify Automated Solutions
- 1.1 Definition of Information Requirements
- 1.2 Formulation of Alternative Courses of Action
- 1.3 Formulation of Acquisition Strategy
- 1.4 Third-Party Service Requirements
- 1.5 Technological Feasibility Study
- 1.6 Economic Feasibility Study
- 1.7 Information Architecture
- 1.8 Risk Analysis Report
- 1.9 Cost-Effective Security Controls
- 1.10 Audit Trails Design
- 1.11 Ergonomics
- 1.12 Selection of System Software
- 1.13 Procurement Control
- 1.14 Software Product Acquisition
- 1.15 Third-Party Software Maintenance
- 1.16 Contract Application Programming
- 1.17 Acceptance of Facilities
- 1.18 Acceptance of Technology

2.0 Acquire and Maintain Application Software
- 2.1 Design Methods
- 2.2 Major Changes to Existing Systems
- 2.3 Design Approval
- 2.4 File Requirements Definition and Documentation
- 2.5 Programme Specifications
- 2.6 Source Data Collection Design

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

ACQUISITION & IMPLEMENTATION *continued*

- 2.7 Input Requirements Definition and Documentation
- 2.8 Definition of Interfaces
- 2.9 User-Machine Interface
- 2.10 Processing Requirements Definition and Documentation
- 2.11 Output Requirements Definition and Documentation
- 2.12 Controllability
- 2.13 Availability as a Key Design Factor
- 2.14 IT Integrity Provisions in Application Programme Software
- 2.15 Application Software Testing
- 2.16 User Reference and Support Materials
- 2.17 Reassessment of System Design

3.0 Acquire and Maintain Technology Infrastructure

- 3.1 Assessment of New Hardware and Software
- 3.2 Preventative Maintenance for Hardware
- 3.3 System Software Security
- 3.4 System Software Installation
- 3.5 System Software Maintenance
- 3.6 System Software Change Controls
- 3.7 Use and Monitoring of System Utilities

4.0 Develop and Maintain Procedures

- 4.1 Operational Requirements and Service Levels
- 4.2 User Procedures Manual
- 4.3 Operations Manual
- 4.4 Training Materials

5.0 Install and Accredit Systems

- 5.1 Training
- 5.2 Application Software Performance Sizing
- 5.3 Implementation Plan
- 5.4 System Conversion
- 5.5 Data Conversion
- 5.6 Testing Strategies and Plans
- 5.7 Testing of Changes
- 5.8 Parallel/Pilot Testing Criteria and Performance
- 5.9 Final Acceptance Test
- 5.10 Security Testing and Accreditation
- 5.11 Operational Test
- 5.12 Promotion to Production
- 5.13 Evaluation of Meeting User Requirements
- 5.14 Management's Post-Implementation Review

6.0 Manage Changes

- 6.1 Change Request Initiation and Control
- 6.2 Impact Assessment
- 6.3 Control of Changes
- 6.4 Emergency Changes
- 6.5 Documentation and Procedures
- 6.6 Authorised Maintenance
- 6.7 Software Release Policy
- 6.8 Distribution of Software

DELIVERY & SUPPORT

1.0 Define and Manage Service Levels

- 1.1 Service Level Agreement Framework
- 1.2 Aspects of Service Level Agreements
- 1.3 Performance Procedures
- 1.4 Monitoring and Reporting
- 1.5 Review of Service Level Agreements and Contracts
- 1.6 Chargeable Items
- 1.7 Service Improvement Programme

2.0 Manage Third-Party Services

- 2.1 Supplier Interfaces
- 2.2 Owner Relationships
- 2.3 Third-Party Contracts
- 2.4 Third-Party Qualifications
- 2.5 Outsourcing Contracts
- 2.6 Continuity of Services
- 2.7 Security Relationships
- 2.8 Monitoring

3.0 Manage Performance and Capacity

- 3.1 Availability and Performance Requirements
- 3.2 Availability Plan
- 3.3 Monitoring and Reporting
- 3.4 Modeling Tools
- 3.5 Proactive Performance Management
- 3.6 Workload Forecasting

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

- 3.7 Capacity Management of Resources
- 3.8 Resources Availability
- 3.9 Resources Schedule

4.0 Ensure Continuous Service

- 4.1 IT Continuity Framework
- 4.2 IT Continuity Plan Strategy and Philosophy
- 4.3 IT Continuity Plan Contents
- 4.4 Minimising IT Continuity Requirements
- 4.5 Maintaining the IT Continuity Plan
- 4.6 Testing the IT Continuity Plan
- 4.7 IT Continuity Plan Training
- 4.8 IT Continuity Plan Distribution
- 4.9 User Department Alternative Processing Back-up Procedures
- 4.10 Critical IT Resources
- 4.11 Back-up Site and Hardware
- 4.12 Off-site Back-up Storage
- 4.13 Wrap-up Procedures

5.0 Ensure Systems Security

- 5.1 Manage Security Measures
- 5.2 Identification, Authentication and Access
- 5.3 Security of Online Access to Data
- 5.4 User Account Management
- 5.5 Management Review of User Accounts
- 5.6 User Control of User Accounts
- 5.7 Security Surveillance
- 5.8 Data Classification
- 5.9 Central Identification and Access Rights Management
- 5.10 Violation and Security Activity Reports
- 5.11 Incident Handling
- 5.12 Reaccreditation
- 5.13 Counterparty Trust
- 5.14 Transaction Authorisation
- 5.15 Non-Repudiation
- 5.16 Trusted Path
- 5.17 Protection of Security Functions
- 5.18 Cryptographic Key Management
- 5.19 Malicious Software Prevention, Detection and Correction
- 5.20 Firewall Architectures and Connections with Public Networks
- 5.21 Protection of Electronic Value

6.0 Identify and Allocate Costs

- 6.1 Chargeable Items
- 6.2 Costing Procedures
- 6.3 User Billing and Chargeback Procedures

7.0 Educate and Train Users

- 7.1 Identification of Training Needs
- 7.2 Training Organisation
- 7.3 Security Principles and Awareness Training

8.0 Assist and Advise Customers

- 8.1 Help Desk
- 8.2 Registration of Customer Queries
- 8.3 Customer Query Escalation
- 8.4 Monitoring of Clearance
- 8.5 Trend Analysis and Reporting

9.0 Manage the Configuration

- 9.1 Configuration Recording
- 9.2 Configuration Baseline
- 9.3 Status Accounting
- 9.4 Configuration Control
- 9.5 Unauthorised Software
- 9.6 Software Storage
- 9.7 Configuration Management Procedures
- 9.8 Software Accountability

10.0 Manage Problems and Incidents

- 10.1 Problem Management System
- 10.2 Problem Escalation
- 10.3 Problem Tracking and Audit Trail
- 10.4 Emergency and Temporary Access Authorisations
- 10.5 Emergency Processing Priorities

11.0 Manage Data

- 11.1 Data Preparation Procedures
- 11.2 Source Document Authorisation Procedures
- 11.3 Source Document Data Collection
- 11.4 Source Document Error Handling
- 11.5 Source Document Retention
- 11.6 Data Input Authorisation Procedures
- 11.7 Accuracy, Completeness and Authorisation Checks
- 11.8 Data Input Error Handling
- 11.9 Data Processing Integrity

DOMAINS, PROCESSES AND CONTROL OBJECTIVES

DELIVERY & SUPPORT *continued*

- 11.10 Data Processing Validation and Editing
- 11.11 Data Processing Error Handling
- 11.12 Output Handling and Retention
- 11.13 Output Distribution
- 11.14 Output Balancing and Reconciliation
- 11.15 Output Review and Error Handling
- 11.16 Security Provision for Output Reports
- 11.17 Protection of Sensitive Information During Transmission and Transport
- 11.18 Protection of Disposed Sensitive Information
- 11.19 Storage Management
- 11.20 Retention Periods and Storage Terms
- 11.21 Media Library Management System
- 11.22 Media Library Management Responsibilities
- 11.23 Back-up and Restoration
- 11.24 Back-up Jobs
- 11.25 Back-up Storage
- 11.26 Archiving
- 11.27 Protection of Sensitive Messages
- 11.28 Authentication and Integrity
- 11.29 Electronic Transaction Integrity
- 11.30 Continued Integrity of Stored Data

12.0 Manage Facilities

- 12.1 Physical Security
- 12.2 Low Profile of the IT Site
- 12.3 Visitor Escort
- 12.4 Personnel Health and Safety
- 12.5 Protection Against Environmental Factors
- 12.6 Uninterruptible Power Supply

13.0 Manage Operations

- 13.1 Processing Operations Procedures and Instructions Manual
- 13.2 Start-up Process and Other Operations Documentation
- 13.3 Job Scheduling
- 13.4 Departures from Standard Job Schedules
- 13.5 Processing Continuity
- 13.6 Operations Logs
- 13.7 Safeguard Special Forms and Output Devices
- 13.8 Remote Operations

MONITORING

1.0 Monitor the Processes

- 1.1 Collecting Monitoring Data
- 1.2 Assessing Performance
- 1.3 Assessing Customer Satisfaction
- 1.4 Management Reporting

2.0 Assess Internal Control Adequacy

- 2.1 Internal Control Monitoring
- 2.2 Timely Operation of Internal Controls
- 2.3 Internal Control Level Reporting
- 2.4 Operational Security and Internal Control Assurance

3.0 Obtain Independent Assurance

- 3.1 Independent Security and Internal Control Certification/Accreditation of IT Services
- 3.2 Independent Security and Internal Control Certification/Accreditation of Third-Party Service Providers
- 3.3 Independent Effectiveness Evaluation of IT Services
- 3.4 Independent Effectiveness Evaluation of Third-Party Service Providers
- 3.5 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments
- 3.6 Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers
- 3.7 Competence of Independent Assurance Function
- 3.8 Proactive Audit Involvement

4.0 Provide for Independent Audit

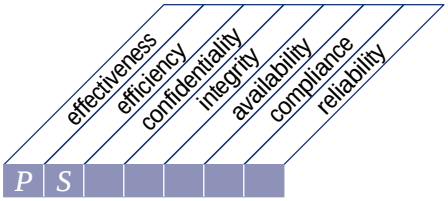
- 4.1 Audit Charter
- 4.2 Independence
- 4.3 Professional Ethics and Standards
- 4.4 Competence
- 4.5 Planning
- 4.6 Performance of Audit Work
- 4.7 Reporting
- 4.8 Follow-up Activities

AUDIT GUIDELINES

This page intentionally left blank

PLANNING & ORGANISATION

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining a strategic IT plan

that satisfies the business requirement

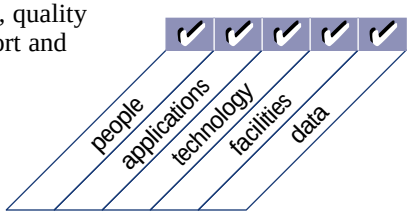
to strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment

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



DEFINE A STRATEGIC INFORMATION TECHNOLOGY PLAN

CONTROL OBJECTIVES	
1	IT as Part of the Organisation's Long-and Short-Range Plan
2	IT Long-Range Plan
3	IT Long-Range Planning — Approach and Structure
4	IT Long-Range Plan Changes
5	Short-Range Planning for the IT Function
6	Communication of IT Plans
7	Monitoring and Evaluating of IT Plans
8	Assessment of Existing Systems

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Executive Officer
Chief Operations Officer
Chief Financial Officer
Chief Information Officer
IT planning/steering committee members
IT senior management and human services staff

J **Obtaining:**

Policies and procedures relating to the planning process
Senior management steering roles and responsibilities
Organisation objectives and long- and short-range plans
IT objectives and long- and short-range plans
Status reports and minutes of planning/steering committee meetings

Evaluating the controls by:

J **Considering whether:**

IT or business enterprise policies and procedures address a structured planning approach
A methodology is in place to formulate and modify the plans and at a minimum, they cover:

- organisation mission and goals
- IT initiatives to support the organisation mission and goals
- opportunities for IT initiatives
- feasibility studies of IT initiatives
- risk assessments of IT initiatives
- optimal investment of current and future IT investments
- re-engineering of IT initiatives to reflect changes in the enterprise's mission and goals
- evaluation of the alternative strategies for data applications, technology and organisation

Organisational changes, technology evolution, regulatory requirements, business process re-engineering, staffing, in- and out-sourcing, etc. are taken into account and adequately addressed in the planning process

Long- and short-range IT plans exist, are current, adequately address the overall enterprise, its mission and key business functions

IT projects are supported by the appropriate documentation as identified in the IT planning methodology

Checkpoints exist to ensure that IT objectives and long- and short-range plans continue to meet organisational objectives and long- and short-range plans

Review and sign-off IT plan by process owners and senior management occurs

The IT plan assesses the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses

The absence of long-range planning for information systems and supporting infrastructure results in systems that do not support enterprise objectives and business processes, or do not provide appropriate integrity, security and control

Assessing the compliance by:

J **Testing that:**

Minutes from IT planning/steering committee meetings reflect the planning process

Planning methodology deliverables exist and are as prescribed

Relevant IT initiatives are included in the IT long- and short- range plans (i.e., hardware changes, capacity planning, information architecture, new system development or procurement, disaster recovery planning, installation of new processing platforms, etc.)

IT initiatives support the long- and short-range plans and consider requirements for research, training, staffing, facilities, hardware and software

Technical implications of IT initiatives have been identified

Consideration has been given to optimising current and future IT investments

IT long- and short-range plans are consistent with the organisation's long- and short-range plans and organisation requirements

Plans have been changed to reflect changing conditions

IT long-range plans are periodically translated into short-range plans

Tasks exist to implement the plans

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of strategic IT plans against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the IT plans to ensure that IT initiatives reflect the organisation's mission and goals

A detailed review of the IT plans to determine if known areas of weakness within the organisation are being identified for improvement as part of the IT solutions contained in the plans

J **Identifying:**

IT failures to meet the organisation's missions and goals

IT failures to match short-range plans with long-range plans

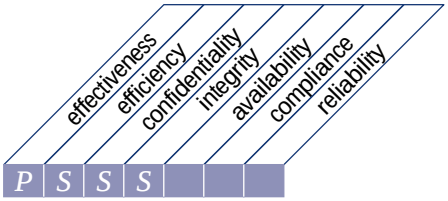
IT projects failures to meet short-range plans

IT failures to meet cost and time guidelines

Missed business opportunities

Missed IT opportunities

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining the information architecture

that satisfies the business requirement

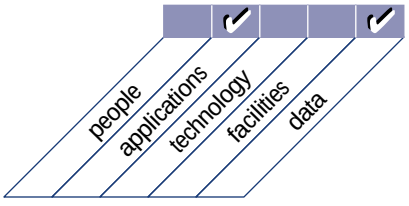
of optimising the organisation of the information systems

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



DEFINE THE INFORMATION ARCHITECTURE

CONTROL OBJECTIVES	
1	Information Architecture Model
2	Corporate Data Dictionary and Data Syntax Rules
3	Data Classification Scheme
4	Security Levels

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Information Officer
IT planning/steering committee members
IT senior management
Security Officer

J **Obtaining:**

Policies and procedures relating to the information architecture
Information architecture model
Documents supporting the information architecture model, including the corporate data model
Corporate data dictionary
Data ownership policy
Senior management steering roles and responsibilities
IT objectives and long- and short-range plans
Status reports and minutes of planning/steering committee meetings

Evaluating the controls by:

J **Considering whether:**

IT policies and procedures address the development and maintenance of the data dictionary
The process used to update the information architecture model is based on long- and short-range plans, considers associated costs and risks, and ensures that senior management sign-off is obtained prior to making changes to the model
A process is used to keep the data dictionary and data syntax rules up to date
A medium is used to distribute the data dictionary to ensure that it is accessible to development areas and that changes are reflected immediately
IT policies and procedures address the classification of data, including security categories and data ownership, and access rules for the classes of data are clearly and appropriately defined.
Standards define the default classification for data assets which do not contain a data classification identifier

Considering whether, *continued*

IT policies and procedures address the following:

- authorisation process is in place requiring the owner of the data (as defined in the data ownership policy) to authorise all access to that data and to the security attributes of the data
- security levels are defined for each data classification
- access levels are defined and are appropriate for the data classification
- access to sensitive data requires explicit access levels and data is only provided on a "need to know" basis

Assessing the compliance by:

J **Testing that:**

Changes made to the information architecture model to confirm that these changes reflect those in the IT long- and short-range plans and that associated costs and risks are identified

Assess the impact of any modifications to the data dictionary and changes made to the data dictionary to ensure that they are effectively communicated

Various operational application systems and development projects to confirm that the data dictionary is used for data definitions

Adequacy of data dictionary documentation to confirm that it defines data attributes and security levels for each data item

Appropriateness of the data classifications, security levels, access levels and defaults

That each data classification clearly defines:

- who can have access
- who is responsible for determining the appropriate level of access
- specific approval needed for access
- special requirements for access (i.e., non-disclosure or confidentiality agreement)

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of the information architecture model against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the data dictionary for completeness of key elements

A detailed review of security levels defined for sensitive data to verify that appropriate authorisation was obtained for access and access permitted is consistent with the security levels defined in the IT policies and procedures

J **Identifying:**

Inconsistencies in the information architecture model and the corporate data model, corporate data dictionary, associated information systems, and IT long- and short-range plans

Out of date corporate data dictionary items and data syntax rules where time has been lost due to poorly communicated changes to the data dictionary

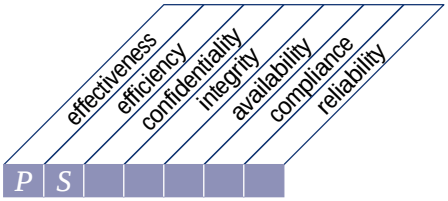
Data items where ownership is not clearly and/or appropriately defined

Data classes that are inappropriately defined

Data security levels inconsistent with the "need to know" rule

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

determining technological direction

that satisfies the business requirement

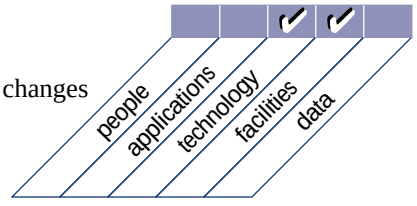
to take advantage of available and emerging technology to drive and make possible the business strategy

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



DETERMINE TECHNOLOGICAL DIRECTION

CONTROL OBJECTIVES	
1	Technological Infrastructure Planning
2	Monitoring Future Trends and Regulations
3	Technological Infrastructure Contingency
4	Hardware and Software Acquisition Plans
5	Technology Standards

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Executive Officer
Chief Operations Officer
Chief Financial Officer
Chief Information Officer
IT planning/steering committee members
IT senior management

J **Obtaining:**

Policies and procedures relating to technological infrastructure planning and monitoring
Senior management steering roles and responsibilities
Organisation objectives and long- and short-range plans
IT objectives and long- and short-range plans
IT hardware and software acquisition plan
Technological infrastructure plan
Technology standards
Status reports and minutes of planning/steering committee meetings

Evaluating the controls by:

J **Considering whether:**

There is a process for creating and regularly updating the technological infrastructure plan for confirming that proposed changes are first examined to assess associated costs and risks and that senior management sign-off is obtained prior to making changes to the plan

Technological infrastructure plan is compared to the IT long- and short-range plans

There is a process for evaluating the organisation's current technological status to ensure that it encompasses aspects such as systems architecture, technological direction and migration strategies

Considering whether, *continued*

The IT policies and procedures ensure addressing the need to evaluate and monitor current and future technology trends and regulatory conditions, and that they are taken into consideration during the development and maintenance of the technological infrastructure plan

The logistical and environmental impact of technological acquisitions are planned for

The IT policies and procedures ensure that the need to systematically assess the technological plan for contingency aspects is addressed (i.e., redundancy, resilience, adequacy and evolutionary capability of the infrastructure)

IT management evaluate emerging technologies, and incorporate appropriate technologies into the current IT infrastructure

It is the practice for the hardware and software acquisition plans to comply with the needs identified in the technological infrastructure plan and are being properly approved

Technology standards are in place for the technological components described in the technological infrastructure plan

Assessing the compliance by:

J **Testing that:**

IT management understands and uses the technological infrastructure plan

Changes made to the technological infrastructure plan to identify associated costs and risks and that these changes reflect the changes in the IT long- and short-range plans

IT management understands the process for monitoring and evaluating emerging technologies, and incorporating appropriate technologies into the current IT infrastructure

IT management understands the process for systematically assessing the technological plan for contingency aspects (i.e., redundancy, resilience, adequacy and evolutionary capability of the infrastructure)

IT function's existing physical environment for adequacy in accommodating presently installed hardware/software and new hardware/software to be added under the current approved acquisition plan

The hardware and software acquisition plan complies with the IT long- and short-range plans and reflects the needs identified in the technological infrastructure plan

Technological infrastructure plan addresses the use of current and future technology

Technology standards are adhered to and incorporated as part of the development process

Access permitted is consistent with the security levels defined in the IT policies and procedures, and that appropriate authorisation was obtained for access in place

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of technological infrastructure planning against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the data dictionary for completeness of key elements

A detailed review of security levels defined for sensitive data

J **Identifying:**

Inconsistencies in the information architecture model and the corporate data model, corporate data dictionary, associated information systems, and IT long-and short-range plans

Out of date corporate data dictionary items and data syntax rules

Contingency aspects not addressed in the technological infrastructure plan

IT hardware and software acquisition plans that do not reflect the needs of the technological infrastructure plan

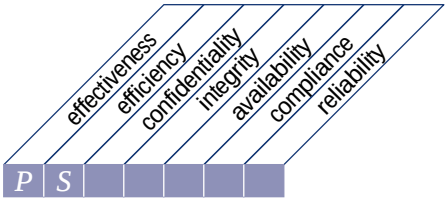
Technology standards that are not consistent with the technological infrastructure plan or IT hardware and software acquisition plans

Technological infrastructure plan or IT hardware and software acquisition plans that are not consistent with technology standards

Key elements that are missing in the data dictionary

Sensitive data not classified as such or not having a security level

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining the IT organisation and relationships

that satisfies the business requirement

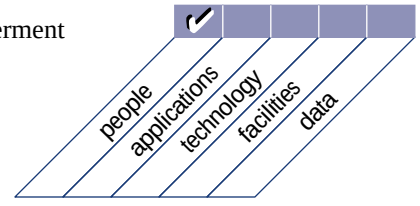
to deliver the right IT services

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



DEFINE THE INFORMATION TECHNOLOGY ORGANISATION AND RELATIONSHIPS

CONTROL OBJECTIVES	
1	IT Planning or Steering Committee
2	Organisational Placement of the IT Function
3	Review of Organisational Achievements
4	Roles and Responsibilities
5	Responsibility for Quality Assurance
6	Responsibility for Logical and Physical Security
7	Ownership and Custodianship
8	Data and System Ownership
9	Supervision
10	Segregation of Duties
11	IT Staffing
12	Job or Position Descriptions for IT Staff
13	Key IT Personnel
14	Contracted Staff Policies and Procedures
15	Relationships

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Executive Officer
Chief Operations Officer
Chief Financial Officer
Chief Information Officer
Quality Assurance Officer
Security Officer
IT planning/steering committee members, human resources and senior management

J **Obtaining:**

Senior management planning/steering roles and responsibilities
Organisation objectives and long- and short-range plans
IT objectives and long- and short-range plans
Organisation chart showing the IT function in relation to other functions
Policies and procedures relating to the IT organisation and relationships
Policies and procedures relating to quality assurance
Policies and procedures used to determine the IT staffing requirements

Obtaining, *continued*

IT function organisation chart

IT function roles and responsibilities

IT function key position (job) descriptions

Status reports and minutes of planning/steering committee meetings

Evaluating the controls by:

J **Considering whether:**

Policy statements and communications from senior management ensure the independence and authority of the IT function

Membership and functions of the IT planning/steering committee have been defined and responsibilities identified

IT planning/steering committee charter aligns the committee's goals with the organisation's objectives and long- and short-range plans, and the IT objectives and long- and short-range plans

Processes are in place to increase awareness, understanding and skill in identifying and resolving information management issues

Policies address the need for evaluation and modification of organisational structure to meet changing objectives and circumstances

Processes and performance indicators exist to determine the effectiveness and acceptance of the IT function

Senior management ensures roles and responsibilities are carried out

Policies exist outlining roles and responsibilities for all personnel within the organisation with respect to information systems, internal control and security

Regular campaigns exist to increase internal control and security awareness and discipline

Quality assurance function and policies exist

Quality assurance function has sufficient independence from system development personnel, and adequate staffing and expertise to perform its responsibilities

Processes are in place within quality assurance to schedule resources and ensure completion of quality assurance testing and sign-off before systems or system changes are implemented

Management has formally assigned organisation-wide responsibility for formulation of internal control and security (both logical and physical) policies and procedures to a security officer

Security officer's understanding of the office's roles and responsibilities are adequately understood and demonstrated as consistent with the organisation's information security policy

Organisation's security policy clearly defines responsibilities for information security that each information asset owner (e.g., users, management, and security administrators) is required to perform

Policies and procedures exist, covering data and system ownership for all major data sources and systems

Procedures exist to review and maintain changes in data and system ownership on a regular basis

Policies and procedures exist describing supervisory practices to ensure that roles and responsibilities are properly exercised, and all personnel have sufficient authority and resources to perform their roles and responsibilities

Segregation of duties exists between the following pairs of units:

- systems development and maintenance
- systems development and operations
- systems development/maintenance and information security
- operations and data control
- operations and users
- operations and information security

IT staffing and competence is maintained to ensure its ability to provide effective technology solutions

Policies and procedures exist for the evaluation and re-evaluation of IT position (job) descriptions

Appropriate roles and responsibilities exist for key processes, including system development life cycle activities (requirements, design, development, testing), information security, acquisition and capacity planning

Appropriate and effective key performance indicators and/or critical success factors are used in measuring results of the IT function in achieving organisational objectives

IT policies and procedures exist to control the activities of consultants and other contract personnel, and thereby ensure the protection of the organisation's assets

Procedures applicable to contracted IT services for adequacy and consistency with organisation acquisition policies

Processes exist to coordinate, communicate and document interests both inside and outside the IT function directorate

Assessing the compliance by:

J **Testing that:**

The IT planning/steering committee oversees the IT function and its activities and resolves action items

Appropriateness of the reporting hierarchy for the IT function

Effectiveness of IT function's location in the organisation with respect to providing a partnership relationship with top management

Senior IT management understand what processes are used to monitor, measure and report on IT function performance

Key indicators are used to assess performance

Process for analysing actual results against target levels to determine the corrective actions taken when actual results do not meet target levels

Actions taken by management for any significant variances from expected levels of performance

Users/owners management assess the IT function's responsiveness and ability to provide information technology solutions which meet user/owner needs

IT management is aware of its roles and responsibilities

Quality assurance involvement in testing and sign-off on IT project plans

Security personnel review core operating system and application systems

Adequacy of security function reports or documentation evaluating information security (both logical and physical) in place or under development

There is sufficient awareness and consistent application of information security policies and procedures

Personnel attend information security and internal control training

Data and system ownership is defined for all information assets

Data and system owners approved changes made to data and systems

All data and systems have an owner or custodian who is responsible for the level of control over the data and systems

Access to all data and system assets is approved by the asset's owner(s)

Direct line of authority and supervision associated with a position (job) is commensurate with the responsibilities of the incumbent

Position (job) descriptions clearly delineate both authority and responsibility

Position (job) descriptions clearly describe the required business, relational and technical competencies

Position (job) descriptions have been communicated accurately and are understood by the individual

Testing that, *continued*

Position (job) descriptions for the IT function contain key performance indicators which have been communicated to the personnel

IT staff duties and responsibilities correspond to both the published position (job) descriptions and the organisation chart

Position (job) descriptions are in place for key positions and include organisation mandates in relation to information systems, internal control and security

Accuracy of position (job) descriptions compared to the current responsibilities of the incumbents in these positions

Nature and extent of compliance with the intended segregation of duties and limitation of functions within the IT function

IT staffing maintains competence

Appropriateness of the position (job) descriptions as a basis for adequacy and clarity of responsibilities and authority and performance criteria

Contract administration responsibilities are assigned to appropriate personnel

Terms of the contracts are consistent with normal organisation standards for contracts and standard contractual terms and conditions have been reviewed and evaluated by legal counsel and their concurrence obtained

Contracts contain appropriate clauses with respect to adherence to: corporate security and internal control policies, and standards for information technology

Processes and/or structures provide for effective and efficient coordination necessary for successful relationships

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of the organisation and relationships against similar organisations or appropriate international standards/recognised industry best practices

A detailed review to determine the impact on the organisation caused by an ineffective IT planning/steering committee

A detailed review to measure the IT function's progress in dealing with information system issues and implementing technology solutions

A detailed review to assess the organisation's structure, staffing and personnel competencies, assigned roles and responsibilities, data and system ownership, supervision, segregation of duties, etc.

