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

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

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

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

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

Management Guidelines

To ensure a successful enterprise, you must effectively manage the union between business processes and information systems. The new *Management Guidelines* is composed of maturity models, critical success factors, key goal indicators and key performance indicators. These *Management Guidelines* will help answer the questions of immediate concern to all those who have a stake in enterprise success.

Executive Summary

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

Framework

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

Audit Guidelines

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

Control Objectives

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

Implementation Tool Set

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

CD-ROM

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

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

See order form, donation information and membership application on the following pages.

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

ITGI Contribution Form

Contributor: _____

Address: _____

_____

City _____ State/Province _____

Zip/Postal Code _____ Country _____

Remitted by: _____

Phone: _____

E-mail: _____

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

Contribution amount (US $):

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

☐ $500 (Platinum) ☐ Other US $_____

☐ Check enclosed payable in US dollars to ITGI

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

Card number _____ Exp. Date _____

Name of cardholder: _____

Signature of cardholder: _____

Complete card billing address if different from address on left

_____

_____

_____

U.S. Tax ID number: 95-3080691

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

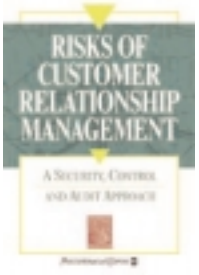
Direct any questions to Scott Artman at +1.847.253.1545, ext. 459, or *finance@isaca.org*.

Thank you for supporting CobiT!

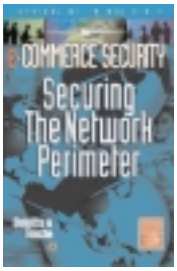
Recent ITGI Research Projects

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

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



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



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

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

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

Pricing and Order Form

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

GOVERNANCE INSTITUTE®

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

Individual components are also available for purchase:

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

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

Name _____ Date _____

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

Company Name _____

Address: ❑ Home ❑ Company _____

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

Phone Number ( ) _____ Fax Number ( ) _____

E-mail Address _____ Special Shipping Instructions or Remarks _____

_____

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

PAYMENT INFORMATION – PREPAYMENT REQUIRED

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

Account # _____ Exp. Date _____

Print Cardholder Name _____ Signature of Cardholder _____

Cardholder Billing Address if different than above _____

_____

Shipping and Handling Rates

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

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

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

PDF

Information Systems Audit and Control Association®

MEMBERSHIP APPLICATION

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

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

Name _____
FIRST MIDDLE LAST/FAMILY

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

Residence address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

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

Company name _____

Business address _____
STREET

_____
CITY STATE/PROVINCE/COUNTRY POSTAL CODE/ZIP

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

E-mail _____

Send mail to
☐ Home
☐ Business

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

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

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

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

Date of Birth _____
MONTH/DAY/YEAR

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

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

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

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

Payment due

• Association dues †	$ 120.00	(US)
• Chapter dues *(see following page)*	$ _____	(US)
• New member processing fee	$ 30.00	(US)*
PLEASE PAY THIS TOTAL	$ _____	(US)

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

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

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

All payments by credit card will be processed in US dollars

ACCT # _____

Print name of cardholder _____

Expiration date _____
MONTH/YEAR

Signature _____

Cardholder billing address if different than address provided above:

_____

_____

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

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

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

Membership dues allocated to a 1-year subscription to the *IS Control Journal* are as follows: $45 for US members, $60 for non-US members. This amount is not deductible from dues.