A detailed review of the quality assurance function to determine its effectiveness in satisfying the requirements of the organisation

A detailed review of the security function to determine its effectiveness in providing organisation-wide information security (both logical and physical) and information security awareness training

A detailed review of a sample of contracts to confirm that these contracts have been properly executed by both counterparts and are in compliance with the organisation's standard contracting terms

J **Identifying:**

Weaknesses in the IT function and its activities caused by ineffective oversight by the IT planning/steering committee

Organisational structure gaps, overlaps, etc., resulting in the ineffectiveness or inefficiencies in the IT function

Inappropriate organisational structures, missing functions, insufficient staffing, competency deficiencies, improper roles and responsibilities, data and system ownership confusion, supervisory problems, lack of segregation of duties, etc.

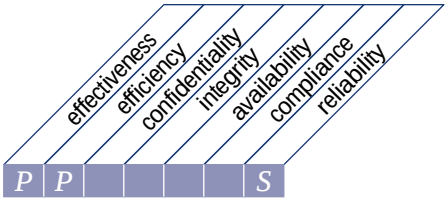
Systems being developed, modified or implemented that do meet quality assurance requirements

Systems being developed, modified or implemented that do meet security (either logical or physical, or both) requirements

Contracts which do not meet the organisation's contracting requirements

Ineffective coordination and communication between the IT function and various other interests inside and outside of the IT function

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing the IT investment

that satisfies the business requirement

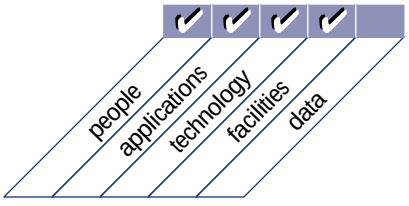
to ensure funding and to control disbursement of financial resources

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



MANAGE THE INFORMATION TECHNOLOGY INVESTMENT

CONTROL OBJECTIVES	
1	Annual IT Operating Budget
2	Cost and Benefit Monitoring
3	Cost and Benefit Justification

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Financial Officer
Chief Information Officer
IT planning/steering committee members
IT senior management

J **Obtaining:**

Organisation policies, methods and procedures relating to budgeting and costing
IT policies and procedures relating to budgeting and costing
Current and immediate prior year's annual operating budget for the IT function
Organisation objectives and long- and short-range plans
IT objectives and long- and short-range plans
Senior management planning/steering roles and responsibilities
Variance reports and other communications connected with variance monitoring and control
Status reports and minutes of planning/steering committee meetings

Evaluating the controls by:

J **Considering whether:**

The IT budgetary process is consistent with the organisation's process
Policies and procedures are in place to ensure the preparation and appropriate approval of an annual IT operating budget which is consistent with the organisation's budget and long- and short-range plans, and the IT long- and short-range plans
The budgetary process is participatory with the management of the IT function's major units contributing in its preparation
Policies and procedures are in place to regularly monitor actual costs and compare them with the projected costs, and the actual costs are based on the organisation's cost accounting system
Policies and procedures are in place to guarantee that the delivery of services by the IT function is cost justified and in line with industry costs

Assessing the compliance by:

- **Testing that:**

The support in the IT budget is adequate in justifying the IT annual operating plan

IT expenditure categories are comprehensive, appropriate and properly classified

The system for routinely recording, processing and reporting on the costs associated with the activities of the IT function is adequate

The cost monitoring process is comparing actuals to budgets adequately

Cost/benefit analyses by the management of the affected user groups, IT function and the organisation's senior management are adequately reviewed

The tools used to monitor costs are effective and properly used

Substantiating the risk of control objectives not being met by:

- **Performing:**

Benchmarking of budgets and costs against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the immediate past and current year budgets versus actual results, variances and corrective actions taken

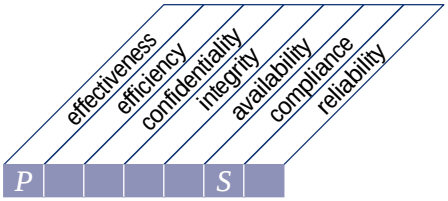
- **Identifying:**

IT budgets that are not in line with the organisation's budget and the long- and short-range plans, and the IT long- and short-range plans

The actual costs of the IT function which are not captured

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

communicating management aims and direction

that satisfies the business requirement

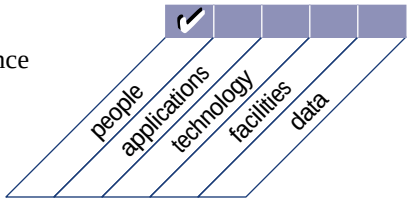
to ensure user awareness and understanding of those aims

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



COMMUNICATE MANAGEMENT AIMS AND DIRECTION

CONTROL OBJECTIVES	
1	Positive Information Control Environment
2	Management's Responsibility for Policies
3	Communication of Organisation Policies
4	Policy Implementation Resources
5	Maintenance of Policies
6	Compliance with Policies, Procedures and Standards
7	Quality Commitment
8	Security and Internal Control Framework Policy
9	Intellectual Property Rights
10	Issue-Specific Policies
11	Communication of IT Security Awareness

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Executive Officer
Chief Operations Officer
Chief Financial Officer
Chief Information Officer
Security Officer
IT senior management
IT planning/steering committee members

J **Obtaining:**

Policies and procedures relating to management's positive control framework and awareness programme, security and internal control framework, and the IT quality programme
Senior management steering roles and responsibilities
Organisation objectives and long- and short-range plans
IT objectives and long- and short-range plans
Status reports and minutes of planning/steering committee meetings
Communications programme

Evaluating the controls by

J **Considering whether:**

Organisation policies and procedures create a framework and awareness programme, giving specific attention to information technology, fostering a positive control environment, and addressing such aspects as:

- integrity

Considering whether, *continued*

- ethical values
- code of conduct
- security and internal controls
- competence of personnel
- management philosophy and operating style
- accountability, attention and direction provided by the board of directors or its equivalent

Top management promotes a positive control environment by example

Management has accepted full responsibility for formulating, developing, documenting, promulgating, controlling and regularly reviewing policies governing general aims and directives

Formal awareness programme exists to provide ongoing communication and training related to management's positive control environment

Organisation policies and procedures exist to ensure that appropriate and adequate resources are assigned to implement the organisation's policies in a timely manner

Appropriate procedures are in place to ensure personnel understand the implemented policies and procedures, and that the policies and procedures are being followed

IT policies and procedures define, document and maintain a formal philosophy policies and objectives governing quality of systems and services produced which are consistent with the organisation's philosophy, policies and objectives

IT management ensures that the quality philosophy, policies and objectives are understood, implemented and maintained at all levels of the IT function

Procedures exist which address the need to periodically review and re-approve key standards, directives, policies and procedures relating to information technology

Senior management has accepted full responsibility for developing a framework for the overall approach to security and internal control.

Security and internal control framework document specifies the security and internal control policy, purpose and objectives, management structure, scope within the organisation, assignment of responsibilities, and definition of penalties and disciplinary actions associated with failing to complying with security and internal control policies

Formal security and internal control policies identify the organisation's internal control process and includes control components such as:

- control environment
- risk assessment
- control activities
- information and communication
- monitoring

Issue specific policies exist to document management decisions addressing particular activities, applications, systems or technologies

Assessing compliance by:

J **Testing that:**

Management's efforts in fostering a positive control cover the key aspects, such as: integrity, ethical values, code of conduct, security and internal controls, competence of the personnel, management philosophy and operating style, and accountability, attention and direction provided

Employees have received the code of conduct and understand it

Management's communication of policies addressing the organisation's internal control environment is occurring

Management's commitment of resources to formulating, developing, documenting, promulgating and controlling polices covering the internal control environment is occurring

Management's regular reviews of standards, directives, policies and procedures for continued appropriateness and its ability to adapt to changing conditions

Management's monitoring efforts are ensuring that appropriate and adequate resources are assigned to implement the organisation's policies in a timely manner

Management's enforcement efforts related to standards, directives, policies and procedures concerning its internal control environment are ensuring compliance throughout the organisation

Quality philosophy, policy and objectives are determining compliance and consistency with the organisation's corporate and IT function philosophy and policies and procedures

Selected IT management, development and operations staff are determining the quality philosophy and related policy, procedures and objectives are understood and adhered to by all levels within the IT function

Quality measurement processes are ensuring organisation objectives are met

Selected members of management are involved and understand the contents for security and internal control activities (i.e., exception reports, reconciliations, comparisons, etc.) under their review responsibility

Individual roles, responsibilities and authorities are clearly communicated and understood at all levels of the organisation

Selected departments assess procedures for routinely monitoring security and internal control activities (i.e., exception reports, reconciliations, comparisons, etc.) and the process for providing feedback to management is occurring

Selected system documentation confirms that system specific management decisions have been documented and approved in compliance with the organisation's policies and procedures

Selected system documentation confirms that management decisions addressing particular activities, applications systems or technologies have been signed off by senior management

Substantiating the risk for the control objectives not being met by:

J **Performing:**

Benchmarking of management's information control framework and awareness programme against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of a sample of approved security and internal control related projects to determine that the projects were prioritised and approved based on risk and cost/benefit analysis

J **Identifying:**

A weak control framework which brings into question management's commitment to fostering a positive internal control environment throughout the organisation

Failure of management to communicate effectively its policies addressing the organisation's internal control environment

Lack of resources assigned to formulating, developing, documenting, promulgating and controlling polices covering the internal control environment

Standards, directives, policies and procedures that are not current

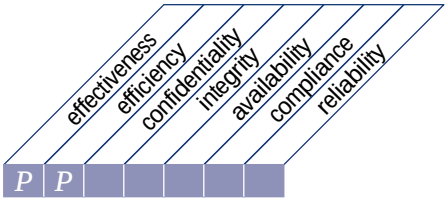
Inadequate management compliance monitoring to ensure that standards, directives, policies and procedures are being adhered to throughout the organisation

IT function deficiencies in its commitment to quality or its ability to effectively define, document, maintain and communicate a quality philosophy, policies and objectives

Weaknesses in the organisation's and/or IT function's security and internal control framework

Missing issue-specific policies needed to address particular activities, applications or technologies

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing human resources

that satisfies the business requirement

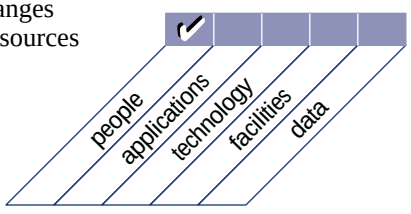
to acquire and maintain a motivated and competent workforce and maximise personnel contributions to the IT processes

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



MANAGE HUMAN RESOURCES

CONTROL OBJECTIVES	
1	Personnel Recruitment and Promotion
2	Personnel Qualifications
3	Roles and Responsibilities
4	Personnel Training
5	Cross-Training or Staff Back-up
6	Personnel Clearance Procedures
7	Employee Job Performance Evaluation
8	Job Change and Termination

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Human Resources Officer and selected staff
Security Officer
Selected security staff
IT manager
IT human resources officer
Selected IT management
Selected IT staff
Selected personnel associated with sensitive positions in the IT function

J **Obtaining:**

Policies and procedures relating to human resources management
Position descriptions, performance evaluation forms, and training and development forms
Personnel files for selected positions and personnel

Evaluating the controls by:

J **Considering whether:**

Criteria are used for recruiting and selecting personnel to fill open positions
Specifications of required qualifications for staff positions take into account relevant requirements of professional bodies where appropriate
Management and employees are accepting of the job competency process
Training programmes are consistent with the organisation's documented minimum requirements concerning education and general awareness covering security issues
Management is committed to personnel training and career development
Technical and management skill gaps are identified and appropriate actions are taken to address these gaps
On-going cross-training and back-up of staff for critical job functions occurs

Considering whether, *continued*

Enforcement of uninterrupted holiday policy occurs

Organisation's security clearance process is adequate

Employees are evaluated based on a standard set of competency profiles for the position and evaluations are held on a periodic basis

Job change and termination processes ensure the protection of the organisation's resources

Human resources management policies and procedures are in accordance with applicable laws and regulations

Assessing the compliance by:

J **Testing that:**

Recruiting and/or promotion actions, and selection criteria reflect objectiveness and relevancy to the requirements of the position

Personnel have adequate knowledge of the operations for their job function or areas of responsibility

Position (job) descriptions exist, are reviewed and are kept up-to-date

Personnel files contain employee acknowledgments of their understanding of the organisation's overall education and general awareness programme

Ongoing training and education occurs for appropriate personnel assigned to critical functions

IT personnel have received proper training in security procedures and techniques

IT management and staff are aware of and understand organisational policies and procedures

Security clearance investigation procedures are consistent with applicable laws governing privacy

Knowledge of business objectives by personnel assigned to critical IT functions include internal controls philosophy, and information systems security and controls concepts

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of human resources management activities against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the IT human resources management activities

J **Identifying:**

Causes of objections/grievances from potential/actual job candidates

Discrepancies in recruitment, transfer, promotion and termination actions related to:

- policies and procedures not being followed
- actions not being signed off by appropriate management
- actions not being based on job specifications and personnel qualifications

Personnel whose:

- qualifications are inappropriate
- training and development opportunities are not tied to competency gaps
- job performance evaluations are missing or do not support the position occupied and/or tasks being performed
- security investigation associated with hiring were not followed
- periodic security investigation has not been performed

Inadequacies in training programmes and staff development activities

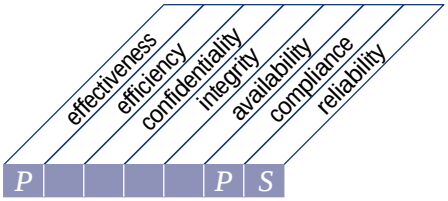
Inadequacies in the cross-training and back-up of key personnel

Security policy acknowledgments that have not been signed

Inadequate budget and time allocated to training and staff development

Personnel time reports for staff performing critical functions that do not indicate that holidays and vacation days have been taken

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring compliance with external requirements

that satisfies the business requirement

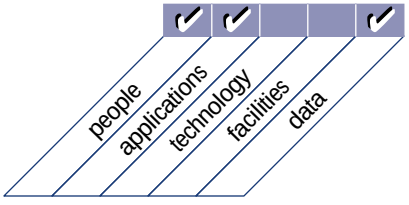
to meet legal, regulatory and contractual obligations

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



ENSURE COMPLIANCE WITH EXTERNAL REQUIREMENTS

CONTROL OBJECTIVES	
1	External Requirements Review
2	Practices and Procedures for Complying with External Requirements
3	Safety and Ergonomic Compliance
4	Privacy, Intellectual Property and Data Flow
5	Electronic Commerce
6	Compliance with Insurance Contracts

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Legal counsel
Human Resources Officer
Senior management of the IT function

J **Obtaining:**

Relevant government and or external requirements (i.e., laws, legislation, guidelines, regulations and standards) related to external relationships and external requirements reviews, safety and health (including ergonomics) compliance issues, privacy issues, information systems security requirements,and cryptographic data transmission — both nationally and internationally

National or international 'accounting standards/pronouncements' relating to the use of electronic commerce

Taxation rulings relating to the use of electronic commerce

Standards, policies and procedures concerning:

- external requirements reviews
- safety and health (including ergonomics)
- privacy
- security
- sensitivity rating of data being input, processed, stored, outputted and transmitted
- electronic commerce
- insurance

Copies of all contracts with all electronic trading partners and with the electronic data interchange (EDI) vendor, if applicable

Copies of all IT function related insurance contracts

Legal counsel advice on the requirements of "uberrimae fidei" (in the utmost good faith) for the insurance contracts (Uberrimae fidei requires both parties to make full disclosures to each other of all matters material to the risk. If good faith in this sense is not shown the contract is voidable by the aggrieved party and unenforceable by the offending party.)

Audit reports from external auditors, third-party service providers and governmental agencies

Evaluating the controls by:

J **Considering whether:**

Policies and procedures are in place for:

- ensuring appropriate corrective action in relation to the external requirements review is undertaken on a timely basis and procedures are in place to ensure continuous compliance
- coordinating the external requirements review, to ensure that corrective actions are taken on a timely basis which guarantee compliance with external requirements
- addressing appropriate safeguards, and safety and health objectives
- ensuring appropriate safety and health training and education is provided to all employees
- monitoring compliance with applicable safety and health laws and regulations
- providing adequate direction/focus on privacy in order that all legal requirements fall within its scope
- informing the insurers of all material changes to the IT environment
- ensuring compliance with the requirements of the insurance contracts
- ensuring updates are made when a new/modified insurance contract is entered into

Security procedures are in accordance with all legal requirements and are being adequately addressed, including:

- password protection and software to limit access
- authorisation procedures
- terminal security measures
- data encryption measures
- firewall controls
- virus protection
- timely follow-up of violation reports

Assessing the compliance by:

J **Testing that:**

External requirements reviews are:

- current, complete and comprehensive with respect to legal, government and regulatory issues
- result in prompt corrective action

Reviews of safety and health are undertaken within the IT function to ensure compliance with external requirements

Problem areas which do not comply with the safety and health standards are rectified

IT compliance with the documented privacy and security policies and procedures

Data being transmitted across international borders does not violate export laws

Existing contracts with electronic commerce trading partners adequately address the requirements specified in organisational policies and procedures

Existing insurance contracts adequately address the requirements specified in organisational policies and procedures

Where regulatory limits are imposed on the types of encryption that can be used (e.g., length of key), that the encryption being used conforms with the regulations

Where regulations or internal procedures require certain data items to be highly protected and/or encrypted (e.g., Bank PIN numbers, Tax File Numbers, Passwords, Military Intelligence), that such protection/encryption is being afforded to such data

Actual EDI processes being deployed by the organisation ensure compliance with organisational policies and procedures, and compliance with the individual electronic commerce trading partner contracts (and the EDI vendor contract if applicable)

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of external requirements compliance, EDI activities and insurance contract requirements against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the external requirements review files to ensure corrective actions have been undertaken or are being implemented

A detailed review of security reports to assess whether sensitive/private information (whether defined as such by either internal procedures or by external regulations) is being afforded appropriate security and privacy protections

J **Identifying:**

External requirements which are not being adhered to by the organisation

Significant unresolved/uncorrected actions in response to external requirements reviews

Safety and health (including ergonomics) risks in the work environment that are not being addressed

Privacy and security weaknesses related to data flow and/or transborder data flow

Breakdowns in electronic commerce

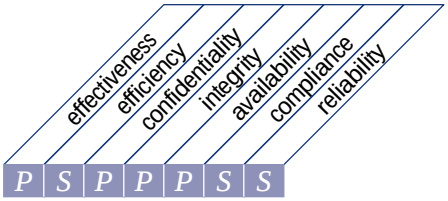
Weaknesses in contracts with trading partners related to communications processes, transaction messages, security and/or data storage

Weaknesses in trust relationships of trading partners

Insurance coverage weaknesses/lapses

Noncompliances with insurance contract terms

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing risks

that satisfies the business requirement

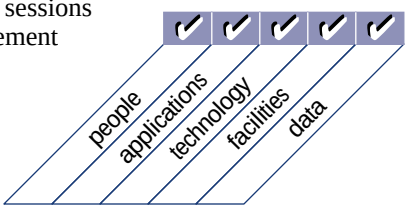
of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors

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



ASSESS RISKS

CONTROL OBJECTIVES	
1	Business Risk Assessment
2	Risk Assessment Approach
3	Risk Identification
4	Risk Measurement
5	Risk Action Plan
6	Risk Acceptance
7	Safeguard Selection
8	Risk Assessment Commitment

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Senior management of the IT function
Selected IT staff
Selected risk management personnel
Key users of IT services

J **Obtaining:**

Policies and procedures relating to risk assessment
Business risk assessment documents
Operating risk assessment documents
IT risk assessment documents
Details of the basis upon which risk and exposure to risk is measured
Personnel files for selected risk assessment personnel
Insurance policies covering residual risk
Results of expert opinions
Peer group reviews
Insight from the risk management database

Evaluating the controls by:

J **Considering whether:**

Systematic risk assessment framework is in place, incorporating the relevant information risks to the achievement of the organisation's objectives and forming a basis for determining how the risks should be managed to an acceptable level

Risk assessment approach provides for regularly updated risk assessments at both the global and system specific levels

Risk assessment procedures are in place to determine that identified risks include both external and internal factors, and take into consideration results of audits, inspections and identified incidents

Considering whether, *continued*

Organisation-wide objectives are included in the risk identification process

Procedures for monitoring changes in systems processing activity determine that system risks and exposures are adjusted in a timely manner

Procedures exist for ongoing monitoring and improving of the risk assessment and mitigating controls creation processes

The risk assessment documentation includes:

- a description of the risk assessment methodology
- the identification of significant exposures and the corresponding risks
- the risks and corresponding exposures which are addressed

Probability, frequency and threat analysis techniques are included in the identification of risks

Qualifications of risk assessment staff are adequate

Formal quantitative and/or qualitative (or combined) approach exists for identifying and measuring risks, threats, and exposures

Calculations and other methods are used in the measurement of risks, threats, and exposures

Risk action plan is used in implementing appropriate measures to mitigate the risks, threats and exposures

Acceptance of residual risk, takes into account:

- organisational policy
- risk identification and measurement
- uncertainty incorporated in the risk assessment approach itself
- cost and effectiveness of implementing safeguards and controls

Insurance coverage offsets the residual risk

Formal quantitative and/or qualitative approaches exist to select control measures that maximise return on investment

There is a balance between the detection, prevention, correction and recovery measures used

Formal procedures exist to communicate the purpose of the control measurers

Assessing the compliance by:

J **Testing that:**

Risk assessment framework is complied with in that the risk assessments are regularly updated to reduce the risk to an acceptable level

Risk assessment documentation complies with the risk assessment framework and documentation is appropriately prepared and maintained

IT management and staff are aware of and involved in the risk assessment process

Management understands risk-related factors and threat likelihood

Relevant personnel understand and formally accept residual risk

Reports issued to senior management for their review and concurrence of identified risks and use in monitoring of risk-reduction activities are timely

Approach used to analyse risk results in a quantitative or qualitative (or combined) measurement of exposure to risk

Risks, threats and exposures identified by management and risk-related attributes are used to detect each occurrence of a specific threat

Risk action plan is current and includes cost-effective controls and security measures to mitigate risk exposure

Priorities from highest to lowest exist, and for each risk an appropriate response exists:
- planned preventive mitigating control
- secondary detective control
- tertiary corrective control

Scenarios of risk versus control are documented, current and communicated to appropriate staff

Sufficient insurance coverage exists with respect to accepted residual risk and considered against various threat scenarios, including:
- fire, flood, earthquake, tornadoes, terrorism, other unforeseeable natural disasters
- breach of employee fiduciary responsibilities
- business interruption — lost revenues, lost customers, etc.
- other risks not generally covered by above IT and business risk/continuity plans

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of the risk assessment framework against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the risk assessment approach used to identify, measure and mitigate risk to an acceptable level of residual risk

J **Identifying:**

Risks not being identified

Risks not being measured

Risks not being addressed/managed to an acceptable level

Out of date risk assessments and/or out of date information in risk assessments

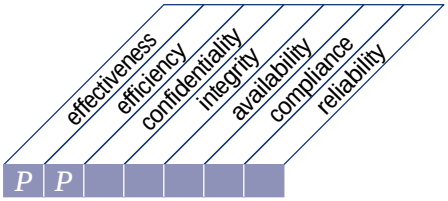
Faulty quantitative and/or qualitative measures of risks, threats and exposures

Risk action plans which do not provide for cost-effective controls and security measures

The lack of formal acceptance of the residual risk

Inadequate insurance coverage

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing projects

that satisfies the business requirement

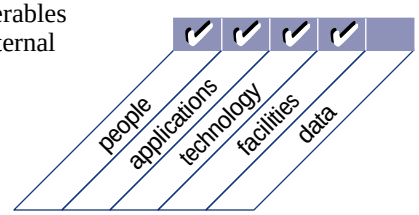
to set priorities and to deliver on time and within budget

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



MANAGE PROJECTS

CONTROL OBJECTIVES	
1	Project Management Framework
2	User Department Participation in Project Initiation
3	Project Team Membership and Responsibilities
4	Project Definition
5	Project Approval
6	Project Phase Approval
7	Project Master Plan
8	System Quality Assurance Plan
9	Planning of Assurance Methods
10	Formal Project Risk Management
11	Test Plan
12	Training Plan
13	Post-Implementation Review Plan

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Quality Manager
Project Quality Manager/Coordinator
Project Owners/Sponsors
Project Team Leader
Quality Assurance Coordinator
Security Officer
IT planning/steering committee members
IT management

J **Obtaining:**

Policies and procedures related to the project management framework
Policies and procedures related to the project management methodology
Policies and procedures related to quality assurance plans
Policies and procedures related to quality assurance methods
Software Project Master Plan (SPMP)
Software Quality Assurance Plan (SQAP)
Project status reports
Status reports and minutes of planning/steering committee meetings
Project quality reports

Evaluating the controls by:

J **Considering whether:**

Project management framework:

- defines scope and boundaries for managing projects
- provides for project requests to be reviewed for their consistency with the approved operational plan and projects prioritised according to this plan
- defines the project management methodology to be adopted and applied to each project undertaken, including:
  - project planning
  - staffing
  - allocation of responsibilities and authorities
  - task breakdown
  - budgeting of time and resources
  - milestones
  - checkpoints
  - approvals
- is complete and current
- provides for participation by the affected user department (owner/sponsor) management in the definition and authorisation of a development, implementation or modification project
- specifies the basis on which staff members are assigned to projects
- defines responsibilities and authorities of project team members
- provides for the creation of a clear written statement defining the nature and scope of the project before work on the project begins
- provides for an initial project definition document which includes a clear statement of the nature and scope of the project
- includes the following reasons for undertaking the project:
  - a statement of the problem to be remedied or process to be improved
  - a statement of the need for the project expressed in terms of enhancing the organisation's ability to achieve its goals
  - an analysis of the deficiencies in relevant existing systems
  - the opportunities that would be provided for increasing economy or efficiency of operation
  - the internal control and security need that would be satisfied by the projects
- addresses the manner in which proposed project feasibility studies are to be prepared, reviewed and approved by senior management, including the:
  - environment of the project — hardware, software, telecommunications
  - scope of the project — what it will include and exclude in the first and following implementations
  - constraints of the project — what must be retained during this project, even if short-term improvement opportunities seem apparent
  - benefits and costs to be realised by the project sponsor or owner/sponsor
- delineates the manner in which each phase of the development process (i.e., preparation of feasibility study, requirements definition, system design, etc.) is to be approved prior to proceeding to the next phase of the project (i.e., programming, system testing, transaction testing, parallel testing, etc.)
- requires the development of an SPMP for each project and specifies the manner in which control will be maintained throughout the life of the project, and project timeframes (milestones) and budgets

- complies with either the organisation standard for SPMPs or, if none exists, an appropriate standard is used
- requires the development of an SQAP for each project and ensures that this is integrated with the SPMP and formally reviewed and agreed to by all involved parties
- delineates the manner in which the formal project risk management programme eliminates or minimises the risks associated with the project
- provides for the development of a test plan for every development, implementation and modification project
- provides for the development of an adequate plan for training the owner/sponsor staff and IT staff for every development, implementation and modification project

Budgeted versus actual project milestones and costs are monitored and reported to senior management throughout every major project phase (i.e., software purchase, hardware purchase, contract programming, network upgrades, etc.)

Project milestones and costs in excess of budgeted timeframes and amounts are required to be approved by appropriate organisation management

SQAP complies with either the organisation standard for SQAPs or if none exists, the criteria selected above

SQAP assurance tasks support the accreditation of new or modified systems and assure that internal controls and security features meet requirements

All project owners/sponsors had input into both the SPMP and SQAP and all agreed to final deliverables

Post-implementation process is an integral part of the project management framework to ensure that new or modified information systems have delivered the planned benefits

Assessing the compliance by:

J **Testing that:**

Project management methodology and all requirements were consistently followed

Project management methodology was communicated to all appropriate personnel involved in the project

Written definition of the nature and scope of the project conforms to a standard template

Nature and extent of owner/sponsor involvement in the project definition and authorisation and conformance with expected owner/sponsor involvement as provided for by the project management framework

Assignment of staff members to the project, and definition of responsibilities and authorities of the project team members are being adhered to

Evidence that a clear, written definition of the nature and scope of the project exists, which is defined before work on the project begins

Relevant feasibility study has been prepared and approved

Appropriate owner/sponsor and IT management approvals are obtained for each phase of the development project

Each phase of the project is being completed and appropriate sign-off is occurring as required by the SPMP

SPMP and SQAP developed and approved in accordance with the project management framework

SPMP and SQAP are detailed and specific enough

Mandatory activities/reports identified have in fact been executed/produced (i.e., Executive Steering Committee meetings, project meetings or the like are to be held at set intervals, minutes of the meetings were taken and distributed to relevant parties, and reports are prepared and distributed to relevant parties)

Test plan has been developed and approved in accordance with the project management framework, and is detailed and specific enough

Mandatory activities/reports identified in the test plan have in fact been executed/produced

Testing that, *continued*

Accreditation criteria used for the project exist and:

- are derived from goals and performance indicators
- are derived from agreed-upon quantitative requirements
- assure internal control and security requirements are met
- are related to the essential 'What" versus the arbitrary "How"
- define a formal Pass/Fail process
- are capable of objective demonstration within a limited time period
- do not simply restate requirements of design documents

Project risk management programme was used to identify and eliminate, or at least minimise, risks associated with the project

Test plan was adhered to, written testing reviews were created by the owner/sponsor, programming and quality assurance functions, and sign-off process was complied with as intended

Written plan for training the staff of the affected owner/sponsor and IT functions was prepared, it allowed sufficient time for completing the required training activities and the plan was used for the project

Post-implementation review plan was adhered to and carried out for the project

Substantiating the risk of control objectives not being met:

J **Performing:**

Benchmarking of the project management framework against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of:

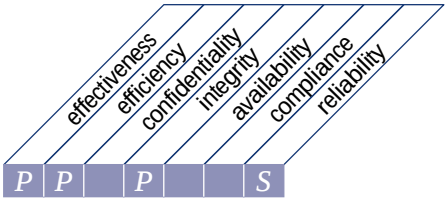
- the project master plan to determine the extent of owner/sponsor participation and the adequacy of the general process of defining, authorising, and executing the project, including:
  - definition of system functions
  - feasibility, given constraints of the project
  - determination of system costs and benefits
  - appropriateness of system controls
  - impact and integration in other owner/sponsor systems
  - owner/sponsor commitment of resources (people and money)
  - definition of responsibilities and authorities of project participants
  - acceptance criteria are both desirable and achievable
  - use of milestones and checkpoints in authorising the various project phases
  - use of Gantt charts, problem logs, meeting summaries, etc., in managing the project
- quality reports to determine if systemic problems exist in the organisation's system quality assurance planning process
- the formal project risk management programme to determine if risks have been identified and eliminated, or at least minimised
- the execution of the test plan to determine that it thoroughly tested the entire system development, implementation, or modification project
- the execution of the training plan to determine that it adequately prepared the owners/sponsors and IT staff in the use of the system
- the post-implementation review to determine if planned versus delivered benefits of the project were ascertained

J **Identifying:**

Projects that:

- are poorly managed
- exceed milestone dates
- exceed costs
- are run-away projects
- have not been authorised
- are not technically feasible
- are not cost justified
- do not achieve planned benefits
- do not contain checkpoints
- are not approved at key checkpoints
- are not accredited for implementation
- do not meet internal control and security requirements
- do not eliminate or mitigate risk
- have not been thoroughly tested
- needed training which has not occurred or is inadequate for the system being implemented
- a post-implementation review has not occurred

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing quality

that satisfies the business requirement

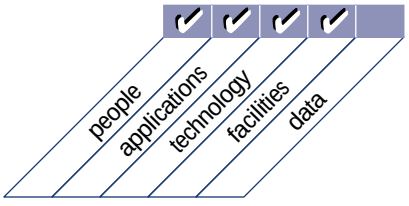
to meet the IT customer requirements

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



MANAGE QUALITY

CONTROL OBJECTIVES	
1	General Quality Plan
2	Quality Assurance Approach
3	Quality Assurance Planning
4	Quality Assurance Review of Adherence to IT Standards and Procedures
5	System Development Life Cycle Methodology
6	System Development Life Cycle Methodology for Major Changes to Existing Technology
7	Updating of the System Development Life Cycle Methodology
8	Coordination and Communication
9	Acquisition and Maintenance Framework for the Technology Infrastructure
10	Third-Party Implementor Relationships
11	Programme Documentation Standards
12	Programme Testing Standards
13	System Testing Standards
14	Parallel/Pilot Testing
15	System Testing Documentation
16	Quality Assurance Evaluation of Adherence to Development Standards
17	Quality Assurance Review of the Achievement of IT Objectives
18	Quality Metrics
19	Reports of Quality Assurance Reviews

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Executive Officer
IT function planning/steering committee members
Chief Information Officer
Security Officer
Organisation Quality Manager
IT Function Quality Manager
IT function management
System owners/sponsors

J **Obtaining:**

Policies and procedures related to quality assurance, system development life cycle and system documentation
Senior management steering roles and responsibilities
Organisation strategic plan, quality policy, quality manual and quality plan
IT strategic plan, quality policy, quality manual, quality plan and configuration management plan

Obtaining, *continued*

Charters of all quality assurance functions

Minutes from individual quality planning meetings

Minutes of meetings convened to review the system development life cycle methodology

Copies of reviews of the system development life cycle methodology

Status reports and minutes of planning/steering committee meetings

Evaluating the controls by:

J **Considering whether:**

Quality plan is:
- based on the organisation's long- and short-range plans
- promoting the continuous improvement philosophy and answers the basic questions of what, who and how
- complete and current

IT quality plan is:
- based on the organisation's overall quality plan and the IT long- and short-range plans
- promoting the continuous improvement philosophy and answers the basic questions of what, who and how
- complete and current

Standard approach to quality assurance exists, and that the approach is:
- applicable to both general and project-specific quality assurance activities
- scaleable and thus applicable to all projects
- understood by all individuals involved in a project and quality assurance activities
- applied throughout all phases of a project

Standard approach to quality assurance prescribes the types of quality assurance activities (and specific reviews, audits, inspections, etc.) to be performed to achieve the objectives of the overall quality plan

Quality assurance planning prescribes the scope and timing of quality assurance activities

Quality assurance reviews evaluate general adherence to the IT standards, policies and procedures

Senior management has defined and implemented IT standards, policies and procedures, including a formal system development life cycle methodology - purchased, developed in-house or combination of the two

System development life cycle methodology:
- governs the process of developing, acquiring, implementing and maintaining computerised information systems and related technology
- supports and encourages development/modification efforts that comply with the organisation's and IT long- and short-range plans
- requires a structured development or modification process with contains checkpoints at key decision points and requires authorisation to proceed with the project at each checkpoint
- is complete and current
- is capable of being tailored/scaled to accommodate all types of development that is occurring within the organisation
- is applicable for both in-house and purchased software creation and maintenance
- has documented provisions for technological change
- has built in a general framework regarding the acquisition and maintenance of the technology infrastructure
- has steps to be followed (such as acquiring; programming, documenting and testing; parameter setting; maintaining and applying fixes) should be governed by, and in line with, the acquisition and maintenance framework for the technology infrastructure
- calls for provisions outlining third-party implementor acceptance criteria, handling of changes, problem handling, participant roles, facilities, tools and software standards and procedures

- requires the maintenance of detailed programme and system documentation (i.e., flow-charts, data flow diagrams, written programme narratives, etc.) and these requirements have been communicated to all concerned staff
- requires that documentation be kept current as changes occur
- requires the application of rigorous and robust programme/system testing
- defines circumstances under which parallel or pilot testing of a new or modified system will be conducted
- requires, as part of every system development, implementation or modification project that tests are independently verified, documented and retained
- requires authorisation for undertaking projects
- requires cost benefit analysis for developing new systems and modifying existing systems

Organisation's quality assurance approach:

- requires that a post-implementation review be performed to ensure that all new or modified systems are developed and put into production in compliance with and the project team adhered to the organisation's system development life cycle methodology
- requires a review of the extent to which new or modified systems have achieved the objectives established for them by management
- results in reports, making system development and effectiveness recommendations to management (both user and IT function) as appropriate
- has recommendations that are periodically followed-up and reported to appropriate senior management officials

Senior IT management reviews and appropriately updates the system development life cycle methodology on a regular basis to ascertain its sufficiency for new development/modification and new technology

Varying levels of control exist for various types of development and maintenance projects (for example, large projects receive more control than small ones)

Achievement of close coordination and communication throughout the entire system development life cycle occurs between customers of the IT function and system implementors

Appropriate involvement exists from different functions/individuals within the organisation (e.g., IT management, security officer, legal staff, quality assurance staff, auditor staff, users, etc.)

Metrics exist to measure the results of activities, allowing an assessment of whether quality goals have been achieved

Assessing the compliance by:

J **Testing that:**

Procedures for developing the IT Quality Plan include the following as inputs:

- organisation long- and short-range plans
- IT long- and short-range plans
- organisation Quality Policy
- IT Quality Policy
- organisation Quality Plan
- IT Configuration Management Plan

IT Quality Plan is based on the IT long- and short-range plans which define:

- application systems development efforts and/or acquisitions
- interfaces with other systems (internal and external)
- IT platform/infrastructure required to support the systems and interfaces
- resources (both financial and human) to develop/support the targeted IT environment
- training required to develop and support the targeted IT environment

Testing that, *continued*

IT Quality Plan addresses the following:

- in unambiguous measurable terms, the targeted level of service to be delivered to clients (whether internal or external clients)
- in unambiguous measurable terms, the targeted maximum outages for each system and platform
- the performance statistics required to monitor the targeted performance/outage objectives, including how they are to be reported and who they are to be distributed to
- the monitoring/review processes necessary to ensure the development/modification/transition in the IT environment/infrastructure identified in the IT long- and short-range plans is well: planned, monitored, resourced, tested, trained, documented and implemented
- the intervals the Quality Plan is to be updated

Quality assurance personnel are consistently adhering to the quality assurance approach and plan and other established operating procedures

Appropriateness of the system development life cycle methodology in ensuring:

- sufficient controls during the developmental process for new systems and technologies
- communication to all appropriate employees involved in development and maintenance of systems
- procedures for technological change are being used
- procedures ensuring user acceptance and sign-off are being used
- adequacy of third-party implementor agreements

Users understand system development life cycle methodology controls and requirements

Change control mechanisms within the system development life cycle methodology allow changes to be made to the methodology and the methodology is a 'living' document

Record of revisions and modifications to the organisation's system development life cycle methodology reflect new systems and technologies currently being considered and expected in the future

Completed programme and system test results (including parallel/pilot test results) are reviewed and retained for future testing

Process is in place to resolve problems encountered during the testing

Post-implementation review has been performed by quality assurance staff

User department representatives involved in system development projects are satisfied with the current use of the methodology

Quality assurance staff clearly understand their role within the organisation

Quality assurance review is required to be performed subsequent to the completion of all system testing and test results review and approval by appropriate IT management, quality assurance, and user personnel

Quality assurance review results in remedial actions by management

Post-implementation reviews are performed and results communicated to senior management and action plans are required for all implementation areas in need of improvement

Measurement results of quality goals exist and are acted upon

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of the system development life cycle methodology against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of the performance measures included in the Quality Plan and ascertain whether they:

- are achievable
- meet corporate requirements/expectations

- meet user requirements/expectations
- are measurable

A detailed review of a sample of projects to ensure that:

- the system development life cycle methodology has been complied with
- any tailoring/scaling of the system development life cycle methodology is appropriate and has been approved
- sign-offs have been obtained at all checkpoints and from all key control personnel (e.g., IT security officer, quality assurance personnel, user representatives, etc.)
- close coordination and communication between users of the IT function and system implementors (whether in-house or third-party) has occurred
- acquisition and maintenance framework for the technical infrastructure, together with any relevant steps involved, have been followed
- development/modification was completed satisfactorily and in a timely manner
- appropriate quality assurance review reports were completed and any needed corrective actions were taken in a timely manner

A detailed review of the manner in which programme and system documentation is prepared, reviewed, approved and maintained

A detailed review of the manner in which programme and system testing (including parallel/pilot testing) and documentation is prepared, reviewed, approved and maintained

A detailed review of quality assurance's post-implementation review process to ensure that reports address adherence to the provisions of the system development life cycle process, and effectiveness and quality aspects of newly implemented/modified systems

J **Identifying:**

Quality plans that have no relationship to long- and short-range plans

Instances of non-utilisation of the system development life cycle methodology and those occurrences of over-use of the system development life cycle methodology (i.e., too much structure on small projects, and not enough on large ones)

Where the system development life cycle methodology was inappropriately used (i.e., applying a system development life cycle methodology for in-house development to the implementation of an off-the-shelf software package, without modifying it accordingly)

Instances of poor or non-existent coordination and communication between individuals (including third-party implementors) involved in the system development life cycle process

Where the different steps to be followed in the acquisition and maintenance of the technology infrastructure (i.e., acquiring; programming, documenting and testing; parameter setting; maintaining and applying fixes) have not been adequately followed

Where programme and/or system documentation does not exist, is inadequate or is not current

Where programme and/or system testing (including parallel/pilot testing) was not performed or was inadequately performed, and/or was not documented or was inadequately documented

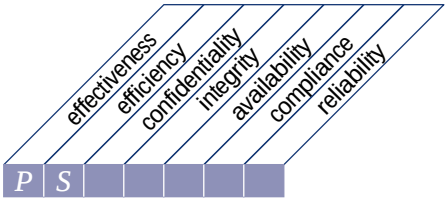
Where quality assurance reviews/post-implementation reviews were not performed or were inadequately performed

Where quality assurance reviews/post-implementation reviews were ignored by management and systems were implemented that should not have been

This page intentionally left blank

ACQUISITION & IMPLEMENTATION

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

identifying automated solutions

that satisfies the business requirement

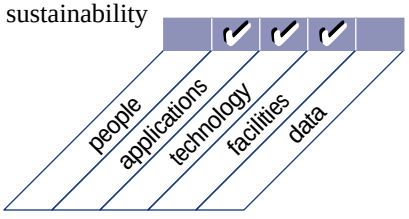
of ensuring an effective and efficient approach to satisfy the user requirements

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



IDENTIFY AUTOMATED SOLUTIONS

CONTROL OBJECTIVES	
1	Definition of Information Requirements
2	Formulation of Alternative Courses of Action
3	Formulation of Acquisition Strategy
4	Third-Party Service Requirements
5	Technological Feasibility Study
6	Economic Feasibility Study
7	Information Architecture
8	Risk Analysis Report
9	Cost-Effective Security Controls
10	Audit Trails Design
11	Ergonomics
12	Selection of System Software
13	Procurement Control
14	Software Product Acquisition
15	Third-Party Software Maintenance
16	Contract Application Programming
17	Acceptance of Facilities
18	Acceptance of Technology

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Information Officer
Security Officer
IT senior management
Project owners/sponsors
Contractor management

J **Obtaining:**

Policies and procedures relating to the system development life cycle and procurement of software

IT objectives and long- and short-range plans

Selected project documentation, including requirements definition, alternatives analyses, technological feasibility studies, economic feasibility studies, information architecture/enterprise data model analyses, risk analyses, internal control/security cost-effectiveness studies, audit trail analyses, ergonomic studies, and facilities and specific technology acceptance plans and test results

Selected contracts relating to software purchase, development or maintenance.

Evaluating the controls by:

J **Considering whether:**

Policies and procedures exist requiring that:

- user requirements satisfied by the existing system or to be satisfied by the proposed new or modified system be clearly defined before a development, implementation or modification project is approved
- the user requirements documentation be reviewed and approved in writing by the cognisant owner/sponsor prior to the development, implementation or modification project being approved
- the solution's functional and operational requirements be satisfied including performance, safety, reliability, compatibility, security and legislation
- alternative solutions to user requirements are studied and analysed prior to choosing one software solution over another
- the identification of commercial software packages that satisfy user requirements for a particular system development or modification project before a final selection decision is made
- alternatives for the acquisition of software products are clearly defined in terms of off-the-shelf, developed internally, through contract, or by enhancing the existing software, or a combination of all of these
- a technical feasibility study of each alternative for satisfying the user requirements established for the development of a proposed new or modified system project be prepared, analysed and approved by the cognisant owner/sponsor
- in each proposed system development, implementation and modification project, an analysis be performed of the costs and benefits associated with each alternative being considered for satisfying the user requirements
- an economic feasibility study be prepared, analysed and approved by the cognisant owner/sponsor prior to making the decision whether to develop or modify a proposed new or modified system project
- attention is paid to the enterprise data model while solutions are being identified and analysed for feasibility
- in each proposed system development, implementation or modification project, an analysis is prepared and documented of the security threats, potential vulnerabilities and impacts, and the feasible security and internal control safeguards for reducing or eliminating the identified risk
- the costs and benefits of security are carefully examined to guarantee that the costs of controls do not exceed the benefits
- formal management sign-off of the cost/benefit study
- appropriate audit trails and controls are required to be built into all proposed new or modified systems during the design phase of the project
- audit trails and controls provide the possibility to protect the users against discovery and misuse of their identity by other users (e.g., by offering anonymity, pseudonymity, unlinkability or unobservability), without jeopardising the systems security
- each proposed system development, implementation or modification project pay attention to ergonomic issues associated with the introduction of automated systems
- IT management identify all potential system software programmes that will satisfy its operational requirements
- products be reviewed and tested prior to their use and financial settlement
- software product acquisitions follow the organisation's procurement policies setting the framework for the creation of the request for proposal, the selection of the software product supplier and the negotiation of the contract

- for licensed software acquired from third-party providers, the providers have appropriate procedures to validate, protect and maintain the software product's integrity rights
- procurement of contract programming services be justified with a written request for services from a designated member of the IT function
- an acceptance plan for facilities is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria
- the end products of completed contract programming services be tested and reviewed according to the related standards by the IT quality assurance group and other concerned parties before payment for the work and approval of the end product
- an acceptance plan for specific technology is agreed upon with the supplier in the contract and this plan defines the acceptance procedures and criteria
- the procurement of contract programming services be justified with a written request for services from a designated member of the IT function

Risk analysis is performed in line with the overall risk assessment framework

Mechanisms exist to assign or maintain security attributes to exported and imported data, and to interpret them correctly

Management has developed and implemented a central procurement approach, describing a common set of procedures and standards to be followed in the procurement of IT hardware, software and services

Contracts stipulate that the software, documentation and other deliverables are subject to testing and review prior to acceptance

Testing included in contract specifications consists of system testing, integration testing, hardware and component testing, procedure testing, load and stress testing, tuning and performance testing, regression testing, user acceptance testing and, finally, pilot testing of the total system to avoid any unexpected system failure

Facilities acceptance tests are performed to guarantee that the accommodation and environment meet the requirements specified in the contract

Specific technology acceptance tests should include inspection, functionality tests and workload trials

Assessing the compliance by:

J **Testing that:**

User requirements satisfied by the existing system and to be satisfied by the proposed new or modified system, have been clearly defined, reviewed and approved in writing by the cognisant user before the development, implementation or modification of the project

Solution's functional and operational requirements are satisfied including performance, safety, reliability, compatibility, security and legislation

All weaknesses and processing deficiencies in the existing system have been identified, and are to be completely addressed and resolved by the proposed new or modified system

Alternative courses of action that will satisfy the user requirements established for a proposed new or modified system have been appropriately analysed

Commercial software packages that satisfy the needs of a particular system development or modification project have been appropriately identified and considered

All identifiable costs and benefits associated with each alternative have been properly supported and included as part of the required economic feasibility study

Attention was paid to the information architecture/enterprise data model as solutions were identified and analysed for feasibility

Testing that, *continued*

Risk analysis report of the security threats, potential vulnerabilities and impacts, and the feasible security and internal control safeguards for reducing or eliminating the identified risk is accurate and comprehensive

Security and internal control issues have been appropriately addressed in the system design documentation

Management's approval that the controls in place and planned are sufficient, with appropriate benefits to offset costs

Adequate mechanisms for audit trails are available or can be developed for the solution identified and selected

User friendly design to enhance end-user skills has been taken into account during system design and development of screen layouts, report formats, online help facilities, etc.

Ergonomic issues have been taken into consideration during system design and development

User performance issues (i.e., system response time, download/upload capabilities, ad hoc reporting) have been included in the system requirements specifications prior to design and development

IT function identification of all potential system software programmes that satisfy operational requirements

IT function adheres to a common set of procedures and standards in the procurement of IT related hardware, software and services

Purchased products are reviewed and tested prior to their use and the financial settlement

Software purchase agreement allows the user to have a copy of the programme source code, if applicable

Software product upgrades, technology refreshments and fixes are specified in the procurement documents

Third-party software maintenance includes requirements for the validation, protection and maintenance of the software product's integrity

Contract programming personnel work is subject to the same level of testing, review and sign-off as is required of the organisation's own programmers

Organisation's quality assurance function is responsible for the review and sign-off on work performed by contract programmers

Appropriateness and completeness of facilities acceptance plan is occurring, including the acceptance procedures and criteria

Appropriateness and completeness of specific technology acceptance plan, including inspections, functionality tests and workload trials

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of the identification of user requirements to meet automated solutions against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of:

- the identification of automated solutions to meet user requirement (including the definition of user requirements; formulation of alternative courses of action; identification of commercial software packages; and performance of technology feasibility, economic feasibility, information architecture and risk analysis studies)
- security, internal controls (including consideration of user friendly design, ergonomics, etc.) and audit trails available or capable of being developed for the solution identified and selected
- the selection and implementation of system software
- existing software procurement policies and procedures for organisation and internal control adequacy and compliance
- the manner in which third-party maintenance is being managed
- the manner in which contract application programming has been monitored and managed
- the facilities acceptance process to ensure that the accommodation and environment tests meet the requirements specified in the contract

- the acceptance process for specific technology to ensure that inspections, functionality tests and workload trials meet the requirements specified in the contract

J **Identifying:**

Deficiencies in the organisation's system development life cycle methodology

Solutions that do not meet user requirements

System development efforts that:

- did not consider alternative courses of action, thereby resulting in a more costly solution
- did not consider commercial software packages which could have been implemented in less time and at less cost
- did not consider the technological feasibility of the alternatives or inappropriately considered the technological feasibility of the chosen solution, and as a result could not implement the solution as originally designed
- made erroneous assumptions in the economic feasibility study and as a result chose the wrong course of action
- did not consider the information architecture/enterprise data model and as a result chose the wrong course of action
- did not conduct robust risk analyses and thus either did not adequately identify risks (including threats, potential vulnerabilities and impacts) or did not identify appropriate security and internal controls for reducing or eliminating identified risks

Solutions that:

- were either over controlled or under controlled because the cost-effectiveness of controls and security was improperly examined
- did not have adequate audit trails
- did not consider user friendly design and ergonomic issues, thereby resulting in data input errors that could have been avoided
- did not follow the organisation's established procurement approach and thus resulted in additional costs being borne by the organisation

The lack of needed system software

The ineffectiveness of system software because improper parameters were set

Third-party software maintenance that did not live up to the terms of the contract and as a result was adversely affecting the organisation in meeting its mission and/or goals

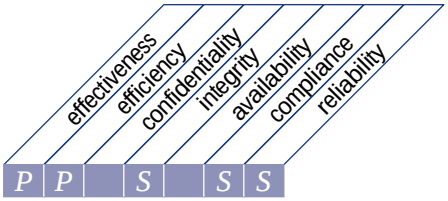
Contract application programming that did not live up to the terms of the contract and, as a result cost the organisation additional money, delayed system implementation, etc.

Situations where facilities have been accepted without thoroughly testing the accommodation environment and as a result do not meet user requirements and/or do not comply with contact terms

Where a specific technology is accepted but inspections, functionality tests, and workload trials have not been adequately performed, and as a result the technology does not meet user requirements and/or does not comply with contract terms

Any system failures

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

acquiring and maintaining application software

that satisfies the business requirement

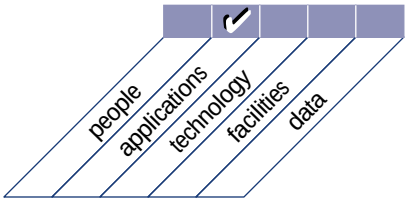
to provide automated functions which effectively support the business process

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



ACQUIRE AND MAINTAIN APPLICATION SOFTWARE

CONTROL OBJECTIVES	
1	Design Methods
2	Major Changes to Existing Systems
3	Design Approval
4	File Requirements Definition and Documentation
5	Programme Specifications
6	Source Data Collection Design
7	Input Requirements Definition and Documentation
8	Definition of Interfaces
9	User-Machine Interface
10	Processing Requirements Definition and Documentation
11	Output Requirements Definition and Documentation
12	Controllability
13	Availability as a Key Design Factor
14	IT Integrity Provisions in Application Programme Software
15	Application Software Testing
16	User Reference and Support Materials
17	Reassessment of System Design

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Information Officer
Security Officer
IT senior management
Project owners/sponsors

J **Obtaining:**

Policies and procedures relating to the system development life cycle methodology
IT objectives and long- and short-range plans
Selected project documentation, including design approvals, file requirements definition, programme specifications, source data collection design, input requirements definition, user-machine interface, processing requirements definition, output requirements definition, internal control/security requirements, availability requirements, IT integrity provisions, application software test plan and results, user reference and support materials, and re-assessment of system design

Evaluating the controls by:

J **Considering whether:**

Policies and procedures ensure that:

- the organisation's system development life cycle methodology applies to both the development of new systems and major changes to existing systems, and user participation
- close liaison with the user in creating the design specifications and verifying the design specifications against user requirements
- in the event of major changes to existing systems, a similar system development life cycle process is observed as in the case of the development of new systems
- design specifications are signed-off by management, the affected user departments and the organisation's senior management, when appropriate for all new system development and modification projects
- an appropriate process is being applied for defining and documenting the file format for each new system development or modification project, including a requirement that the data dictionary rules are respected
- detailed written programme specifications are prepared for each information development or modification project and these programme specifications agree with the system design specifications
- adequate mechanisms for the collection and entry of data are specified for each new system development or modification project
- adequate mechanisms for defining and documenting the input requirements for each new system development or modification project exist
- the development of an interface between the user and the machine exists which is easy to use and self-documenting (by means of online help functions)
- adequate mechanisms for defining and documenting internal and external interfaces for each new system development or modification project exist
- adequate mechanisms for defining and documenting the processing requirements for each new system development or modification project exist
- adequate mechanisms for defining and documenting the output requirements for each new system development or modification project exist
- adequate mechanisms for ensuring internal control and security requirements are specified for each new system development or modification project
- the internal control and security requirements include application controls which guarantee the accuracy, completeness, timeliness and authorisation of inputs and outputs
- availability is considered in the design process of new or modified systems at the earliest possible stage, and this consideration should analyse and, if necessary, increase through maintainability and reliability improvements
- applications programmes contain provisions which routinely verify the tasks performed by the software and which provide in the restoration of the integrity through rollback or other means
- application software is tested according to the project test plan and established testing standards before being approved by the user
- adequate user reference and support manuals are prepared (preferably in electronic format) as part of every system development or modification process
- the system design is re-assessed whenever significant, technological and/or logical discrepancies occur during system development or maintenance

System development life cycle methodology ensures that user reference and support materials are updated in an accurate and timely manner

Sensitivity assessment is required by the system development life cycle methodology to be performed during the initiation of new system development or modification

System development life cycle methodology requires that basic security and internal control aspects of a new system to be developed or modified be assessed along with the conceptual design of the system in order to integrate security concepts in the design as early as possible

Logical security and application security issues are required by the system development life cycle methodology to be addressed and included in the design of new systems or modifications of existing ones

The assessment of the security and internal control aspects is based on a sound framework

Artificial Intelligence systems are placed in an interaction or control framework with human operators to ensure that vital decisions are approved

Disclosure of sensitive information used during application testing is mitigated by either strong access limitations or depersonalisation of the used historical data

Assessing the compliance by:

J **Testing that:**

User participation in the system development life cycle process is high

The organisation's system development life cycle methodology ensures that a process is in place that appropriately addresses all system design issues (i.e., input, processing, output, internal controls, security, disaster recovery, response time, reporting, change control, etc.)

Key system users are involved in the system design process

Design review and approval process ensures that all issues have been resolved prior to beginning work on the next phase of the project

Major changes to existing systems ensure they are developed using a similar system development life cycle methodology to that used for the development of new systems

Design sign-off procedures are in place to ensure that programming of the system is not started until proper design sign-offs are obtained

System file requirements and documentation, and data dictionary are all consistent with standards

User sign-off on final file specifications occurs

Programme specifications agree with system design specifications

Data collection and data entry design specifications match

User-machine interface design specifications exist

User-machine specifications are easy to use and self-documenting (using online help facilities) functions are employed

Internal and external interfaces are documented

Processing requirements are in design specifications

Output requirements are in design specifications

Internal control and security requirements are in design specifications

Application control requirements design specifications guarantee the accuracy, completeness, timeliness and authorisation of inputs and outputs

Internal control and security requirements have been included in the conceptual design of the system (whether a new system or one being modified) as early as possible

Security officer is actively involved in the system design, development and implementation process of the new system or system modification project

System design determines whether improved availability/reliability has been quantified in terms of time and more efficient procedures over prior methods if applicable

Application programme provisions routinely verify the tasks performed by the software to help assure data integrity

Established testing standards exist

Testing that, *continued*

Project test plan and user approval process exist

User reference and support materials, and online help facility are available

Help desk function is effectively assisting users in addressing more complex processing issues

Process for escalating help desk issues includes the tracking, monitoring and reporting of such issues to appropriate IT management

Mechanism in place to update user documentation is required

Communication of user documentation changes is occurring

Re-assessment process occurs whenever significant technological and/or logical discrepancies occur

Substantiating the risk of the control objectives not being met by:

J **Performing:**

Benchmarking costs of acquiring and developing application software against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of selected:

- system design documentation to evaluate the adequacy of the design specifications and adherence of the design to those specifications
- new system development or modification projects determine whether design specification documents have been reviewed and approved by the management of the IT function and the affected user functions as well as the organisation's senior management when appropriate
- software documentation to ensure that file requirements (for at least those files listed below) are clearly understood by the project implementation team and are being structured per system and user requirements, and the organisation's data dictionary rules:
  - Master
  - Transaction
  - Command
  - Programme
  - Control
  - Table
  - Report
  - Print
  - Log
  - Transmission
- new system development and modification projects to ensure that files, programmes, source data collection instruments, inputs, user-machine interfaces, processing steps and outputs identified in flowcharts/flow diagrams correspond to the various system design specifications
- new system development and modification projects to determine that whenever significant technical and/or logical discrepancies are identified an effective system design re-assessment process occurs
- new system development and modification projects to determine the existence of any technical design discrepancies or functional changes needed
- new system development and modification projects and conceptual system designs to evaluate the adequacy of the internal control and security provisions that ensure the accuracy, completeness, timeliness and authorisation of inputs and outputs, and the integration of security concepts in the design at the earliest possible time

- new system development and modification projects to evaluate the design in light of improved availability and reliability for the end-user and maintainability for IT maintenance personnel
- projects to evaluate the adequacy of application programme data integrity verification
- new system development and modification projects to ensure that user reference materials are current and consistent with the system documentation and fully meet user needs

A detailed review of the effectiveness of:

- the programme specifications process to ensure programmes are written according to user design specifications
- the input specifications process to ensure programmes are written according to user design specifications
- the user-machine interface specifications process to ensure programmes are written according to user design specifications
- the processing specifications process to ensure programmes are written according to user design specifications
- the output specifications process to ensure programmes are written according to user design specifications

A detailed review of the organisation's testing standards and the implementation of associated test plans for selected new system development and modification projects

A detailed review of user satisfaction with the system, its reports, user documentation and reference materials, help facilities, etc.

J **Identifying:**

Deficiencies in the organisation's system development life cycle methodology used for new system development or modification projects

Design specifications that do not reflect user requirements

File requirements that are not consistent with the organisation's data dictionary rules

New system development or modification projects that contain inadequately defined file, programme, source data selection, input, user-machine interface, processing, output and/or controllability requirements

New system development or modification projects where availability was not considered in the design process

Data integrity deficiencies in application programme software in new system development or modification projects

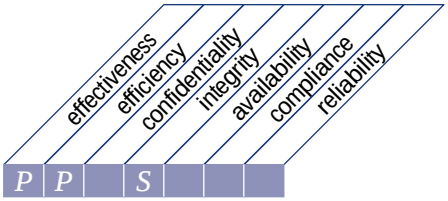
Deficiencies in the organisation's testing standards which have resulted in the implementation of systems which do not process data correctly, report data incorrectly, etc.

Test plan deficiencies in new system development or modification projects

Deficiencies in user reference and support materials in new system development or modification projects

Significant technical and/or logical discrepancies that have occurred during system development or maintenance that did not result in re-assessment of the system design, and therefore went uncorrected or resulted in inefficient, ineffective and uneconomical patches to the system

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

acquiring and maintaining technology infrastructure

that satisfies the business requirement

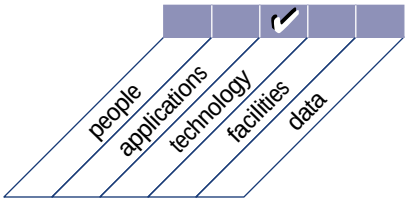
to provide the appropriate platforms for supporting business applications

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



ACQUIRE AND MAINTAIN TECHNOLOGY INFRASTRUCTURE

CONTROL OBJECTIVES	
1	Assessment of New Hardware and Software
2	Preventative Maintenance for Hardware
3	System Software Security
4	System Software Installation
5	System Software Maintenance
6	System Software Change Controls
7	Use and Monitoring of System Utilities

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT planning/steering committee
Chief Information Officer
IT senior management

J **Obtaining:**

Policies and procedures relating to hardware and software acquisition, implementation and maintenance
Senior management steering roles and responsibilities
IT objectives and long- and short-range plans
Status reports and minutes of meetings
Vendor hardware and software documentation
Hardware and software rental contracts or lease agreement

Evaluating the controls by:

J **Considering whether:**

Policies and procedures exist to ensure that:

- a formal evaluation plan is prepared to assess new hardware and software for any impact on the overall performance of the system
- ability to access system software and thereby interrupt the operational information systems environment is limited
- set-up, installation and maintenance of system software does not jeopardise the security of the data and programmes being stored on the system
- system software parameters are selected in order to ensure the integrity of the data and programmes being stored on the system
- system software is installed and maintained in accordance with the acquisition and maintenance framework for the technology infrastructure
- system software vendors provide integrity assurance statements with their software and all modifications to their software

Considering whether, *continued*

- the thorough testing (i.e., using a system development life cycle methodology) of system software is occurring before it is introduced into the production environment
- vendor provided system software installation passwords are changed at the time of installation and system software changes are controlled in line with the organisation's change management procedures

Policies and procedures exist for the preventive maintenance of hardware (both operated by the IT function and affected user functions) to reduce the frequency and impact of performance failures

Vendor prescribed preventative maintenance steps and frequency for each hardware device operated by the IT function and the affected user functions are adhered to

Policies and techniques exist for using and monitoring the use of system utilities

Responsibilities for using sensitive software utilities are clearly defined, understood by programmers, and use of the utilities is monitored and logged

Assessing the compliance by:

J **Testing that:**

Vendor supplied system software integrity assurance statements exist for all system software (including all modifications) and address the resulting exposures in the system software

Performance assessment results in comparison to system requirements

Performance assessment formal approval process exists

Preventative maintenance schedule ensures that scheduled hardware maintenance will have no negative impact upon critical or sensitive applications

Scheduled maintenance ensures that it is not being scheduled for peak workload periods and that the IT function and affected user groups operations are sufficiently flexible to accommodate routinely scheduled preventative maintenance

IT operating schedules ensure that there are adequate preparations to accommodate anticipated hardware downtime for unscheduled maintenance

System software parameters ensure that the correct ones were chosen by appropriate IT personnel to ensure the integrity of the data and programmes being stored on the system

Access is restricted only to a limited number of operators within the IT function

System software is installed and maintained in accordance with the acquisition and maintenance framework for the technology infrastructure

Thorough testing (using a system development life cycle methodology) occurs for all system software before it was authorised to be introduced into the production environment

All vendor provided system software installation passwords were changed at the time of installation

All system software changes were controlled in accordance with the organisation's change management procedures

System administration (e.g., addition of new users to the system and networks; database creation and backup; space allocation for data storage; system priorities; etc.) are restricted only to a limited number of operators within the IT function

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of hardware and software acquisition, implementation and maintenance against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of:

- documentation for selected operational systems and system development or modification projects to determine whether formal hardware and software performance requirements (including references to transaction volume, processing and response times, file and database sizes, network volumes and compatibility of communications protocols) exist for the systems
- hardware maintenance practices to determine if maintenance is being performed in accordance with vendor guidelines and scheduled in such a manner that it does not impact on the overall performance of the system
- documentation for selected operational systems and systems under development or modification to evaluate potential abilities to circumvent existing logical security access restrictions provided by the system software
- system software installation, maintenance and change controls to ensure compliance with the acquisition and maintenance framework for the technology infrastructure and system integrity is maintained

J **Identifying:**

Performance assessments which have impacted the overall performance of the system

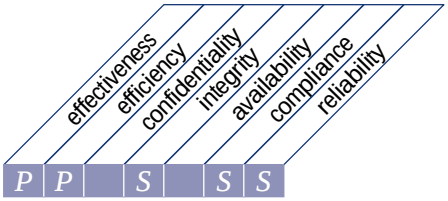
Preventive maintenance problems which have impacted the overall performance of the system

Weaknesses in the set-up, installation and maintenance of system software (including the selection of inappropriate system software parameters) which have jeopardised the security of the data and programmes being stored on the system

Weaknesses in the testing of system software which could jeopardise the security of the data and programmes being stored on the system

Weaknesses in the system software change control process which could jeopardise the security of the data and programmes being stored on the system

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

developing and maintaining procedures

that satisfies the business requirement

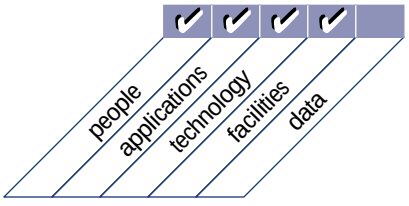
to ensure the proper use of the applications and the technological solutions put in place

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



DEVELOP AND MAINTAIN PROCEDURES

CONTROL OBJECTIVES	
1	Operational Requirements and Service Levels
2	User Procedures Manual
3	Operations Manual
4	Training Materials

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT applications development
IT maintenance
IT change control
IT operations
IT human resources/training
IT quality assurance management
Selected users of information systems resources

J **Obtaining:**

Organisational policies and procedures relating to: strategic planning and business objectives, information systems planning and applications development

IT policies and procedures relating to system development including: organisation chart, system development life cycle methodology, capacity planning, user and operations manuals, training materials, testing and migration into production status and business resumption/contingency planning documents

Evaluating the controls by:

J **Considering whether:**

Operational requirements are determined with historical performance statistics available and user input regarding increases/decreases expected

Service level and performance expectations are at sufficient detail to allow tracking, reporting and improvement opportunities

Operational requirements and service levels are determined using both historical performance, user adjustments, and industry benchmarks

Service levels and processing requirements are an integral step in planning for new systems

User procedures manuals, operations manual and training materials are developed as part of every information system development, implementation or modification project, and are kept up-to-date

Assessing the compliance by:

J **Testing that:**

Operational requirements are in place and reflect both operations and user expectations

Operational performance is being measured, communicated and corrected where deficient

Operations staff and users are aware of performance requirements

Operations staff have operations manuals for all systems and processing within their responsibility

All movement of programmes from applications development into production requires operations manual update or creation

User training manuals exist for all applications and currently reflect functionality of the application

Training manuals for all current and any new systems exist and are satisfactory to users, reflecting the system's use in daily practice

Users manual to confirm contents include, but are not limited to:

- overview of system and environment
- explanation of all system inputs, programmes, outputs and integration with other systems
- explanation of all data entry screens and data display screens
- explanation of any and all error messages, and appropriate response
- problem escalation procedures and/or resources

Operators manual to confirm contents include, but are not limited to:

- system name, programme names, sequence of execution
- definition of all file names input, processed, and output and media format
- schedule for running daily, weekly, monthly, quarterly, year end, etc.
- console commands and parameters requiring entry by operator
- console error messages and response
- backup, restart, restore procedures at various points or upon abnormal end
- special output forms or procedures; report/output distribution
- emergency fix procedures, if appropriate

Ongoing maintenance of application documentation, user and operations manuals, and training is occurring

Substantiating the risk of control objectives not being met by:

J **Performing:**

For a selection of systems development projects, documentation review and approvals for:

- considering future requirements and service levels of users
- task and delivery for creation and maintenance of users manuals
- task and delivery for creation and maintenance of operations manual
- task and delivery of user training to understand and use new system or new modification

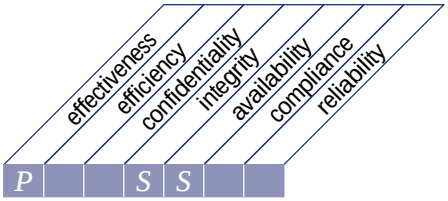
Interview of users to confirm sufficiency of the systems development effort, including manuals developed and training provided

Analysis of both users and operations manuals for currency and ongoing maintenance

J **Identifying:**

- deficiencies in users, operations and training manuals
- non-existence of service level agreements between
  - vendor and IT function
  - IT function and users
- organisational weaknesses in developing and running the required applications

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

installing and accrediting systems

that satisfies the business requirement

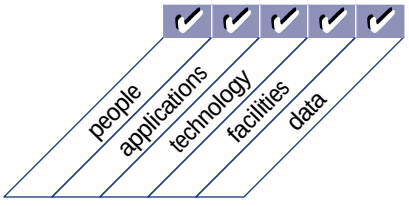
to verify and confirm that the solution is fit for the intended purpose

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



INSTALL AND ACCREDIT SYSTEMS

CONTROL OBJECTIVES	
1	Training
2	Application Software Performance Sizing
3	Implementation Plan
4	System Conversion
5	Data Conversion
6	Testing Strategies and Plans
7	Testing Of Changes
8	Parallel/Pilot Testing Criteria and Performance
9	Final Acceptance Test
10	Security Testing and Accreditation
11	Operational Test
12	Promotion to Production
13	Evaluation of Meeting User Requirements
14	Management's Post-implementation Review

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Information Officer
IT management
IT training, applications development, security, quality assurance and operations management
Security Officer
Selected user management of newly developed/developing systems
Contracts with vendors for system development resources

J **Obtaining:**

Organisational policies and procedures relating to system development life cycle planning and IT policies and procedures relating to: security policies and committees; systems development life cycle planning; systems development testing procedures for programme, unit, system test plans; training of users; migration of systems from test to production, quality assurance and training

System development life cycle plan and schedule, system development life cycle programming standards, including change request process

Sample system development effort status reports

Post-implementation reports from prior developmental efforts

Evaluating the controls by:

J **Considering whether:**

Policies and procedures relating to the system development life cycle process exist

A formal system development life cycle methodology is in place for system installation and accreditation including, but not limited to, a phased approach of: training, performance sizing, conversion plan, testing of programmes, groups of programmes (units) and the total system, a parallel or prototype test plan, acceptance testing, security testing and accreditation, operational testing, change controls, implementation and post-implementation review and modification

User training as part of each developmental effort is occurring

Programme/system controls are consistent with security standards of the organisation and IT policies, procedures and standards

There are various development, test and production libraries for in-process systems

Pre-determined criteria exist for testing success, failure and termination of further efforts

Quality assurance process includes independent migration of development into production libraries and completeness of required user and operations groups' acceptance

Test plans for simulation of volumes, processing intervals, and output availability, installation and accreditation are part of the process

Training programme associated with a sample of several system development efforts contain: difference from prior system, changes affecting input, entry, processing, scheduling, distribution, interfaces to other systems, errors and error resolution

Automated tools optimise systems developed, once in production, and these tools are being used for efficiency opportunities

Problem resolution is occurring relating to less than optimal performance

Assessing the compliance by:

J **Testing that:**

A formal plan for user training has been included in all new systems development efforts

Staff is aware and understands need for formal system development controls and user training for every developmental installation and implementation

Selected users' awareness and understanding of their responsibilities in the systems design, approval, testing, training, conversion and implementation processes is known and acknowledged

Actual costs of systems versus estimated costs and actual performance versus expected performance of new or modified systems are being tracked

A test plan covering all areas of information system resources exists: application software, facilities, technology and users

Users understand all phases and responsibilities in systems development, including:

- design specifications, including iterations during development cycle
- cost/benefit analysis and feasibility study
- approval at each step of the system development process
- involvement and assessment of test plan and test results as they occur
- approval and acceptance of system as it moves through development cycle
- final approval and acceptance of system
- assessment of training received for recently delivered systems for sufficiency

Development staff and management ascertain stability of user requirements once agreed

User satisfaction compares with vendor deliverables, as opposed to in-house products

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of installation and accreditation of systems against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of:

- development group in meeting deadlines and tasks to user satisfaction — including system functionality when completed
- training materials associated with prior systems
- quality assurance function's independent review and migration of systems from test into production status and libraries
- network and resource monitoring tools being used to collect statistics for maintenance and optimisation, and ensuring support of the applications developed towards maximum performance at minimal cost
- records of a developmental effort to determine availability of:
  - User training
  - Security
  - Software performance
  - Testing documentation and results
  - Conversion plan
  - Migration into production
  - Change control during development
  - Meeting of user needs
  - Parallel or pilot testing
  - Post-implementation review
- internal or external audit conclusions regarding the systems design process
- test results to confirm results meet pre-defined criteria and all functions of the system were included in test plans
- management discussions of test results, and any terminated tests or development projects
- user participation in the developmental process
- audit trails towards recreating activity or error analysis as needed
- vendor participation in the developmental effort including:
  - Reasonableness of costs
  - Meeting of deadlines
  - Delivered functionality

J **Identifying:**

For a selection of recent system development life cycle projects:

- user involvement and formal approval at each phase of the system development process
- test plan for programmes, units, systems (including parallel or prototype), conversion, implementation and post-implementation review
- appropriate consistency with security and internal control standards

Identifying, *continued*

- appropriate data conversion tasks and schedules
- testing occurs independently from those developing, modifying or maintaining the system
- formal acceptance by users of system functionality, security, integrity and remaining risk

That operations manuals for scheduling, running, restore/restart, backup/backout and error resolution address:

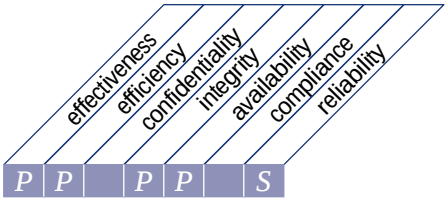
- physical and logical separation of production libraries from development or test ones
- resolution procedures between user expectations and functionality of system delivered when in conflict

For vendors:

- vendor relationships are formal and contracts exist
- specific services and costs are outlined
- vendor's performance is equally controlled with the organisation's system development life cycle methodology
- vendor has met performance, deadline and cost specifics of the contracts

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing changes

that satisfies the business requirement

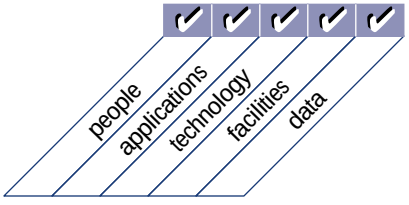
to minimise the likelihood of disruption, unauthorised alterations and errors

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



MANAGE CHANGES

CONTROL OBJECTIVES	
1	Change Request Initiation and Control
2	Impact Assessment
3	Control of Changes
4	Emergency Changes
5	Documentation and Procedures
6	Authorised Maintenance
7	Software Release Policy
8	Distribution of Software

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief Information Officer
IT management
IT system development, change control quality assurance, operations, and security management
Selected user management involved in the design and use of information systems applications

J **Obtaining:**

Organisational policies and procedures relating to: information systems planning, change control, security and system development life cycle
IT policies and procedures relating to: formal system development life cycle methodology, security standards, testing standards, independent quality assurance, implementation, distribution, maintenance, emergency change, software release and version control of systems.
Applications development plan
Change control request form and log
Vendor contracts relating to applications development services

Evaluating the controls by:

J **Considering whether:**

Methodology for prioritising system change requests from users exists and is in use
Emergency change procedures are addressed in operation manuals
Change control is a formal procedure for both user and development groups
Change control log ensures all changes shown were resolved
User is satisfied with turnaround of change requests — timeliness and cost

Considering whether, *continued*

For a selection of changes on the change control log:

- that change resulted in programme and operations documentation change
- that changes were made as documented
- current documentation reflects changed environment

Change process is being monitored for improvements in acknowledgment, response time, response effectiveness and user satisfaction with the process

Maintenance to Private Branch Exchange (PBX) system is included in the change control procedures

Assessing the compliance by:

J **Testing that:**

For a sample of changes, the following have been approved by management:

- request for change
- specification of change
- access to source programme
- programmer completion of change
- request to move source into test environment
- completion of acceptance testing
- request for compilation and move into production
- overall and specific security impact has been determined and accepted
- distribution process has been developed

Review of change control documentation for inclusion of:

- date of requested change
- person(s) requesting
- approved for change request
- approval of change made — IT function
- approval of change made — users
- documentation update date
- move date into production
- quality assurance sign-off of change
- acceptance by operations

Analyse types of changes made to system for identification of trends

Evaluate adequacy of IT libraries and determine the existence of base line code levels to prevent error regression

Code check-in and check-out procedures for changes exist

Change control log ensures all changes on log were resolved to user satisfaction and that there were no changes made not on log

Users are aware and understand need for formal change control procedures

Staff enforcement process ensures compliance to change control procedures

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of change control management against similar organisations or appropriate international standards/recognised industry best practices

For selected information services function systems:

- documentation determines request or system change has been approved and prioritised by the management of the affected users areas and services provider
- confirm existence and adequacy of impact assessment on change control form
- acknowledgment by system services function of change request receipt
- assignment of change to appropriate development resources
- adequacy of systems and user test plan and results
- formal migration from test into production via quality assurance group
- updated user and operations manuals to reflect change
- new version distribution to appropriate users

J **Identifying:**

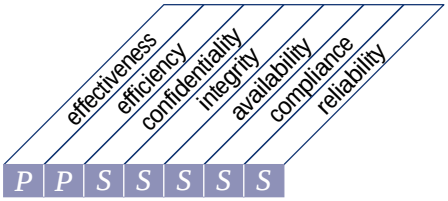
For a selection of information changes that:

- only approved changes were made
- all changes are accounted for
- current libraries (source and object) reflect most recent changes
- change control procedure variances are recorded and accounted for between:
  - purchased and in-house applications
  - applications and system software
  - vendor treatment of change control

This page intentionally left blank

DELIVERY & SUPPORT

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

defining and managing service levels

that satisfies the business requirement

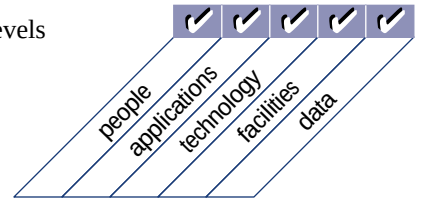
to establish a common understanding of the level of service required

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



DEFINE AND MANAGE SERVICE LEVELS

CONTROL OBJECTIVES	
1	Service Level Agreement Framework
2	Aspects of Service Level Agreements
3	Performance Procedures
4	Monitoring and Reporting
5	Review of Service Level Agreements and Contracts
6	Chargeable Items
7	Service Improvement Programme

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief information officer
IT senior management
IT contract/service level administrator
IT operations management
User management

J **Obtaining:**

Organisation-wide polices and procedures relating to provider/user relationships
IT policies and procedures relating to:

- Service level agreements
- Operational reporting content, timing and distribution
- Performance tracking methods
- Corrective action activities

IT documentation relating to:

- Service level performance reports
- Chargeback algorithms and methodology for calculating charges
- Service improvement programmes
- Recourse resulting from non-performance
- Service level agreements with internal and external users and providers of services

Evaluating the controls by:

J **Considering whether:**

A service level agreement process is identified by policy
User participation in process is required for creation and modification of agreements

Considering whether, *continued*

Responsibilities of users and providers are defined

Management monitors and reports on the achievement of the specified service performance criteria and all problems encountered

Regular review process by management exists

Recourse process is identified for non-performance

Service level agreements include, but are not limited to having:

- definition of service
- cost of service
- quantifiable minimum service level
- level of support from the IT function
- availability, reliability, capacity for growth
- continuity planning
- security requirements
- change procedure for any portion of the agreement
- written and formally approved agreement between provider and user of service
- effective period and new period review/renewal/non-renewal
- content and frequency of performance reporting and payment for services
- charges are realistic compared to history, industry, best practices
- calculation for charges
- service improvement commitment

Assessing the compliance by:

J **Testing that:**

For a sample of past and in-process service level agreements, that content includes:

- definition of service
- cost of service
- quantifiable minimum service level
- level of support from the IT function
- availability, reliability, capacity for growth
- change procedure for any portion of agreement
- continuity planning
- security requirements
- written and formally approved agreement between provider and user of service
- effective period and new period review/renewal/non-renewal
- content and frequency of performance reporting and payment for services
- charges are realistic compared to history, industry, best practices
- calculation for charges
- service improvement commitment
- both user and provider formal approval

Appropriate users are aware and understand service level agreement processes and procedures

User's level of satisfaction with current service level process and actual agreements is sufficient

Service provides records to ascertain reasons for non-performance and to ensure performance improvement programme in place

Accuracy of actual charges matches agreement content

Historical performance against prior service improvement commitments is tracked

Reports on achievement of the specified service performance are appropriately used by management to ensure satisfactory performance

Reports of all problems encountered are appropriately used by management to ensure corrective actions are taken

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of service level agreements against similar organisations or appropriate international standards/recognised industry best practices

Review of:

- service level agreement to determine qualitative and quantitative provisions confirming obligations are defined and being met
- selected service level agreement to confirm resolution procedures for problems, specifically non-performance, are included and being met

J **Identifying:**

Adequacy of provision describing, coordinating and communicating the relationship between the provider and user of information services

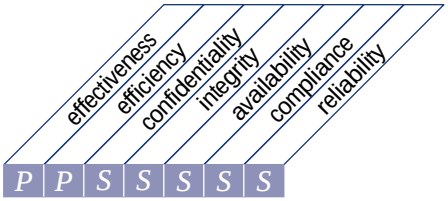
Incorrect calculations for selected categories of information

Ongoing review and corrective action by management of service level reporting

Adequacy of proposed service improvements in comparison with cost/benefit analysis

Adequacy of providers ability to meet improvement commitments in future

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing third-party services

that satisfies the business requirement

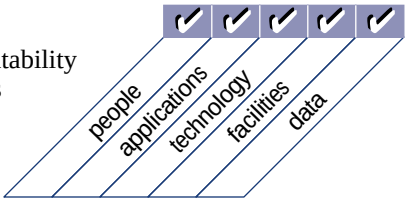
to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements

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



MANAGE THIRD-PARTY SERVICES

CONTROL OBJECTIVES	
1	Supplier Interfaces
2	Owner Relationships
3	Third-Party Contracts
4	Third-Party Qualifications
5	Outsourcing Contracts
6	Continuity of Services
7	Security Relationships
8	Monitoring

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief information officer
IT senior management
IT contract/service level administrator
IT operations management
Security officer

J **Obtaining:**

Organisation-wide polices and procedures relating to purchased services and, in particular, third-party vendor relationships
IT policies and procedures relating to: third-party relationships, vendor selection procedures, contract content of such relationships, physical and logical security, quality maintenance of vendors, contingency planning and outsourcing
List of all current third-party relationships and actual contracts associated with each
Service level reporting related to third-party relationships and services
Minutes of meetings discussing contract review, performance evaluation and relationship management
Confidentiality agreements for all third-party relationships
Security access listings with profiles and resources available to vendors

Evaluating the controls by:

J **Considering whether:**

IT policies and procedures relating to third-party relationships exist and are consistent with organisational general policies
Policies exist specifically addressing need for contracts, definition of content of contracts, owner or relationship manager responsible for ensuring contracts are created, maintained, monitored and renegotiated as required

Considering whether, *continued*

Interfaces are defined to independent agents involved in the conduct of the project and any other parties, such as subcontractors

Contracts represent a full and complete record of third-party supplier relationships

Contracts are established for continuity of services specifically, and that these contracts include contingency planning by vendor to ensure continuous service to user of services

Contract contents include at least the following:

- formal management and legal approval
- legal entity providing services
- services provided
- service level agreements both qualitative and quantitative
- cost of services and frequency of payment for services
- resolution of problem process
- penalties for non-performance
- dissolution process
- modification process
- reporting of service — content, frequency, and distribution
- roles between contracting parties during life of contract
- continuity assurances that services will be provided by vendor
- user of services and provider communications process and frequency
- duration of contract
- level of access provided to vendor
- security requirements
- non-disclosure guarantees
- right to access and right to audit

Escrow agreements have been negotiated where appropriate

Potential third-parties are properly qualified through an assessment of their capability to deliver the required service (due diligence)

Assessing the compliance by:

J **Testing that:**

List of contracts, and actual contracts in place, is accurate

No services are being provided by vendors not on the contract list

Providers on contracts are actually performing services defined

Provider management/owners understand their responsibilities in contracts

IT policies and procedures relating to third-party relationships exist and are consistent with organisational general policies

Policies exist specifically addressing need for contracts, definition of content of contracts, owner or relationship manager responsible for ensuring contracts are created, maintained, monitored and renegotiated as required

Contracts represent a full and complete record of third-party supplier relationships

Contracts are established for continuity of services specifically, and that these contracts include contingency planning by vendor to ensure continuous service to user of services

Contract contents include at least the following:

- formal management and legal approval
- legal entity providing services
- services provided
- service level agreements both qualitative and quantitative
- cost of services and frequency of payment for services
- resolution of problem process
- penalties for non-performance
- dissolution process
- modification process
- reporting of service — content, frequency and distribution
- roles between contracting parties during life of contract
- continuity assurances that services will be provided by vendor
- user of services and provider communications process and frequency
- duration of contract
- level of access provided to vendor
- security requirements
- non-disclosure guarantees
- right to access and right to audit

Users are aware and understand need for contract policies and contracts to provide services
Appropriate independence between vendor and organisation exists
Independence of vendor sourcing and selection processes is occurring
Security access lists include only minimum number of vendor staff as required, and that access is the least needed
Access hardware and software to organisation resources is managed and controlled to minimise vendor use
Actual level of service being performed compares highly to contractual obligations
Outsourcing facilities, staff, operations, and controls ensure required level of performance comparable to expectation
Continuous monitoring of service delivery by third-parties is performed by management
Independent audits of contractor operations occurs
Assessment reports exist for potential third-parties to assess their capability to deliver the required service
History of litigation activity — past and current
Interfaces to independent agents involved in the conduct of the project are documented in the contract
Contracts with Private Branch Exchange (PBX) suppliers are covered

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of third-party services against similar organisations or appropriate international standards/recognised industry best practices
A detailed review of each third-party contract to determine qualitative and quantitative provisions confirming obligations are defined

J **Identifying:**

Provisions describing, coordinating and communicating the relationship between the provider and user of information services
Third-party invoices reflect charges accurately for selected contract services

Identifying, *continued*

Organisational liaison with third-party vendors ensures communication of contract issues between parties and users of services

Legal counsel and management approve all contracts

Ongoing risk assessment occurs to confirm need for relationship or need for modifying the relationship

Ongoing review and corrective action by management of contract reporting is occurring

Reasonableness of charges compared to various internal, external and industry comparable performance is done

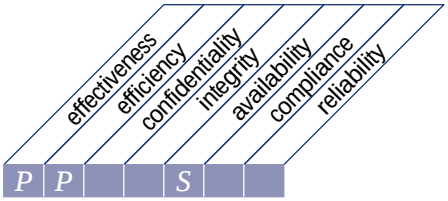
Contingency plans are in place for all contracted services, specifically disaster recovery services for the IT function

For outsourced functions, apparent shortcomings or opportunities to improve performance or reduce costs exist

Implementation of recommendations contained in independent audits of the contractor is occurring

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing performance and capacity

that satisfies the business requirement

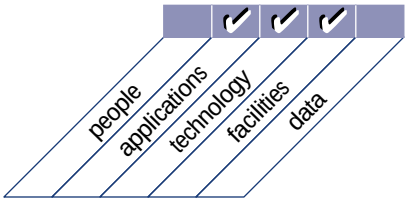
to ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs

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



MANAGE PERFORMANCE AND CAPACITY

CONTROL OBJECTIVES	
1	Availability and Performance Requirements
2	Availability Plan
3	Monitoring and Reporting
4	Modeling Tools
5	Proactive Performance Management
6	Workload Forecasting
7	Capacity Management of Resources
8	Resources Availability
9	Resources Schedule

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT senior management
IT operations management
IT capacity management
IT network management

J **Obtaining:**

Organisation-wide polices and procedures relating to availability, performance monitoring and reporting, workload forecasting, capacity management and scheduling
IT policies and procedures relating to: linkage of capacity to business plan of the organisation availability of services, availability planning, continuous monitoring and performance management
Vendor product representations with respect to capacity and performance norms
List of all current vendor products for hardware, software, communications and peripherals
Communications network monitoring reports
Minutes of meetings discussing capacity planning, performance expectations and “fine tuning” of performance
Availability, capacity, workload and resource planning documents
Annual IT budget including assumptions regarding capacity and performance
Reports relating to operational performance within the IT function, including problem reporting and resolution history

Evaluating the controls by:

J **Considering whether:**

Time frames and level of service are defined for all services provided by the IT function

Considering whether, *continued*

Time frames and service levels reflect user requirements

Time frames and service levels are consistent with performance expectations of the equipment potentials

An availability plan exists, is current and reflects user requirements

Ongoing performance monitoring of all equipment and capacity is occurring, reported upon, lack of performance addressed by management and performance improvement opportunities are formally addressed

Optimal configuration performance is being monitored by modelling tools to maximise performance while minimising capacity to required levels

Both users and operational performance groups are pro-actively reviewing capacity and performance and workload schedule modifications are occurring

Workload forecasting includes input from users on changing demands and from suppliers on new technology or current product enhancements

Assessing the compliance by:

J **Testing that:**

Statistics on performance, capacity, availability reports are accurate, including historical versus forecast performance variance explanation

Change process for modifying availability, capacity, workload planning documents reflects changing technology or user requirements

Work flow analysis reports address opportunities of additional process efficiencies

Performance reporting information to users relating to usage and availability exists, including, capacity, workload scheduling and trends

Escalation procedures exist, are being followed and are appropriate in resolving problems

System development methodology post-implementation phase includes criteria for determining future growth and changes to performance expectations

Levels of support supplied by the IT function are sufficient to support the goals of the organisation

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking performance and capacity management against similar organisations or appropriate international standards/recognised industry best practices

Tests of on-going business needs, to ensure that the IT availability terms and requirements adequately reflect those needs

Capacity and resource planning process review, to ensure timely modification of plans based on changing business needs

Verification that performance expectations are being met relating to capacity, response and availability

Comparison of the performance requirements from a cost/benefit analysis perspective, to ensure no surplus of capacity or resources exists

Verification of performance reporting produced and reviewed by management on a periodic basis

J **Identifying:**

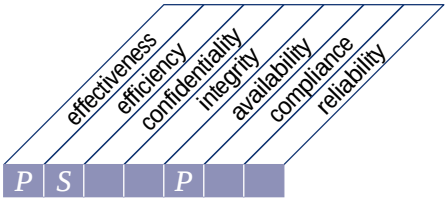
Performance reporting for improvement opportunities or remedy of weaknesses

Users and confirming performance expectations are being met, and modifications based on changing requirements are being reflected in plan

Problem logs or reports that confirm problems occurring during processing were addressed in a timely manner and appropriate corrective action taken

Specific problems encountered and ascertain effectiveness of problem resolution process

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring continuous service

that satisfies the business requirement

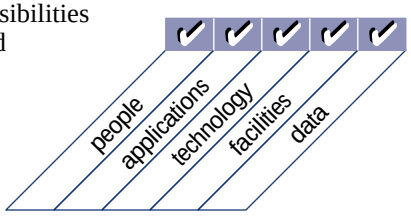
to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption

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



ENSURE CONTINUOUS SERVICE

CONTROL OBJECTIVES	
1	IT Continuity Framework
2	IT Continuity Plan Strategy and Philosophy
3	IT Continuity Plan Contents
4	Minimising IT Continuity Requirements
5	Maintaining the IT Continuity Plan
6	Testing the IT Continuity Plan
7	IT Continuity Plan Training
8	IT Continuity Plan Distribution
9	User Department Alternative Processing Back-up Procedures
10	Critical IT Resources
11	Back-up Site and Hardware
12	Off-site Back-up Storage
13	Wrap-up Procedures

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT senior management
IT operations management
IT continuity management
Human resources or training management
User organisations with continuity needs
Vendor recovery site manager
Off-site storage manager
Risk/insurance manager

J **Obtaining:**

Organisation-wide policies and procedures relating to continuity planning process
IT policies and procedures relating to: continuity framework, plan, philosophy, strategy, prioritisation of applications, plan testing, regular back-up and rotation and training
IT continuity plans
User of services of continuity plans
Results of most recent tests of continuity and business resumption user plans
Methodology for determining application prioritisation in event of need to recover
Vendor contracts supporting continuity support services
Business interruption insurance policies

Evaluating the controls by:

J **Considering whether:**

Organisational policies require a continuity framework and plan be part of normal operational requirements for both the IT function and all organisations dependent on IT resources

IT policies and procedures require:

- a consistent philosophy and framework relating to development of continuity plan development
- a prioritisation of applications with respect to timeliness of recovery and return
- risk assessment and insurance consideration for loss of business in continuity situations for the IT function as well as users of resources
- outline specific roles and responsibilities with respect to continuity planning with specific test, maintenance and update requirements
- formal contract arrangements with vendors to provide services in event of need to recover, including back-up site facility or relationship, in advance of actual need
- in each continuity plan minimum content to include:
  - Emergency procedures to ensure the safety of all affected staff members
  - Roles and responsibilities of the IT function, vendors providing recovery services, users of services and support administrative personnel
  - A recovery framework consistent with long-range plan for continuity
  - Listing of systems resources requiring alternatives (hardware, peripherals, software)
  - Listing of highest to lowest priority applications, required recovery times and expected performance norms
  - Administrative functions for communicating and providing support services such as benefits, payroll, external communications, cost tracking, etc., in event of need to recover
  - Various recovery scenarios from minor to loss of total capability and response to each in sufficient detail for step-by-step execution
  - Specific equipment and supply needs are identified such as high speed printers, signatures, forms, communications equipment, telephones, etc., and a source and alternative source defined
  - Training and awareness of individual and group roles in continuity plan
  - Testing schedule, results of last test and corrective actions taken based on prior test(s)
  - Itemisation of contracted service providers, services and response expectations
  - Logistical information on location of key resources, including back-up site for recovery operating system, applications, data files, operating manuals and programme/system/user documentation
  - Current names, addresses, telephone/pager numbers of key personnel
  - Reconstruction plans are included for re-recovery at original location of all systems resources
  - Business resumption alternatives for all users for establishing alternative work locations once IT resources are available; i.e., system recovered at alternative site but user building burned to the ground and unavailable

Regulatory agency requirements with respect to continuity planning are met

User continuity plans are developed based on unavailability of physical resources for performing critical processing — manual and computerised

The telephone system, VoiceMail, fax and image systems are part of the continuity plan

Image systems, fax systems, paper documents as well as microfilm and mass storage media are part of the continuity plan

Assessing the compliance by:

J **Testing that:**

Continuity plan exists, is current and is understood by all affected parties
Regular continuity plan training has been provided to all parties involved

All policies and procedures regarding plan development have been followed

Content of plan is based on content described above and includes:

- continuity plan objectives have been met
- appropriate individuals have been selected to provide leadership roles
- plan has received appropriate review and approval by management
- plan has been tested recently and it worked according to the plan or any deficiencies identified resulted in corrections to the plan
- linkage between continuity plan and business plan of the organisation
- alternative manual procedures are documented and tested as part of overall test

Training and awareness of users and IT staff has occurred on specific role, tasks and responsibilities within the plan

Contracted vendor relationships and lead times are consistent with user expectation and need

Back-up site contents are current and sufficient with respect to normal off-site rotation procedures

Critical data and operations are identified, documented and prioritised

Senior management approves critical data and operations

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of continuity planning against similar organisations or appropriate international standards/recognised best practices

Detailed review of:

- plan objectives to ensure an appropriate strategy and interface with overall business continuity strategy
- appropriate individuals understanding of responsibilities with respect to providing leadership as the plan coordinators
- plan as reviewed and approved by the appropriate levels of senior management
- selected members of the IT function and user department to verify that the business needs are included in the continuity plan
- alternative manual data processing user procedures to ensure they are documented by user departments for use when a need to occurs, and until able to restore processing operations after the event
- application-specific supplies, to ensure there is sufficient inventory at an off-site location (i.e., magnetic tapes, check stock, stock certificates, etc.)

J **Identifying:**

Vendor contracts to verify lead times to obtain supplies and sufficiency of detail on services, timing, service levels and costs

Provisions for acquiring specialised telecommunications or network components

Varying scenarios as part of the plan from short-term to permanent outages

Applications prioritisation that occurred as consistent with user expectation

That there are written contracts for off-site computer facilities commensurate with needs

Identifying, *continued*

Alternative site processing speeds, response, availability, support, as sufficient for user requirements

Vendor(s) continuity plan(s) to ensure continuity of their services in event of need to recover

Alternative service provider's remoteness from own site, to eliminate possibility of mutual recovery events

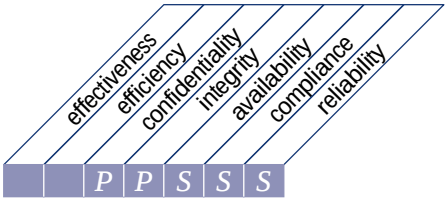
Periodic tests of the plan having occurred and plan adjusted based on tests

Both IT and user staff, are receiving training on continuity planning on a regular basis

That there are similar reconstruction teams, tasks and responsibilities, and tests to migrate processing from alternative processing to original site

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

ensuring systems security

that satisfies the business requirement

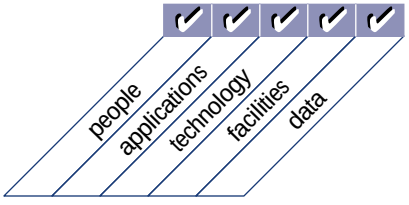
to safeguard information against unauthorised use, disclosure or modification, damage or loss

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



ENSURE SYSTEMS SECURITY

CONTROL OBJECTIVES	
1	Manage Security Measures
2	Identification, Authentication and Access
3	Security of Online Access to Data
4	User Account Management
5	Management Review of User Accounts
6	User Control of User Accounts
7	Security Surveillance
8	Data Classification
9	Central Identification and Access Rights Management
10	Violation and Security Activity Reports
11	Incident Handling
12	Reaccreditation
13	Counterparty Trust
14	Transaction Authorisation
15	Non-Repudiation
16	Trusted Path
17	Protection of Security Functions
18	Cryptographic Key Management
19	Malicious Software Prevention, Detection and Correction
20	Firewall Architectures and Connections with Public Networks
21	Protection of Electronic Value

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Senior security officer of the organisation
IT senior and security management
IT data base administrator
IT security administrator
IT application development management

J **Obtaining:**

Organisation-wide policies and procedures relating to information system security and access
IT policies and procedures relating to information systems security and access
Relevant policies and procedures, and legal and regulatory body information systems security requirements (i.e., laws, regulations, guidelines, industry standards) including:

- user account management procedures

Obtaining, *continued*

- user security or information protection policy
- standards regarding electronic commerce
- data classification schema
- inventory of access control software
- floor plan of buildings/rooms housing IT resources
- inventory or schematic of physical access points to IT resources (i.e., modems, telephone lines and remote terminals)
- security software change control procedures
- problem tracking, resolution and escalation procedures
- security violation reports and management review procedures
- inventory of data encryption devices and encryption standards
- list of vendors and customers with access to system resources
- list of service providers used in transmission of data
- network management practices regarding continuous security testing
- copies of contracts with service providers for data transmission
- copies of signed user security and awareness documents
- content of new employee training materials relating to security
- audit reports from external auditors, third-party service providers and governmental agencies related to information system security

Evaluating the controls by:

J **Considering whether:**

Strategic security plan is in place providing centralised direction and control over information system security, along with user security requirements for consistency

Centralised security organisation is in place responsible for ensuring only appropriate access to system resources

Data classification schema is in place and being used, that all system resources have an owner responsible for security and content

User security profiles are in place representing "least access as required" and profiles are regularly reviewed by management for re-accreditation

Employee indoctrination includes security awareness, ownership responsibility and virus protection requirements

Reporting exists for security breaches and formal problem resolution procedures are in place, and these reports include:

- unauthorised attempts to access system (sign on)
- unauthorised attempts to access system resources
- unauthorised attempts to view or change security definitions and rules
- resource access privileges by user ID
- authorised security definitions and rule changes
- authorised access to resources (selected by user or resource)
- status change of the system security
- accesses to operating system security parameter tables

Cryptographic modules and key maintenance procedures exist, are administered centrally and are used for all external access and transmission activity

Cryptographic key management standards exist for both centralised and user activity

Change control over security software is formal and consistent with normal standards of system development and maintenance

The authentication mechanisms in use provide one or more of the following features:
- single-use of authentication data (e.g., passwords are never re-usable)
- multiple authentication (i.e., two or more different authentication mechanisms are used)
- policy-based authentication (i.e., ability to specify separate authentication procedures for specific events)
- on-demand authentication (i.e., ability to re-authenticate the user at times after the initial authentication)

The number of concurrent sessions belonging to the same user is limited

At log-on, an advisory warning message to users regarding the appropriate use the hardware, software or connection logged on

A warning screen is displayed prior to completing log-on to inform reader that unauthorised access may result in prosecution

Upon successful session establishment, a history of successful and unsuccessful attempts to access the user's account is displayed to the user

Password policy includes:
- initial password change on first use enforced
- an appropriate minimum password length
- an appropriate and enforced frequency of password changes
- password checking against list of not allowed values (e.g., dictionary checking)
- adequate protection of emergency passwords

Formal problem resolution procedures include:
- User ID is suspended after 5 repeated unsuccessful log-on attempts
- Date, time of last access and number of unsuccessful attempts is displayed to authorised user at log-on
- Authentication time is limited to 5 minutes, after which the session is terminated
- User is informed of suspension, but not the reason for it

Dial in procedures include dial-back or token based authentication, frequent changes of dial-up numbers, software and hardware firewalls to restrict access to assets and frequent changes of passwords and deactivation of former employees' passwords

Location control methods are used to apply additional restrictions at specific locations

Access to the VoiceMail service and the PBX system are controlled with the same physical and logical controls as for computer systems

Enforcement of sensitive position policies occurs, including:
- employees in sensitive job positions are required to be away from the organisation for an appropriate period of time every calendar year; during this time their user ID is suspended; and persons replacing the employee are instructed to notify management if any security-related abnormalities are noted
- unannounced rotation of personnel involved in sensitive activities is performed from time to time

Security-related hardware and software, such as cryptographic modules, are protected against tampering or disclosure, and access is limited to a "need to know" basis

Access to security data such as security management, sensitive transaction data, passwords and cryptographic keys is limited to a need to know basis

Trusted paths are used to transmit non-encrypted sensitive information

To prevent denial of service due to an attack with junk faxes, protective measures are taken such as:
- limiting the disclosure of fax numbers outside the organisation to a "need-to-know" basis
- fax lines used for solicitation of business are not used for other purposes

Preventative and detective control measures have been established by management with respect to computer viruses

To enforce integrity of electronic value, measures are taken such as:
- card reader facilities are protected against destruction, disclosure or modification of the card information
- card information (PIN and other information) is protected against insider disclosure
- counterfeiting of cards is prevented

To enforce protection of security features, measures are taken such as:
- the identification and authentication process is required to be repeated after a specified period of inactivity
- a one-button lock-up system, a force button or a shut-off sequence can be activated when the terminal is left alone

Assessing the compliance by:

J **Testing that:**

IT function is in compliance with security standards relating to:

- authentication and access
- managing user profiles and data security classifications
- violation and security incident reporting and management review
- cryptographic key management standards
- virus detection, resolution, and communication
- data classification and ownership

Procedures for requesting, establishing and maintaining user access to system exist

Procedures for external access to system resources exist, i.e., logon, ID, password, dial-back

Inventory of access devices for completeness is maintained

Operating system security parameters are based on vendor/local standards

Network security management practices are communicated, understood and enforced

External access provider contracts include consideration of security responsibilities and procedures

Actual log-on procedures for systems, users and external vendor access exist

Security reporting is occurring for timeliness, accuracy and management response to incidents

Secret keys exist for transmission utilisation

Procedures for protection from malicious software include:

- all software acquired by the organisation is checked for viruses prior to installation and use
- a written policy exists on downloading, acceptance, and use of freeware and shareware, and this policy is adhered to
- software for highly critical applications are protected by MAC (Message Authentication Code) or digital signature, and a failure to verify prevents the software from being used
- users have received instructions on the detection and reporting of viruses, such as sluggish performance or mysterious growth of files
- a policy and procedure exists and is adhered to for the checking of diskettes brought in from outside the organisation's normal purchasing programme

Firewalls have at least the following properties:

- all traffic from inside to outside, and vice-versa, must pass through the firewall (this should not be limited to logical controls, but should also be physically enforced)
- only authorised traffic, as defined by local security policy, will be allowed to pass
- the firewall itself is immune to penetration
- traffic is exchanged through the firewall at the application layer only
- the firewall architecture combines control measures both at the application and network level
- the firewall architecture enforces a protocol discontinuity at the transportation layer
- the firewall architecture should be configured according to the "minimal art philosophy"
- the firewall architecture should deploy strong authentication for management of its components
- the firewall architecture hides the structure of the internal network
- the firewall architecture provides an audit trail of all communications to or through the firewall system and will generate alarms when suspicious activity is detected
- organisation's hosts, which provide support for incoming service requests from the public network, are sitting outside the firewall
- the firewall architecture defends itself from direct attack (e.g., through active monitoring of traffic and pattern recognition technology)

- all executable code is scanned for malicious code (e.g., viruses, malicious applets) before it is introduced to the internal network

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of information system security against similar organisations or appropriate international standards/recognised industry best practices

A detailed review of information system security, including penetration evaluations of physical and logical security of computer and communications resources, etc.

Interview of new employees to ascertain awareness of security and individual responsibilities (i.e., confirm signed security statements and new employee training regarding security)

Interview of users to ascertain that access is determined on a business need (“least needed”) and reviewed regularly by management for accuracy

J **Identifying:**

Inappropriate user access to system resources

Inconsistencies with network schematic or inventory relating to missing access points, missing accessories, etc.

Contract deficiencies relating to ownership and responsibilities relating to data integrity and security at any point in transmission between send and receipt

Employees not verified as legitimate users, or separated former employees still having access

Informal or unapproved requests for access to system resources

Network monitoring software that does not alert network management of security breaches

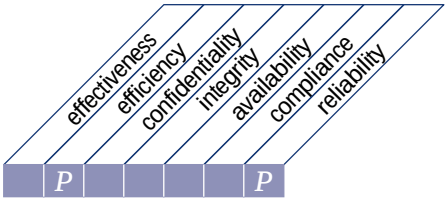
Shortcomings of network software change control procedures

Non-use of secret keys in third-party submission/receipt procedures

Deficiencies in protocols for key generation, distribution, storage, entry, use, archiving and protection

Non-current virus detection software or lack of formal procedures for preventing, detecting, correcting and reporting infestations

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

identifying and allocating costs

that satisfies the business requirement

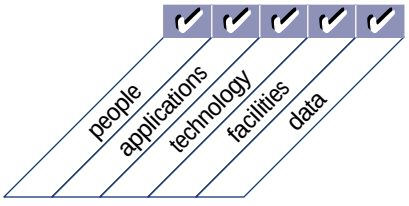
to ensure a correct awareness of the costs attributable to IT services

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



IDENTIFY AND ALLOCATE COSTS

CONTROL OBJECTIVES	
1	Chargeable Items
2	Costing Procedures
3	User Billing and Chargeback Procedures

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT administrative or cost allocation management
Selected user management charged back and absorbing costs

J **Obtaining:**

Organisation-wide polices and procedures relating to planning and budget preparation
IT policies and procedures relating to cost aggregation, chargeback methodology and performance/cost reporting
IT function's:

- Current and prior year budget
- Tracking reports of IT resource utilisation
- Raw data used in preparing tracking reports
- Cost allocation methodology or algorithm
- Historical chargeback reports

User management's:

- Current and prior year budget for IT costs
- Current year information systems development and maintenance plan
- Budgeted expenses for IT resources, including those charged back or absorbed

Evaluating the controls by:

J **Considering whether:**

IT function has a group responsible for reporting and issuing chargeback bills to users
Procedures are in place that:

- develop a yearly development and maintenance plan with user identification of priorities for development, maintenance and operational expenses
- allow for a very high level of user determination of where IT resources are spent
- generate a yearly IT budget including:
  - Compliance to organisational requirements in budget preparation
  - Consistency with what costs are to be allocated by the user departments

Considering whether, *continued*

- Communication of historical costs, assumptions for new costs— for understanding by users of what costs are included in chargeback
- User sign-off on all budget costs to be allocated by IT function
- Frequency of reporting and actual charging of costs to users

- track allocated costs of all IT resources of, but not limited to:
  - Operational hardware
  - Peripheral equipment
  - Telecommunications usage
  - Applications development and support
  - Administrative overhead
  - External vendor service costs
  - Help desk
  - Facilities and maintenance
  - Direct/indirect costs
  - Fixed and variable expenses
  - Sunk and discretionary costs
- for regular reporting to users on performance for the various cost categories
- report to users on external benchmarks regarding cost effectiveness so as to allow comparison to industry expectations, or user alternative sourcing for services
- for timely modification to cost allocations to reflect changing business needs
- formally approve and accept charges as received
- identify IT improvement opportunities to reduce chargebacks or get greater value for chargebacks

Reports provide assurance that chargeable items are identifiable, measurable and predictable

Reports capture and highlight changes in the underlying cost components or allocation algorithm

Assessing the compliance by:

J **Testing that:**

A cost allocation methodology exists, is agreed with users for equity, and is generating both costs and reports, re: calculation to confirm

Improvement programme to reduce costs or increase performance of IT resources exists

Allocation and reporting encourage the most proper, effective and consistent use of IT resources, assure fair treatment of user departments and their needs, and charge rates reflect the associated costs of providing services

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of cost accounting and chargeback methodologies against other similar organisations or appropriate international standards/recognised industry best practices

Recalculation of chargeback from raw data, through chargeback allocation algorithm and into user report streams

Data into performance reporting is accurate, such as:
- CPU usage
- peripheral usage
- DASD usage
- lines of code written
- lines/pages printed
- programme changes made
- number of PCs, telephones, data files
- help desk inquiries
- number, length of transmissions

Compilation of raw information resource data into performance reporting is correct

Actual algorithm for compiling and allocating costs into chargeback exists

Accuracy of chargebacks to specific users is tested frequently

Chargebacks to users are approved

Consistency checks of chargebacks among different users

Progress on user development plan is based on costs expended

Report distribution review for usage and cost information

Review of user satisfaction with:
- reasonableness of chargebacks against budgeted expectations
- yearly development plan progress versus charged back costs
- reasonableness of chargebacks against alternative sources (i.e., benchmarks)
- communications of trends that would increase/decrease chargeback
- resolution of variances from expected chargeback

J **Identifying:**

Opportunities for increased effectiveness and appropriateness of chargeback methodology
- including more cost components
- modifying cost allocation indexes or units of measure
- modifying cost algorithm itself
- mechanising or integrating the job accounting function between equipment and application generating reports

Inconsistencies within the allocation algorithm

Inconsistencies of allocation among different users

Opportunities for systems resource improvements

Improved opportunities for the user to better apply IT resources to accomplish user business requirements

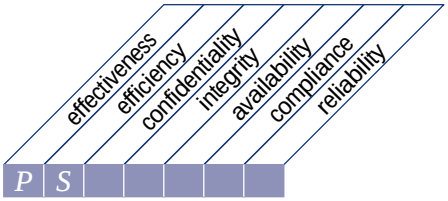
Improved efficiencies in the gathering, accumulation, allocation, reporting, and communicating process that will translate to improved performance or less cost to users for services provided

That cost trends reflected by variance and analysis were translated into modified charges in following periods and reflected in cost structure

That opportunities exist to make the IT function a profit centre, rather than a cost centre by providing services to other internal or external users

If the IT function is a profit centre, that the contribution to profit against plan and budget is being met, and opportunities for increased profitability are outlined

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

educating and training users

that satisfies the business requirement

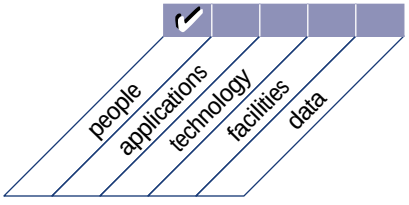
to ensure that users are making effective use of technology and are aware of the risks and responsibilities involved

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



EDUCATE AND TRAIN USERS

CONTROL OBJECTIVES	
1	Identification of Training Needs
2	Training Organisation
3	Security Principles and Awareness Training

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Organisation human resources or training manager
IT human resources or training manager
Selected managers and employees of the IT function
Selected managers and employees of the user departments

J **Obtaining:**

Organisation-wide polices and procedures relating to controls and security awareness training, developmentally focused employee benefits, user of services training programmes, educational resource facilities, and professional continuing education requirements
IT programmes, policies, and procedures on training and education related to controls and security awareness, technical security and controls
Available training programmes (both internal and external) for introductory and ongoing security and controls awareness and training within the organisation

Evaluating the controls by:

J **Considering whether:**

Policies and procedures relating to ongoing security and controls awareness exist
There is an education/training programme focusing on information systems security and control principles
New employees are made aware of security and control responsibility with respect to using and having custody of IT resources
There are policies and procedures in effect relating to training and they are current with respect to technical configuration of IT resources
Availability of in-house training opportunities and frequency of employee attendance
Availability of external technical training opportunities and frequency of employee attendance
A training function is assessing training needs of personnel with respect to security and controls, and translating those needs into in-house or external training opportunities
All employees are required to attend security and control awareness training on an ongoing basis that would include, but not be limited to:
- general system security principles
- ethical conduct related to IT

Considering whether, *continued*

- security practices to protect against harm from failures affecting availability, confidentiality, integrity and performance of duties in a secure manner
- responsibilities associated with custody and use of IT resources
- security of information and information systems when used off-site

Security awareness training includes a policy on preventing the disclosure of sensitive information through conversations (e.g., by announcing the status of the information to all persons taking part in the conversation)

Assessing the compliance by:

J **Testing that:**

New employees have awareness and understanding of security, controls and fiduciary responsibilities of owning and using IT resources

Employee responsibilities with respect to confidentiality, integrity, availability, reliability and security of all IT resources is communicated on an ongoing basis

A group within the IT function is formally responsible for IT training, security and controls awareness, and maintaining continuing education programmes for professional certifications

Ongoing assessment of employee training needs is addressed

Development or participation in training programmes relating to security and controls is part of training requirements

Actual training programmes for new and long-term employee security awareness exist

Confidentiality and conflict of interest statements are signed by all employees

There are no missing confidentiality and conflict of interest statements for employees

There are no missing training needs assessments for employees

Substantiating the risk of control objectives not being met by:

J **Performing:**

A review of training manuals for adequacy and sufficiency with respect to security, confidentiality, reliability, availability and integrity controls

Interviews of IT staff to determine identification of training needs and extent of fulfilment of those needs

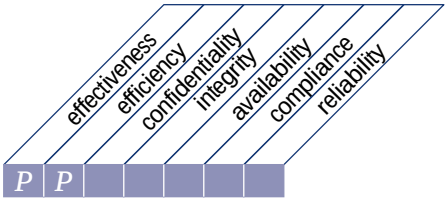
J **Identifying:**

Inconsistencies in curriculum offered in response to training needs

Deficiencies in user awareness of security and internal control issues relating to the use of IT resources

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assisting and advising customers

that satisfies the business requirement

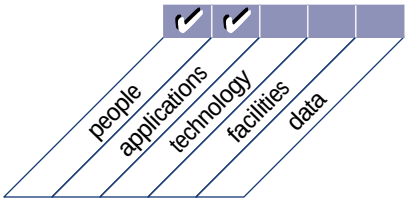
to ensure that any problem experienced by the user is appropriately resolved

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



ASSIST AND ADVISE CUSTOMERS

CONTROL OBJECTIVES	
1	Help Desk
2	Registration of Customer Queries
3	Customer Query Escalation
4	Monitoring of Clearance
5	Trend Analysis and Reporting

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT help desk support manager
Selected users of information services

J **Obtaining:**

Organisation-wide polices and procedures relating to IT user support
IT charter, mission, organisation chart, and policies and procedures relating to help desk activities
Reports relating to user queries, resolution of queries, and performance statistics of help desk
Any performance standards for help desk activities
Service level agreements between IT function and various users
Personnel files outlining experiential and professional credentials of help desk staff

Evaluating the controls by:

J **Considering whether:**

Nature of help desk function (i.e., how requests for assistance are processed and assistance is provided) is effective
Actual facilities, divisions or departments are performing the help desk function and the individuals or positions responsible for the help desk
Level of documentation for help desk activities is adequate and current
Actual process for logging or registering requests for service and use of logs exists
Process for query escalation and management intervention for resolution is sufficient
Time frame for clearing queries received is adequate
Procedures for tracking trends and reporting on help desk activities exist
Performance improvement initiatives are formally identified and executed
Service level agreements and performance standards are being met
User satisfaction level is periodically determined and reported

Assessing the compliance by:

J **Testing that:**

Policies and procedures are current and accurate relating to help desk activities
Service level commitments are being kept and variances explained
Clearing of queries is occurring in a timely manner
Trend analysis and reporting is providing assurances that reports:
- are produced and trends acted upon for improved service
- include specific problems, trend analyses, and response times
- are delivered to a responsible individual with authority to resolve problems

For a sample of help requests, confirmation of accuracy, timeliness and sufficiency of response
User satisfaction level inquiries exist and are acted upon

Substantiating the risk of control objectives not being met by:

J **Performing:**

Interview of selected users to ascertain satisfaction with:
- help desk activities
- activity reporting
- meeting of service level commitments

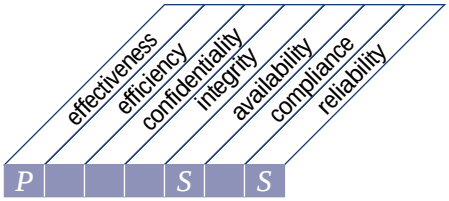
Review of help desk staff competency and capability with respect to performing duties
Review of selected escalated queries for adequacy of response
Review of reporting for trends and possible performance enhancement opportunities

J **Identifying:**

Inadequate interaction of help desk activities with respect to other organisations within the IT function, as well as user organisations
Insufficient procedures and activities relating to problem reporting query receipt, registration, logging, tracking, escalation and resolution
Deficient escalation process with respect to lack of managerial involvement or effective corrective actions
Inadequate timeliness of problem reporting or user dissatisfaction with problem reporting process

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing the configuration

that satisfies the business requirement

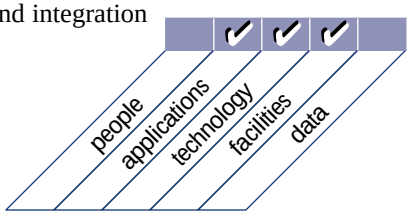
to account for all IT components, prevent unauthorised alterations, verify physical existence and provide a basis for sound change management

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



MANAGE THE CONFIGURATION

CONTROL OBJECTIVES	
1	Configuration Recording
2	Configuration Baseline
3	Status Accounting
4	Configuration Control
5	Unauthorised Software
6	Software Storage
7	Configuration Management Procedures
8	Software Accountability

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT operations management
IT systems support management
IT applications development management
Facilities management
Software vendors support personnel
Computer-related asset management personnel
Quality assurance manager

J **Obtaining:**

Configuration inventory: hardware, operating system software, applications software, facilities and data files — on site and off-site
Organisational polices and procedures relating to the acquisition, inventory and disposition of purchased, rented and leased computer-related equipment and software
Organisation policies relating to use of unauthorised software or equipment
IT policies and procedures relating specifically to acquisition, disposition and maintenance of configuration resources
IT policies and procedures for the quality assurance and change control functions for independent moving and recording migration of new and modified software development into production status and files
Configuration baseline information
Accounting records for fixed assets and leases relating to systems resources
Reports relating to additions, deletions and changes to systems configuration
Listings of various library contents — test, development and production
Inventory of off-site storage contents — equipment, files, manuals and forms — including materials in the hands of suppliers

Evaluating the controls by:

J **Considering whether:**

Process for creating and controlling configuration baselines (the cut-off point in the design and development of a configuration item beyond which evolution does not occur without undergoing strict configuration control) is appropriate

Functions for maintaining configuration baseline exist

Process for controlling status accounting of purchased and leased resources - including inputs, outputs and integration with other processes - exists

Configuration control procedures include:

- configuration baseline integrity
- programmed access authorisation controls over the change management system
- the recovery of configuration items and change requests at any point in time
- completion of configuration and reports assessing the adequacy of configuration recording procedures
- periodic evaluations of the configuration recording function
- individuals responsible for reviewing configuration control have the requisite knowledge, skills and abilities
- procedures exist for reviewing access to software baselines
- results of reviews are provided to management for corrective action

Periodic review of configuration with inventory and accounting records is performed on a regular basis

Configuration baseline has sufficient history for tracking changes

Software change control procedures exist for:

- establishing and maintaining licensed application programme library
- ensuring licensed application programme library is adequately controlled
- ensuring the reliability and integrity of the software inventory
- ensuring the reliability and integrity of the inventory of authorised software used and checking for unauthorised software
- assigning responsibility for unauthorised software control to a specific staff member
- recording use of unauthorised software and reporting to management for corrective action
- determining whether management took corrective action on violations

Process for migrating developmental applications into the testing environment and ultimately into production status interact with configuration reporting

The software storage process includes:

- defining a secure file storage area (library) for all valid software in appropriate phases of the system development life cycle
- requiring that software storage libraries are separated from each other and from development, testing and production file storage areas
- requiring existence within source libraries that allow temporary location of source modules moving into production cycle period
- requiring that each member of all libraries has an assigned owner
- defining logical and physical access controls
- establishing software accountability
- establishing an audit trail
- detecting, documenting and reporting to management all instances of non-compliance with this procedure
- determining whether management took corrective action

Coordination is occurring among applications development, quality assurance and operations with respect to updating configuration baseline upon change

Software is labeled and periodically inventoried

Library management software is used to:

- produce audit trails of program changes
- maintain program version numbers
- record and report program changes

- maintain creation/date information for production modules
- maintain copies of previous versions
- control concurrent updates

Assessing the compliance by:

J **Testing that:**

All configuration items are under baseline control

Policies and procedures relating to configuration reporting are current and accurate

Standards of performance with respect to configuration maintenance and reporting are adhered to

Configuration baseline comparison against physical inventory of equipment and asset accounting records are occurring

There exists independence of migration from test into production and recording of change

For a selection of baseline outputs, that:

- an accurate, appropriate and approved baseline of configuration items is kept
- configuration records reflect the actual status of all configuration items, including history of changes
- consistency of configuration recording is periodically reviewed and evaluated by management, and corrective action is taken
- file libraries were properly and adequately defined and in appropriate phases of the system development life cycle
- any personal computers that contain unauthorised software, violations are reported and management takes corrective action
- configuration records with respect to product, version and modifications to all vendor-supplied resources are accurate
- historical records of changes to configuration are accurate
- mechanism for ensuring no unauthorised software is on computers, including:
  - Policies and statements
  - Training and awareness of potential liabilities (legal and product)
  - Signed forms of compliance by all staff using computers
  - Centralised control of computer software
  - Ongoing review of computer software
  - Reporting on results of review
  - Corrective actions by management based on review results
- storage of application programmes and source code is determined during the developmental cycle and impact on configuration records is being ascertained
- sufficiency and integrity of off-site and vendor records relating to configuration, and accuracy on configuration records is being anticipated and considered
- configuration baseline procedures are defined for:
  - Recording the event that created the baseline, the establishment of the baseline and the configuration items that are to be controlled in the baseline
  - Changing the baseline, including the authority required to approve changes to previously approved configuration baselines
  - Recording the changes to the baseline and the configuration items that are to be controlled in the baseline
  - Ensuring that all configuration items are recorded into baseline products

Testing that, *continued*

- status accounting reporting is occurring for:
  - Type of information to be collected, stored, processed and reported (This should include the status of the baseline; findings of baseline reviews; change requests and status; configuration control board (if applicable) review and approval/disapproval; changes actually made; trouble reports and status; and the revision history of configuration)
  - How change request issues are resolved with incomplete status accounting
  - Types of status accounting reports to be generated and frequency
  - How access to this status data will be controlled

Substantiating the risk of control objectives not being met by:

J **Performing:**

A detailed review of the frequency and timeliness of management reviews of configuration records, changes to records and reconciliation of inventory, accounting and vendor records

Computerised software analysis of various libraries for possible duplication, identification of missing object code and for elimination of unneeded data or programme files — and reflect on configuration recordings

J **Identifying:**

Weaknesses in management and staff awareness and understanding of organisational policies regarding:

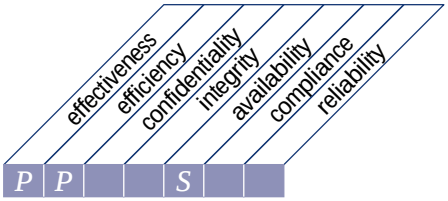
- Configuration records and changes to those records
- Placement of configuration controls in the systems development life cycle
- Integration of configuration, accounting, and vendor records
- Non-use of unauthorised software on personal computers

Inadequacy of possible improvements in effectiveness and efficiency of the baseline configuration creation and maintenance function

Deficiencies in vendor changes being reflected in configuration records, records security or changes to records by vendors being appropriately reflected

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing problems and incidents

that satisfies the business requirement

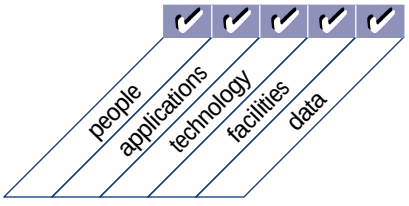
to ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence

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



MANAGE PROBLEMS AND INCIDENTS

CONTROL OBJECTIVES	
1	Problem Management System
2	Problem Escalation
3	Problem Tracking and Audit Trail
4	Emergency and Temporary Access Authorisations
5	Emergency Processing Priorities

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT operations support staff
IT help desk support staff
IT systems support staff
IT applications support staff
Selected users of IT resources

J **Obtaining:**

Summarisation of problem management facilities and positions fulfilling the problem management function
IT policies and procedures relating to problem management, including recognition, logging, resolution, escalation, tracking and reporting processes
List of problems reported during representative period, including date of occurrence, date escalated (if applicable), date of resolution and time frame to resolve
List of critical applications that immediately escalate for senior management attention for a priority resolution or are reportable as critical problems
Understanding of any problem management application, and in particular method for ensuring all problems are captured, resolved and reported upon as required

Evaluating the controls by:

J **Considering whether:**

There is a problem management process that ensures all operational events which are not part of standard operations are recorded, analysed and resolved in a timely manner, and incident reports are generated for significant problems
Problem management procedures exist for:
- defining and implementing a problem management system
- recording, analysing, resolving in a timely manner all non-standard events
- establishing incident reports for critical events and reporting to users
- identifying problem types and prioritisation methodology allowing for varying resolution efforts based on risk
- defining logical and physical control of problem management information

Considering whether, *continued*

- distributing outputs on a "need to know" basis
- tracking of problem trends to maximise resources, reduce turnaround
- collecting accurate, current, consistent and usable data inputs to reporting
- notifying appropriate level of management for escalation and awareness
- determining if management periodically evaluates the problem management process for increased effectiveness and efficiency
- sufficiency of audit trail for system problems
- integration with change, availability, configuration management systems and personnel

Emergency processing priorities exist, are documented and require approval by appropriate program and IT management

There are emergency and temporary access authorisation procedures which require:

- documentation of access on standard forms and maintained on file
- approval by appropriate managers
- secure communication to the security function
- automatic access termination, after a predetermined period of time

Assessing the compliance by:

J **Testing that:**

A selected sample of process outputs comply with stated procedures relating to:

- non-critical problems
- high priority/critical problems requiring escalation
- report requirements, content, accuracy, distribution and actions taken
- user satisfaction with the problem management process and results

Via interview, the awareness and understanding of problem management process

Substantiating the risk of control objectives not being met by:

J **Performing:**

For a selection of problems reported, tests to ensure problem management procedures were followed for all non-standard activities, including:

- recording of all non-standard events by process
- tracking and resolution of each and all events
- appropriate level of response based on priority of event
- escalation of problem for critical events
- appropriate reporting within IT function and user groups
- regular review of process effectiveness and efficiency for improvements
- performance improvement programme expectations and success

J **Identifying:**

Occurrences of problems not controlled formally by problem management process

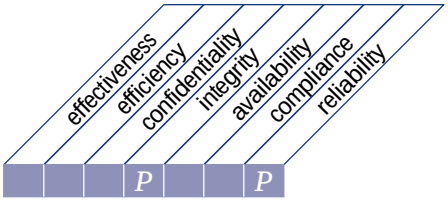
Occurrences of problems recognised but not resolved per problem management process

Variances between actual and formal process events with respect to problem resolution

User shortcomings of problem management process, communication of problem and resolution—for possible improvement opportunities

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing data

that satisfies the business requirement

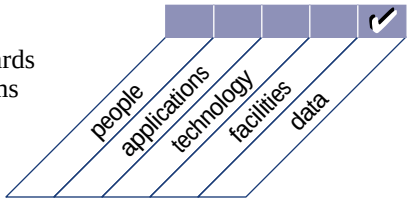
to ensure that data remains complete, accurate and valid during its input, update and storage

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



MANAGE DATA

CONTROL OBJECTIVES	
1	Data Preparation Procedures
2	Source Document Authorisation Procedures
3	Source Document Data Collection
4	Source Document Error Handling
5	Source Document Retention
6	Data Input Authorisation Procedures
7	Accuracy, Completeness and Authorisation Checks
8	Data Input Error Handling
9	Data Processing Integrity
10	Data Processing Validation and Editing
11	Data Processing Error Handling
12	Output Handling and Retention
13	Output Distribution
14	Output Balancing and Reconciliation
15	Output Review and Error Handling
16	Security Provision for Output Reports
17	Protection of Sensitive Information During Transmission and Transport
18	Protection of Disposed Sensitive Information
19	Storage Management
20	Retention Periods and Storage Terms
21	Media Library Management System
22	Media Library Management Responsibilities
23	Back-up and Restoration
24	Back-up Jobs
25	Back-up Storage
26	Archiving
27	Protection of Sensitive Messages
28	Authentication and Integrity
29	Electronic Transaction Integrity
30	Continued Integrity of Stored Data

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT operations management
IT data base administration management
IT applications development management

Interviewing, *continued*

IT human resources/training management

IT systems support management

Back-up site security and administration management

Various user management for mission critical applications

J **Obtaining:**

Organisational policies and procedures relating to the nature and management of data including:

- flow of data within the IT function and to/from users of data
- points in the organisation where data is originated, batched, edited, entered, processed, output, reviewed, corrected and resubmitted, and distributed to users
- source document authorisation process
- data collection, tracking and transmission processes
- procedures for ensuring completeness, accuracy, accounting and transmitting of completed source documents for entry
- procedures used to identify and correct errors during data origination
- procedures for ensuring integrity, confidentiality and non-repudiation of sensitive messages transmitted over the Internet or any other public network
- methods used by the organisation to retain source documents (archiving, imaging, etc.), what documents should be retained, legal and regulatory retention requirements, etc.
- interfacing systems providing and using data of the IT function
- vendor contracts to perform data management tasks
- management reports used to monitor activities and inventories

List of all major applications and user documentation relating to:

- modules performing input accuracy, completeness and authorisation checks
- functions performing data entry for each application
- functions performing data entry error correction routines
- methods used to prevent (manual and programme means), detect, and correct errors
- controlling the processing integrity of submitted data
- data processing validation editing and authentication as close to the point of origination as possible
- handling and retention of output created by applications
- outputs, distribution of output and interfacing systems using output
- procedures for balancing outputs to control totals and reconciliation of variances
- reviewing accuracy of output reports and the information
- securing distributed processing output reports
- securing data transmitted and between applications
- disposing of sensitive input, process and output documentation
- third-party vendor control procedures over preparation, input, processing and output

Policies and procedures relating to any central data base repository of the organisation, including:

- data base organisation and data dictionary
- data base maintenance and security procedures
- data base ownership determination and maintenance
- change control procedures over data base design and content
- management reporting and audit trails defining data base activities

Policies and procedures relating to the media library and off-site storage of data, including:

- administering the media library and library management system
- requiring external identification of all media
- requiring current inventory of all contents and process to control activity
- housekeeping procedures to protect data resources
- reconciliation procedures between actual and data records
- data meeting recycling and rotating of data media
- past test data of inventory and recovery tests performed
- media and off-site personnel's role in continuity plans

Evaluating the controls by:

J **Considering whether:**

For data preparation:

- data preparation procedures ensure completeness, accuracy and validity
- authorisation procedures for all source documents exist
- separation of duties between origination, approval and conversion of source documents into data is occurring
- authorised data remains complete, accurate and valid through source document origination
- data is transmitted in a timely manner
- periodic review of source documents for proper completion and approvals occurs
- appropriate handling of erroneous source documents
- adequate control over sensitive information exists on source documents for protection from compromise
- procedures ensure completeness and accuracy of source documents, proper accounting for source documents and timely conversion
- source document retention is sufficiently long to allow reconstruction in event of loss, availability for review and audit, litigation inquiries or regulatory requirements

For data input:

- appropriate source document routing for approval prior to entry
- proper separation of duties among submission, approval, authorisation and data entry functions
- unique terminal or station codes and secure operator identification
- usage, maintenance and control of station codes and operator IDs
- audit trail to identify source of input
- routine verification or edit checks of inputted data as close to the point of origination as possible
- appropriate handling of erroneously input data
- clearly assign responsibility for enforcing proper authorisation over data

For data processing:

Programmes contain error prevention, detection, correction routines:

- programmes must test input for errors (i.e., validation and editing)
- programmes must validate all transactions against a master list of same
- programmes must disallow override of error conditions

Considering whether, *continued*

Error handling procedures include:

- correction and resubmission of errors must be approved
- individual responsibility for suspense files is defined
- suspense files generate reports for non-resolved errors
- suspense file prioritisation scheme is available based on age and type

Logs of programmes executed and transactions processed/rejected for audit trail exist

A control group for monitoring entry activity and investigating non-standard events, along with balancing of record counts and control totals for all data processed

That all fields are edited appropriately, even if one field has an error

That tables used in validation are reviewed on a frequent basis

Written procedures exist for correcting and resubmitting data in error including a non-disruptive solution to reprocessing

Resubmitted transactions are processed exactly as originally processed

Responsibility for error correction resides with original submitting function

Artificial Intelligence systems are placed in an interactive control framework with human operators to ensure that vital decisions are approved

For output, interfacing, and distribution:

Access to output is restricted physically and logically to authorised people

Ongoing review of need for outputs is occurring

Output is routinely balanced to relevant control totals

Audit trails exist to facilitate the tracing of transaction processing and the reconciliation of disrupted data

Output report accuracy is reviewed and errors contained in output is controlled by cognisant personnel

Clear definition of security issues during output, interfacing and distribution exist

Communication of security breaches during any phase is communicated to management, acted upon and reflected in new procedures as appropriate

Process and responsibility of output disposal is clearly defined

Destruction is witnessed of materials used but not needed after processing

All input and output media is stored in off-site location in event of later need

Information marked as deleted is changed in such a way that it can no longer be retrieved

For media library:

Contents of media library are systematically inventoried

Discrepancies disclosed by the inventory are remedied in a timely manner

Measures are taken to maintain the integrity of magnetic media stored in the library

Housekeeping procedures exist to protect media library contents

Responsibilities for media library management have been assigned to specific members of IT staff

Media back-ups and restoration strategy exists

Media back-ups are taken in accordance with the defined back-up strategy and usability of back-ups is regularly verified

Media back-ups are securely stored and storage sites periodically reviewed regarding physical access security and security of data files and other items

Retention periods and storage terms are defined for documents, data, programmes, reports and messages (incoming and outgoing) as well as the data (keys, certificates) used for their encryption and authentication

In addition to the storage of paper source documents, telephone conversations are recorded and retained — if not in conflict with local privacy laws — for transactions or other activities that are part of the business activities traditionally conducted over telephones

Adequate procedures are in place regarding the archival of information (data and programmes) in line with legal and business requirements and enforcing accountability and reproducibility

For information authentication and integrity:

The integrity of the data files is checked periodically

Requests received from outside the organisation, via telephone or VoiceMail, are verified by callback or other means of authentication

A prearranged method is used for independent verification of the authenticity of source and contents of transaction requests received via fax or image system

Electronic signature or certification is used to verify the integrity and authenticity of incoming electronic documents

Assessing the compliance by:

J **Testing that:**

Data Preparation:

For a selected sample of source documents consistency is evident with respect to stated procedures relating to authorisation, approval, accuracy, completeness and receipt by data entry and data entry is timely

Source, input and conversion staff are aware and understand data preparation control requirements

Data Input:

Submit test data (both good and error transaction types) to ensure accuracy, completeness and authorisation checks are performed

For selected transactions compare master files before and after input

Error handling retention, resolution, and appropriate review integrity exists

Error handling procedures and actions comply with established policies and controls

Data Processing:

Run-to-run control totals and master file update controls are effectively used

Submit test data (both good and error transaction types) to ensure that data processing validation, authentication and editing is performed as close to the point of origination as possible

Error handling process is performed in compliance with established procedures and controls

Error handling retention, resolution and appropriate review integrity exist and are functioning appropriately

Error handling procedures and actions comply with established procedures and controls

Data Output, Interfacing and Distribution:

Output is routinely balanced to the relevant control totals

Audit trails are provided to facilitate the tracing of transaction processing and the reconciliation of disrupted data

Output reports are reviewed for accuracy by the provider and relevant users

Error handling retention, resolution and appropriate review integrity exists and are functioning appropriately

Error handling procedures and actions comply with established policies and controls

Output reports are secured awaiting distribution, as well as those already distributed to users in compliance with established procedures and controls

Testing that, *continued*

Adequate protection exists over sensitive information during transmission and transport against unauthorised access and modification

Disposed sensitive information procedures and actions comply with established policies and controls

Media Library:

Contents of the media library are inventoried systematically, any discrepancies disclosed are remedied in a timely manner and measures are taken to maintain the integrity of media stored in the library

Housekeeping procedures designed to protect media library contents exist and are functioning appropriately

Responsibilities for media library management are appropriately assigned

Media library is independent from preparation, input, processing and output function

Media back-ups and restoration strategy is appropriate

Media back-ups are appropriately occurring in accordance with the defined back-up strategy

Media storage sites are physically secure and inventory current

Data storage considers retrieval requirements and cost effectiveness

Retention periods and storage terms are appropriate for documents, data, programmes and reports

For information authentication and integrity:

Adequate protections ensure integrity, confidentiality and non-repudiation of sensitive messages transmitted over the Internet or any other public network

The risk of misaddressing messages (by letter, fax or e-mail) is mitigated by appropriate procedures

Controls that are normally applied to a specific transaction or process, such as faxing or automatic telephone message answering, also apply to computer systems that support transaction or process (e.g., fax software on a personal computer)

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of data management against similar organisations or appropriate international standards/recognised industry best practices

For a selection of transactions confirm proper processing during:

- data preparation
- input processing
- data processing
- output, distribution or integration
- error handling at all phases of processing
- integrity of data throughout error handling at all phases of processing
- retention and destruction

Tests specifically for the following:

- completeness, accuracy and validity during each phase of processing
- appropriate approvals and authorisation
- existence of preventive, detective and corrective controls — within processing or via control group manual/procedural functions
- retention of source documents for later required review — consistency with retention requirements
- retrieve a selection of source documents and transaction media to confirm existence and accuracy
- analyse audit trail availability: exists, source/operator identifiable and any interfacing systems have equal levels of control over transactions

- editing features of input and processing programmes including, but not limited to:
  - Blanks in required fields
  - Transactions code validation
  - Negative amounts
  - All other appropriate conditions
- sufficiency of validation tests internal to processing
- suspense files with defective transactions include the following controls:
  - Immediate identification of operator making error and notice of error
  - All error transactions are moved to these suspense files
  - Record is maintained until transaction is resolved and removed
  - Transactions show error code, date and time of entry and operator/machine
  - Suspense files create follow up reports for management review, trend analysis and remedial training
- separation of originating, entry, processing, verifying, and distributing functions

For a selection of output transactions:

- review a sample of transactions processed listings for completeness and accuracy
- review a sample of output reports for accuracy and completeness
- review output retention schedules for adequacy and compliance to procedures
- confirm actual distribution of a sample of outputs were distributed accurately
- confirm integrated processing by confirming output of one and input of other system transaction processing logs
- review balancing procedures for all input, processing output and other system use transactions
- confirm that only approved personnel have access to sensitive reports
- confirm destruction or relocation to off-site storage for all data media per retention policies and procedures
- confirm actual retention periods against retention procedures
- witness actual delivery or transmission of sensitive output and compliance to processing, distribution and security procedures
- confirm back-up creation and integrity in association with normal processing as well as for requirements of continuity plan

For the media library:

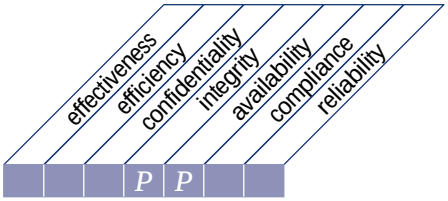
- review user access to sensitive utilities; determine that access is appropriate
- select sample of media to be destroyed and observe entire process; verify compliance with approved procedures
- determine adequacy of controls for data at off-site storage and while data is in transit
- obtain results of most recent media library inventory; confirm accuracy
- confirm record keeping processors are sufficient to access needed media
- review controls for restricting bypass of internal and external labelling rules
- test external and internal control compliance via review of selected media
- review back-up creation procedures to ensure sufficient data in event of disaster
- confirm inspections of media library per scheduled requirements

J **Identifying:**

- when production files accessed directly by operators, that a “before” and “after” image of files is not created and maintained
- sensitive input and output forms (i.e., check stock, stock certificates) are not protected
- logs are not kept for batch and control totals for all phases of processing
- output reports are not useful to users: data is not relevant and useful, report not needed, distribution is not appropriate, format and frequency not appropriate and online access to reports is not controlled
- transmitted data does not have additional controls, including:
  - Limited transmission send/receive access
  - Proper authorisation and identification for sender and receiver
  - Secure means for transmission
  - Encryption of transmitted data and appropriate de-encryption algorithms
  - Transmission integrity tests for completeness
  - Procedures for retransmission
- vendor contracts missing controls such as destruction services
- off-site deficiencies regarding environmental hazards such as fire, water, electrical and unauthorised access

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing facilities

that satisfies the business requirement

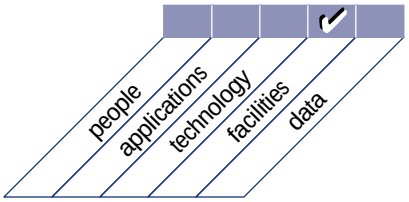
to provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards

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



MANAGE FACILITIES

CONTROL OBJECTIVES	
1	Physical Security
2	Low Profile of the IT Site
3	Visitor Escort
4	Personnel Health and Safety
5	Protection Against Environmental Factors
6	Uninterruptible Power Supply

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Facility manager
Security officer
Risk manager
IT operations manager
IT security manager

J **Obtaining:**

Organisational policies and procedures relating to facility management, layout, security, safety, fixed asset inventory and capital acquisition/leasing

IT policies and procedures relating to layout of facilities, physical and logical security, safety, access, maintenance, signage, visitors, health, safety, and environmental requirements, entrance and exit mechanisms, security reporting, security and maintenance contracts, inventory of equipment, surveillance procedures and regulatory requirements

List of individuals who have access to the facility and floor layout of facility

Lists of performance, capacity, and service level agreements regarding performance expectations of IT resources (equipment and facilities), including industry standards

Copy of continuity planning document

Evaluating the controls by:

J **Considering whether:**

Facility location is not obvious externally, is in least accessible area or organisation and access is limited to least number of people

Logical and physical access procedures are sufficient, including security access profiles for employees, vendors, equipment and facility maintenance staff

"Key" and "card reader" management procedures and practices are adequate, including ongoing update and review on a least-access-needed basis

Considering whether, *continued*

Access and authorisation policies on entering/leaving, escort, registration, temporary required passes, surveillance cameras as appropriate to all and especially sensitive areas are adequate

Periodic and ongoing review of access profiles, including managerial review is occurring

Revocation, response and escalation process occurs in event of security breach

Security and access control measures include portable and/or off-site used information devices

Signage exists with respect to not identifying sensitive areas and being consistent with insurance, local building code and regulatory requirements

Review occurs of visitor registration, pass assignment, escort, person responsible for visitor, log book to ensure both check in and out occurs and receptionist's understanding of security procedures

Review of fire, weather, electrical warning and alarm procedures and expected response scenarios for various levels of environmental emergencies is occurring

Review occurs of air conditioning, ventilation, humidity control procedures and expected response scenarios for various loss or unanticipated extremes

Review exists of security breach alarm process, including:

- definition of alarm priority (i.e., wind blowing door open to armed bomber on premises)
- response scenarios to each priority alarm
- responsibilities of in-house personnel versus local or vendor security personnel
- interaction with local authorities
- review of most recent alarm drill

Organisation is responsible for physical access within the IT function that includes:

- development, maintenance and ongoing review of security polices and procedures
- establishes relationships with security-oriented vendors
- liaisons with facility management on technology issues related to security
- coordinates security awareness and training for the organisation
- coordinates activities affecting logical access control via centralised application and operating system software
- provides security awareness and training not only within the IT function, but for users of services

Vending machine and janitorial services practices for screening staff in organisation's facility occur

Security service contracts content, updating and negotiations occur

Penetration test procedures and results

- coordinates physical penetration test scenarios
- coordinates physical penetration test, with vendors and local authorities

Health, safety and environmental regulations are being complied with

Physical security is addressed in the continuity plan and ensures similar physical security over supplier facilities

Specific existence of alternative infrastructure items necessary to implement security:

- uninterruptible power source (UPS)
- alternative or rerouting of telecommunications lines
- alternative water, gas, air conditioning, humidity resources

Assessing the compliance by:

J **Testing that:**

Staff is aware and understands need for security and safety controls

Wiring closets are physically secure with only authorised access possible and the cabling is routed as much as possible underground or through secured conduits

Signage identifies emergency routes and what to do in an emergency or security breach

Signage or telephone directories in other parts of facility do not identify sensitive locations

Visitor's log is appropriately following security procedures

Identification procedures required for any access in or out exist—via observation

Doors, windows, elevators, docks, air vents and ducts and other methods of access are identified

Computer room is separate, locked and accessed only by operations personnel and maintenance people on an as-needed basis

Facilities staff rotates shifts and takes appropriate holidays and vacation

Maintenance procedures and records for timely performance of work exist

Variances from policies and procedures on 2nd and 3rd shift operations are reported

Physical plans are updated as configuration, environment and facility changes

Environmental and safety monitoring equipment and records—below, on, above, around flooring—are maintained

Hazardous commodities are not stored

Access control audit trails exist on security software or key management reports

Any past emergencies or documentation of same are tracked

Staff with access are actual employees

Access key management completeness checks are occurring

Physical guard education and awareness is the case

Insurance coverage and expertise for expenses associated with a security event, lost business and expenses to recover facility exist

Process for implementing access change to keys and logical process controls is ongoing and known

Environment meets regulated or statutory requirements

Alarm maintenance logs cannot be inappropriately changed

Frequency of access code changes and profile review — user and facilities involvement — is documented

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of facilities management against similar organisations or appropriate international standards/recognised industry best practices

Comparison of physical layout with building drawings and security devices

Determination that:

- facility itself does not appear as a systems service location, nor indirectly suggest this via directions, parking lot signs, etc.
- number of doors is limited by local building/insurance codes
- location of facility is protected by sufficient physical barriers to keep vehicles and people from inappropriate access

Performing, *continued*

- traffic patterns to ensure flow does not direct people to secure areas
- video monitoring and review of tapes is sufficient
- spacing of computer equipment is appropriate for access, heat and maintenance
- sufficient equipment covers are available for water or foreign elements in emergency
- alarms work from maintenance logs and last alarm drill report was reviewed

Tests with respect to temperature, humidity, electricity — above and below raised floors; if abnormalities have occurred, what were investigation/resolution activities which resulted

Check of all locks and hinges (hinges inside room)

Walk through without a badge and determine if inquiry made regarding lack of same

Guard/receptionist coverage review when visitor escorted through facility

Security penetration tests of facilities

J **Identifying:**

Sufficiency of signage, fire extinguishers, sprinkler systems, UPS, drainage, wiring, workability and regular maintenance

For windows: ensure no resources visible externally nor “show case” windows in data centre

Security penetration tests determination

Visitor test, including registration, badge, escort, parcel inspection, release

Discrepancies in visitor log-in to visitor badges

Assessment of access profiles and history based on key management reporting including replacement of lost badges/key cards and making lost items inactive

Review of local disaster statistics

Develop disaster penetration scenarios

Vendor contracts for screening of personnel and compliance with health and safety requirements occur

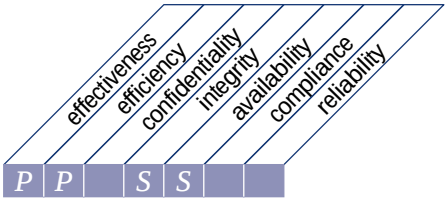
Test UPS and verify that results meet the capacity and operational requirements to sustain critical data processing activities

Tests of access information (logs, tapes, records) are reviewed by users and management for appropriateness

Tests of near-area facility entrances monitoring procedures

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

managing operations

that satisfies the business requirement

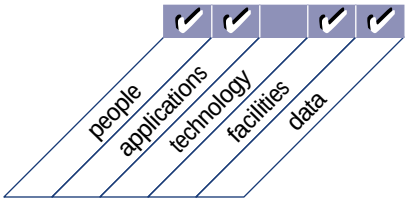
to ensure that important IT support functions are performed regularly and in an orderly fashion

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



MANAGE OPERATIONS

CONTROL OBJECTIVES	
1	Processing Operations Procedures and Instructions Manual
2	Start-up Process and Other Operations Documentation
3	Job Scheduling
4	Departures from Standard Job Schedules
5	Processing Continuity
6	Operations Logs
7	Safeguard Special Forms and Output Devices
8	Remote Operations

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

IT operations management
IT continuity planning management
IT senior management
Selected users of IT resources
Selected vendors providing software or hardware contract services or products

J **Obtaining:**

Organisational policies and procedures relating to operations management and role of information systems in accomplishing business objectives

IT policies and procedures relating to operational role, performance expectations, job scheduling, service level agreements, operator instructions, staff rotation, continuity planning and remote facility operations

Operational instructions for general function of start-up, shut down, workload scheduling, standards, service level agreements, emergency fix procedures, abnormal processing responses, console logs, physical and logical security, separation of development and production libraries and problem escalation procedures

A selected sample of operational instructions for key applications including: schedule, inputs, processing time, error messages, abnormal ending instructions, restart, problem escalation procedures, jobs before and after, and off-site files.

Evaluating the controls by:

J **Considering whether:**

There is evidence of:

- completeness of all processing performed, cold starts and restarts and recoveries
- initial programme load (IPL) and shut down procedural sufficiency
- schedule completion statistics to confirm successful completion of all requirements

Considering whether, *continued*

- physical and logical separation of source and object, test/development/production libraries and change control procedures for moving programmes among libraries
- performance statistics for operational activities, including but not limited to:
  - Hardware and peripheral capacity, utilisation and performance
  - Memory utilisation and performance
  - Telecommunications utilisation and performance
- extent that performance is matching product performance norms, internally defined performance standards and user service level agreement commitments
- operating logs are maintained, retained and reviewed on an ongoing basis
- maintenance is being performed on all equipment in a timely manner
- operators are rotating shifts, taking holidays and vacations and maintaining competencies

Assessing the compliance by:

J **Testing that:**

Operations staff members are aware and understand:

- operating procedures which they are responsible for
- performance expectations within the facility — vendor norms, organisational standards and service level agreements with users
- emergency programme fix, along with restart/recovery procedures
- operations logging requirements and management review
- problem escalation procedures
- shift change communications and inter-shift responsibilities
- turnover procedures for moving development programmes into production
- interaction with remote processing facilities and central processing facilities
- responsibility for communicating productivity improvement opportunities to management

Substantiating the risk of control objectives not being met by:

J **Performing:**

Review of operational performance statistics (equipment and personnel) to ascertain adequacy of utilisation; compare to similar organisations, vendor norms, appropriate international standards and comparable industry benchmarks/best practices

Review of a sample of limited IT operations manuals and determining whether they meet policy and procedures requirements

Examination of start-up and shut down process documentation and experience to confirm procedures are tested and updated on a regular basis

Examination of processing schedule to ensure adequacy and sufficiency of performance against schedule

J **Identifying:**

Selected users and ascertaining sufficiency of operational performance relating to ongoing activities and service level agreements

A sample of abnormal ends (ABENDS) for jobs and determining resolution of problems which occurred

Operator training, shift rotation, holiday/vacation experience

A sample of console logs for accuracy, trends in performance and managerial review for problem resolution—evaluate problem escalation if applicable

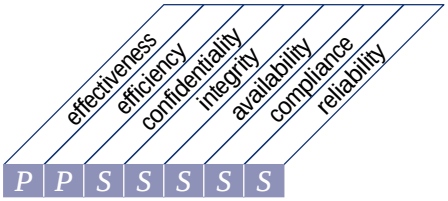
Users to determine service level agreement commitment satisfaction

Preventive maintenance procedures being completed on all equipment per vendor suggestions

This page intentionally left blank

MONITORING

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

monitoring the processes

that satisfies the business requirement

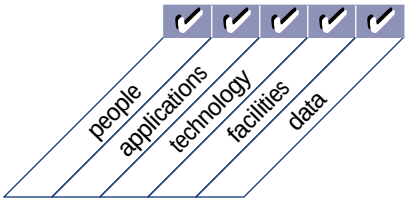
to ensure the achievement of the performance objectives set for the IT processes

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



MONITOR THE PROCESSES

CONTROL OBJECTIVES	
1	Collecting Monitoring Data
2	Assessing Performance
3	Assessing Customer Satisfaction
4	Management Reporting

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief executive officer
Chief information officer
Senior internal audit officer
IT senior and quality control management
External audit senior manager
Selected users of IT resources
Audit committee members, if applicable

J **Obtaining**

Organisation-wide policies and procedures relating to planning, managing, monitoring and reporting on performance

IT policies and procedures relating to monitoring and reporting on performance, establishing performance improvement initiatives and frequency of review

Reports of IT activities including, but not limited to: internal reports, internal audit reports, external audit reports, user reports, user satisfaction surveys, system development plans and status reports, audit committee minutes and any other assessments of the organisation's use of IT resources

Information services function planning documents with deliverables for each resource group and actual performance against those plans

Evaluating the controls by:

J **Considering whether:**

Data identified for monitoring IT resources is appropriate

Key performance indicators and/or critical success factors are used to measure IT performance against target levels

Internal reporting of IT resource utilisation (people, facilities, applications, technology, and data) is adequate

Managerial review of IT resource performance reporting exists

Considering whether, *continued*

Monitoring controls exist to provide reliable and useful feedback in a timely manner

Response of organisation to quality control, internal audit and external audit improvement recommendations is appropriate

Target performance improvement initiatives and results exist

Organisational performance against stated goals of all groups within the organisation is occurring

User satisfaction analysis exists

Reliability and usability of performance reporting for non-users such as external auditor, audit committee and senior management of the whole organisation is sufficient

Timeliness of reporting allows for rapid response to identified performance shortcomings or exceptions

Reporting against policies and procedures established for the performance of activities; (i.e., performance reporting) is sufficient

Assessing the compliance by:

J **Testing that:**

Data performance monitoring reports exist

Managerial review of performance monitoring reports and corrective action initiatives is occurring

Employees are aware and understand policies and procedures relating to performance monitoring

Quality and content of internal reporting relates to:

- collection of performance monitoring data
- analysis of performance monitoring data
- analysis of resource performance data
- management actions on performance issues
- analysis of user satisfaction surveys

Senior management is satisfied with reporting on performance monitoring

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of performance monitoring against similar organisations or appropriate international standards/recognised industry best practices

Review of relevancy of data within processes being monitored

Actual to planned performance review in all IT areas

Actual to anticipated user satisfaction of all IT areas

Analysis of extent of accomplishment of performance goals improvement initiatives

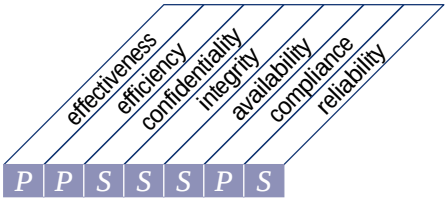
Analysis of level of implementation of managerial recommendations

J **Identifying:**

Competence, authority and independence of monitoring staff within the information systems organisation

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

assessing internal control adequacy

that satisfies the business requirement

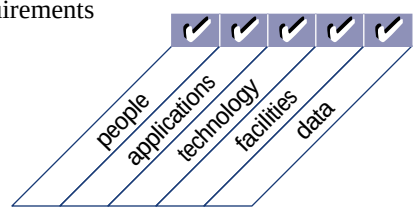
to ensure the achievement of the internal control objectives set for the IT processes

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



ASSESS INTERNAL CONTROL ADEQUACY

CONTROL OBJECTIVES	
1	Internal Control Monitoring
2	Timely Operation of Internal Controls
3	Internal Control Level Reporting
4	Operational Security and Internal Control Assurance

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief executive officer
Chief information officer
Senior internal audit officer
IT senior and quality control management
External audit senior manager
Selected users of IT resources
Audit committee members, if applicable

J **Obtaining**

Organisation-wide policies and procedures relating to planning, managing, monitoring and reporting upon internal controls
IT policies and procedures relating to monitoring and reporting on internal controls and frequency of review
Reports of IT activities including, but not limited to: internal reports, internal audit reports, external audit reports, user reports, system development plans and status reports, audit committee minutes and any other assessments of IT internal controls
Specific IT policies and procedures relating to operational security and internal control assurance

Evaluating the controls by:

J **Considering whether:**

Data identified for monitoring IT internal controls is appropriate
Internal reporting of IT internal control data is adequate
Managerial review of IT internal controls exists
Monitoring controls exist to provide reliable and useful feedback in a timely manner
Response of organisation to quality control, internal audit and external audit improvement recommendations is appropriate
Target internal control improvement initiatives and results exist

Considering whether, *continued*

Organisational performance against stated goals of internal controls is occurring

Information regarding internal control errors, inconsistencies and exceptions is systematically kept and reported to management

Reliability and usability of internal control reporting for non-users such as external auditor, audit committee and senior management of the whole organisation is sufficient

Timeliness of reporting allows for rapid response to identified internal control shortcomings or exceptions

Internal control reporting against policies and procedures established for the performance of activities (i.e., internal control reporting) is sufficient

Assessing the compliance by:

J **Testing that:**

Internal control monitoring reports exist

Managerial review of internal control reports and corrective action initiatives is occurring

Employees are aware and understand policies and procedures relating to internal control monitoring

Quality and content of internal reporting relates to:

- collection of internal control monitoring data
- internal control compliance performance
- management actions on internal control issues
- operational security and internal control assurance

Senior management is satisfied with reporting on security and internal control monitoring

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of internal control assessment against similar organisations or appropriate international standards/recognised industry best practices

Review of relevancy of data within processes being monitored and in internal controls reporting

Internal controls review framework of the overall organisation and IT specifically to ensure sufficiency of coverage and various levels of details for process owners

Actual to planned internal control review in all IT areas

Analysis of extent of accomplishment of internal control goals improvement initiatives

Review of audit committee's satisfaction with reporting on internal controls

Analysis of level of implementation of managerial recommendations

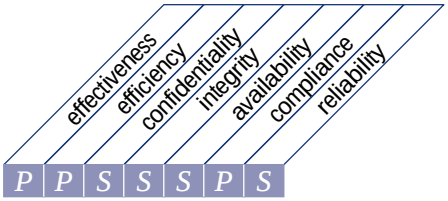
J **Identifying:**

Additional areas for possible internal control reporting consistent with IT audit, management, external auditors and regulatory concerns

Competence, authority and independence of internal control review staff within the information systems organisation

This page intentionally left blank

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

obtaining independent assurance

that satisfies the business requirement

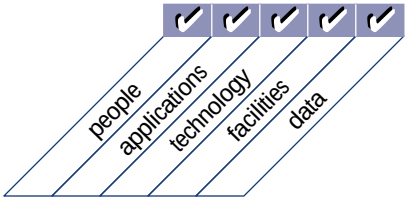
to increase confidence and trust among the organisation, customers, and third-party providers

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



OBTAIN INDEPENDENT ASSURANCE

CONTROL OBJECTIVES	
1	Independent Security and Internal Control Certification/Accreditation of IT Services
2	Independent Security and Internal Control Certification/Accreditation of Third-Party Service Providers
3	Independent Effectiveness Evaluation of IT Services
4	Independent Effectiveness Evaluation of Third-Party Service Providers
5	Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments
6	Independent Assurance of Compliance with Laws and Regulatory Requirements and Contractual Commitments by Third-Party Service Providers
7	Competence of Independent Assurance Function
8	Proactive Audit Involvement

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief executive officer
Chief information officer
IT senior management
Senior internal audit officer
External auditor senior manager
Independent assurance senior manager

J **Obtaining:**

Organisation-wide organisation chart and policies and procedures manual
Policies and procedures relating to the independent assurance process
IT service provider contracts/service level agreements
Pertinent legal and regulatory requirements and contractual commitments
Independent assurance charters/contracts, budgets, prior reports, and performance history
Experience and continuing education records of independent assurance staff
Prior audit reports

Evaluating the controls by:

J **Considering whether:**

Independent assurance charters/contracts are appropriately established/executed to ensure adequate review coverage (e.g., certification/accreditation, effectiveness evaluation and compliance assessments)
Independent certification/accreditation is obtained prior to implementing critical new IT services

Considering whether, *continued*

Independent re-certification/re-accreditation of IT services is obtained on a routine cycle after implementation

Independent certification/accreditation is obtained prior to using IT service providers

Independent re-certification/re-accreditation is obtained on a routine cycle

Independent evaluation of the effectiveness of IT services is obtained on a routine cycle

Independent evaluation of the effectiveness of IT service providers is obtained on a routine cycle

Independent reviews of IT compliance with legal and regulatory requirements and contractual commitments is obtained on a routine cycle

Independent reviews of third-party service providers' compliance with legal and regulatory requirements and contractual commitments is obtained on a routine cycle

Independent assurance staff is competent and performing per appropriate professional standards

Professional continuing education programme assists in providing technical competence of independent assurance staff

Management proactively seeks out audit involvement prior to finalising IT service solutions

Assessing the compliance by:

J **Testing that:**

Senior management approves performance of independent assurance entity

Independent certification/accreditation prior to implementation of critical new IT services is comprehensive, complete and timely

Independent re-certification/re-accreditation of IT services is performed on a routine cycle after implementation and is comprehensive, complete and timely

Independent certification/accreditation prior to using IT service providers is comprehensive, complete and timely

Independent re-certification/re-accreditation is performed on a routine cycle and is comprehensive, complete and timely

Independent evaluation of the effectiveness of IT services is performed on a routine cycle and is comprehensive, complete and timely

Independent evaluation of the effectiveness of IT service providers is performed on a routine cycle and is comprehensive, complete and timely

Independent reviews of IT compliance with legal and regulatory requirements and contractual commitments is performed on a routine cycle and is comprehensive, complete and timely

Independent reviews of third-party service providers' compliance with legal and regulatory requirements and contractual commitments is performed on a routine cycle and is comprehensive, complete and timely

Independent assurance function reports are relevant with respect to findings, conclusions and recommendations

Independent assurance function possesses the necessary skills and knowledge to perform competent work

Proactive involvement, prior to finalising IT service solutions, is occurring

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of independent assurance entity review activities against similar organisations or appropriate international standards/recognised industry best practices

A detailed review that:

- verifies independent assurance charters/contracts against review activities performed
- determines adequacy and timeliness of certifications/accreditations
- determines adequacy and timeliness of re-certifications/re-accreditations
- determines adequacy and timeliness of effectiveness evaluations
- determines adequacy and timeliness of compliance reviews of legal and regulatory requirements and contractual commitments
- verifies the competence of independent assurance function staff
- verifies proactive audit involvement

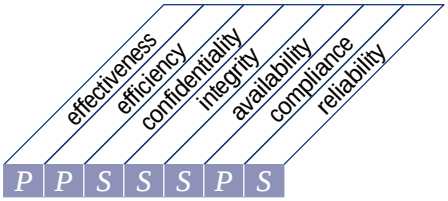
J **Identifying:**

Value-added by independent assurance review activities

Actual to planned performance against independent assurance plans and budgets

Extent and timeliness of proactive audit involvement

HIGH-LEVEL CONTROL OBJECTIVE



Control over the IT process of

providing for independent audit

that satisfies the business requirement

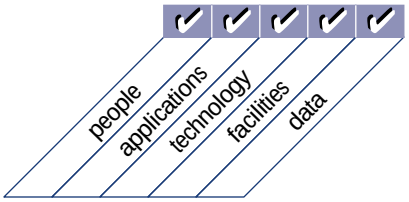
to increase confidence levels and benefit from best practice advice

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)



PROVIDE FOR INDEPENDENT AUDIT

CONTROL OBJECTIVES	
1	Audit Charter
2	Independence
3	Professional Ethics and Standards
4	Competence
5	Planning
6	Performance of Audit Work
7	Reporting
8	Follow-up Activities

BOTH HIGH-LEVEL AND DETAILED CONTROL OBJECTIVES ARE AUDITED BY:

Obtaining an understanding by:

J **Interviewing:**

Chief executive officer
Chief information officer
Senior internal audit officer
IT senior and quality control management
External auditor senior manager
Audit committee members, if applicable

J **Obtaining**

Organisation-wide organisation chart and policies and procedures manual
Organisation-wide code of conduct policy
Policies and procedures relating to the independent audit process
Audit charter, mission statement, policies, procedures and standards, prior reports and audit plans
External audit opinions, reviews and audit plans
Experience and continuing education records of internal audit staff
Audit risk assessment, budget and performance history
Minutes of audit committee meetings, if applicable

Evaluating the controls by:

J **Considering whether:**

Audit committee is appropriately established and meeting regularly, if appropriate
Internal audit organisation is appropriately established
External audits contribute to the accomplishment of the audit plan
Audit adherence to applicable professional codes of conduct is sufficient

Considering whether, *continued*

Independence of auditor is confirmed by signed conflict of interest statements

Audit plan is based on risk assessment methodology and overall sufficiency of the plan

Audits are adequately planned and supervised

Evidence is sufficient enough to support findings and conclusions

Professional continuing education programme assists in providing technical competence of auditors

Audit staff is competent and performing per professional auditing standards

An adequate reporting process of audit findings to management exists

Follow-up of all control issues is occurring in a timely manner

Audit coverage includes the full range of information systems audits (i.e., general and application controls, system development life cycle, value for money, economy, efficiency, effectiveness, proactive audit approach, etc.)

Assessing the compliance by:

J **Testing that:**

Senior management approves performance of ongoing independent audit function

Senior management attitudes are consistent with audit charter

Internal audit benchmarks against professional standards

Assignment of auditors assures independence and sufficient skills

Ongoing improvements in audit staff professional credentials is occurring

Audit report content is relevant with respect to recommendations

Follow-up reports summarising timeliness of implementation exist

Substantiating the risk of control objectives not being met by:

J **Performing:**

Benchmarking of audit function against similar organisations or appropriate international standards/recognised industry best practices

A detailed review that:

- verifies audit plan represents a cyclical and ongoing review
- audit is contributing to success of business and IT plans
- audit function evidence supports conclusions and recommendations
- audit findings are communicated and opportunities taken advantage of or risks reduced
- audit recommendations are implemented with benefit realised

J **Identifying:**

The cost/benefit of audit recommendations

Actual to planned performance against audit plan and budget

Extent of integration between external and internal audit

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

AUDIT PROCESS
(PREPARED BY THE ISACA NATIONAL CAPITAL AREA CHAPTER)

The flowcharts shown below discuss each of the steps in satisfying a single *control objective*. It outlines the objective of the step and specifies what the auditor should have achieved before moving on to the next step. Finally, a flowchart presents a diagram of the information gathering and decision making process that should occur in each step.

Because many objectives are unique, we do not suggest this template as a rigid rule. We found it useful as a guide because it presents a precise conceptual framework for each phase of audit work. A consolidated glossary of terms is presented following the template. Defined terms are presented in *italics* throughout the text.

IDENTIFICATION/DOCUMENTATION AUDIT STEP:

Objective of Step — The objective of the identification/documentation audit step is for the auditor to become familiar with the *task* covered by the *control objective* and how IS management believes they are controlling it. This includes identifying the individuals, processes and location performing that *task*, and the *stated procedures* controlling it.

Desired Outputs of Step — At the conclusion of the identification/documentation audit step the auditor should have identified, documented and verified:

- Who performs the *task* covered by the *control objective*,
- Where the *task* is performed,
- When the *task* is performed,
- On what *inputs* is the *task* performed,
- What *outputs* are expected of the *task*, and
- What are the *stated procedures* for performing the *task.*

EVALUATION AUDIT STEP:

Objective of Step — the objective of the evaluation audit step is to assess the *stated procedures* and determine if the procedures provide an effective control structure. Procedures should be evaluated against identified criteria, industry standard practices and auditor judgment. An effective control structure is cost effective and provides reasonable assurance that the *task* is performed and the *control objective* is met.

Desired Outputs of Step — At the conclusion of the evaluation audit step the auditor should have:

- Evaluated laws, regulations and organisational criteria for applicability to the procedures
- Evaluated *stated procedures* to determine if they are cost effective and provide *reasonable assurance* that the *task* is performed and the *control objective* is met.
- Evaluated any *compensating controls* used to bolster weak procedures
- Concluded whether the *stated procedures* and *compensating controls* together provide and effective control structure.
- Identified whether compliance testing is appropriate.

COMPLIANCE TESTING AUDIT STEP:

Objective of Step — The objective of the compliance testing audit step is to analyse an organisation's adherence to prescribed controls. *Actual procedures* and *compensating controls* should be compared to *stated procedures* and Document reviews and interviews should be conducted to determine if controls are properly and consistently applied. Compliance testing is only performed against procedures which have been determined to be effective.

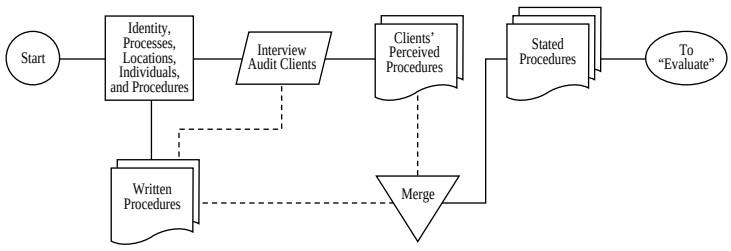


FIGURE 1. Flowchart of Identification/Documentation Audit Step

Desired Outputs of Step — At the conclusion of the compliance testing audit step, the auditor should have documented the organisation's adherence to the procedures identified above and concluded whether the *stated procedures* and *compensating controls* are being properly and consistently applied by the organisation. Based on the level of compliance, the auditor should determine the level of substantive testing needed to provide assurance that the control process is adequate.

SUBSTANTIVE TESTS AUDIT STEP:

Objective of Step — The objective of the substantive tests audit step is to conduct the necessary data testing to provide ultimate assurance or non-assurance to management about the achievement of a given *business objective*.

Desired Outputs of Step — At the conclusion of the substantive tests audit step the auditor should have performed sufficient tests on the outputs of the *task* to conclude whether a given *control objective* is being achieved. Significant substantive tests should be performed if:

- no control measures are in place
- the control measures have been evaluated as being not satisfactory, or
- compliance tests indicate that the control measures have not been properly and consistently applied.

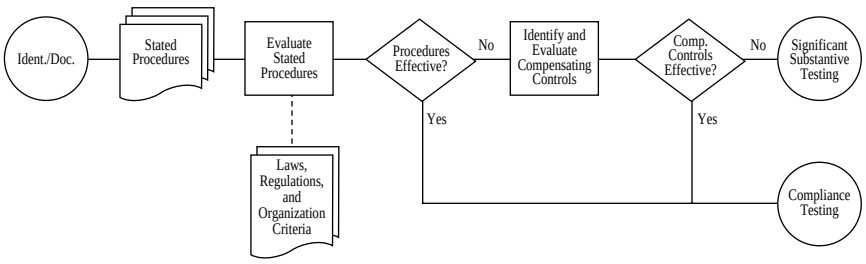


FIGURE 2. Flowchart of Evaluation Audit Step

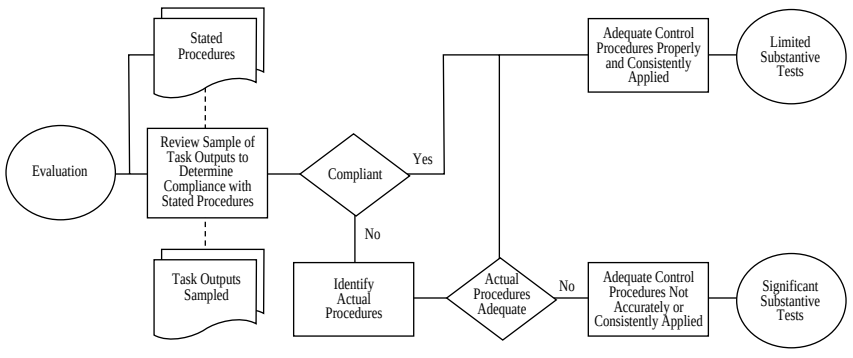


FIGURE 3. Flowchart of Compliance Testing Audit Step

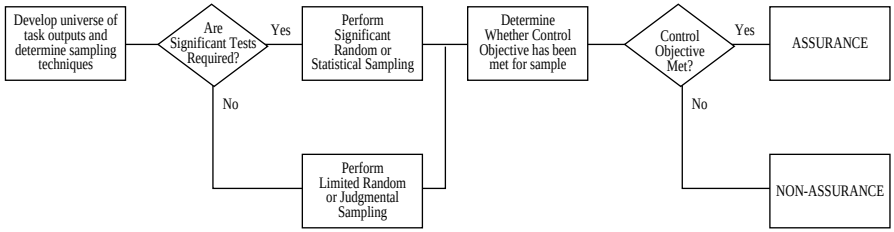


FIGURE 4. Flowchart of Substantive Tests Audit Step

GLOSSARY:

Actual Procedures — Actual procedures are the procedures being performed by the organisation to satisfy the audit objective. Actual procedures are identified during the compliance testing phase of audit.

Compensating Controls — Compensating controls are additional control steps or procedures that are not directly related to the control objective being tested, but whose presence serves to strengthen controls which do relate directly to the control objective. Compensating controls are identified during the compliance testing phase of audit work. Compensating controls are actively sought only when the effectiveness of the stated controls is questionable.

Control Objective — The desired result of any procedure established for an organisation. From an IS standpoint, the control objective is used to categorise and define the scope of audit work being performed.

Reasonable Assurance — A standard for assessing the adequacy of procedures established to meet a particular control objective. Reasonable assurance involves the application of judgment, knowledge and experience to develop an informed opinion. Reasonable assurance requires that a system of controls be effective, but not overly burdensome. The reasonable assurance standard also requires that a system of controls be cost-effective.

Stated Procedures — The controls that the organisation believes are in place and are followed to provide assurance that the control objective is being met. Stated procedures are what management believes is happening. Stated procedures include both written procedures and management identified informal procedures. Stated procedures are identified during the identification/documentation phase of the audit step and are compared to actual procedures during the compliance phase.

Task — The desired output of a series of procedures covered by a control objective. The task is whatever the control objective is designed to ensure.

Task Inputs and Outputs — Products, reports, or information required for, associated with or resulting from the performance of a task.

INDEX

INDEX

INDEX

AUDIT GUIDELINES

GENERIC AUDIT GUIDELINE

OBTAINING AN UNDERSTANDING

The audit steps to be performed to document the activities underlying the control objectives as well as to identify the stated control measures/procedures in place.

Interview appropriate management and staff to gain an understanding of:

- Business requirements and associated risks
- Organisation structure
- Roles and responsibilities
- Policies and procedures
- Laws and regulations
- Control measures in place
- Management reporting (status, performance, action items)

Document the process-related IT resources particularly affected by the process under review. Confirm the understanding of the process under review, the Key Performance Indicators (KPI) of the process, the control implications, e.g., by a process walk through.

EVALUATING THE CONTROLS

The audit steps to be performed in assessing the effectiveness of control measures in place or the degree to which the control objective is achieved. Basically deciding what, whether and how to test.

Evaluate the appropriateness of control measures for the process under review by considering identified criteria and industry standard practices, the Critical Success Factors (CSF) of the control measures and applying auditor professional judgment.

- Documented processes exist
- Appropriate deliverables exist
- Responsibility and accountability are clear and effective
- Compensating controls exist, where necessary

Conclude the degree to which the control objective is met.

ASSESSING COMPLIANCE

The audit steps to be performed to ensure that the control measures established are working as prescribed, consistently and continuously and to conclude on the appropriateness of the control environment.

Obtain direct or indirect evidence for selected items/periods to ensure that the procedures have been complied with for the period under review using both direct and indirect evidence.

Perform a limited review of the adequacy of the process deliverables.

Determine the level of substantive testing and additional work needed to provide assurance that the IT process is adequate.

SUBSTANTIATING THE RISK

The audit steps to be performed to substantiate the risk of the control objective not being met by using analytical techniques and/or consulting alternative sources. The objective is to support the opinion and to 'shock' management into action. Auditors have to be creative in finding and presenting this often sensitive and confidential information.

Document the control weaknesses, and resulting threats and vulnerabilities.

Identify and document the actual and potential impact; e.g., through root-cause analysis.

Provide comparative information, e.g., through benchmarks.