Make checks payable to:
Information Systems Audit and Control Association

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

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

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

Chapter Name	Chapter Number	Dues
ASIA		
Hong Kong	64	$40
Bangalore, India	138	$15
Cochin, India	176	$10
Coimbatore, India	155	$10
Hyderabad, India	164	$17
Kolkata, India	165	⁕
Madras, India (Chennai)	99	$10
Mumbai, India	145	⁕
New Delhi, India	140	$10
Pune, India	159	$17
Indonesia	123	⁕
Nagoya, Japan	118	$130
Osaka, Japan	103	$10
Tokyo, Japan	89	$120
Korea	107	$30
Lebanon	181	$35
Malaysia	93	$10
Muscat, Oman	168	$40
Karachi, Pakistan	148	$15
Manila, Philippines	136	$0
Jeddah, Saudi Arabia	163	$0
Riyadh, Saudi Arabia	154	$0
Singapore	70	$10
Sri Lanka	141	$15
Taiwan	142	$50
Bangkok, Thailand	109	$10
UAE	150	$10
CENTRAL/SOUTH AMERICA		
Buenos Aires, Argentina	124	$35
Mendoza, Argentina	144	⁕
São Paulo, Brazil	166	$25
LaPaz, Bolivia	173	$25
Santiago de Chile	135	$40
Bogotá, Colombia	126	$50
San José, Costa Rica	31	$33
Quito, Ecuador	179	$15
Mérida, Yucatán, México	101	$50
Mexico City, México	14	$65
Monterrey, México	80	$65
Panamá	94	$25
Lima, Perú	146	$15
Puerto Rico	86	$30
Montevideo, Uruguay	133	$100
Venezuela	113	$25
EUROPE/AFRICA		
Austria	157	$45
Belux (Belgium and Luxembourg)	143	$48
Croatia	170	$50
Czech Republic	153	$110
Denmark	96	⁕
Estonian	162	$10
Finland	115	$70
Paris, France	75	⁕
German	104	$80
Athens, Greece	134	$20
Budapest, Hungary	125	$60
Irish	156	$40
Tel-Aviv, Israel	40	⁕
Milano, Italy	43	$53
Rome, Italy	178	$26
Kenya	158	$40
Latvia	139	$10
Lithuania	180	$20
Netherlands	97	$50
Lagos, Nigeria	149	$20
Oslo, Norway	74	$50
Warsaw, Poland	151	$30
Moscow, Russia	167	$0
Romania	172	$50
Slovenia	137	$50
Slovensko	160	$40
South Africa	130	$35
Barcelona, Spain	171	$110
Valencia, Spain	182	$25
Sweden	88	$45
Switzerland	116	$35
Tanzania	174	$40
London, UK	60	$80
Central UK	132	$55
Northern England	111	$50
Scottish, UK	175	$45
NORTH AMERICA		
Canada		
Calgary, AB	121	$0
Edmonton, AB	131	$25
Vancouver, BC	25	$20
Victoria, BC	100	$0
Winnipeg, MB	72	$15
Nova Scotia	105	$0
Ottawa Valley, ON	32	$10
Toronto, ON	21	$25
Montreal, PQ	36	$20
Quebec City, PQ	91	$35
Islands		
Bermuda	147	$0
Trinidad & Tobago	106	$25
Midwestern United States		
Chicago, IL	02	$50
Illini (Springfield, IL)	77	$30
Central Indiana (Indianapolis)	56	$30
Michiana (South Bend, IN)	127	$25
Iowa (Des Moines)	110	$25
Kentuckiana (Louisville, KY)	37	$30
Detroit, MI	08	$35
Western Michigan (Grand Rapids)	38	$25
Minnesota (Minneapolis)	07	$30
Omaha, NE	23	$30
Central Ohio (Columbus)	27	$25
Greater Cincinnati, OH	03	$20
Northeast Ohio (Cleveland)	26	$30
Kettle Moraine, WI (Milwaukee)	57	$25
Quad Cities	169	$0
Northeastern United States		
Greater Hartford, CT (Southern New England)	28	$40
Central Maryland (Baltimore)	24	$25
New England (Boston, MA)	18	$30
New Jersey (Newark)	30	$40
Central New York (Syracuse)	29	$0
Hudson Valley, NY (Albany)	120	$0
New York Metropolitan	10	$50
Western New York (Buffalo)	46	$30
Harrisburg, PA	45	$25
Lehigh Valley (Allentown, PA)	122	$35
Philadelphia, PA	06	$40
Pittsburgh, PA	13	$20
National Capital Area, DC	05	$40
Southeastern United States		
North Alabama (Birmingham)	65	$30
Jacksonville, FL	58	$30
Central Florida (Orlando)	67	$30
South Florida (Miami)	33	$40
West Florida (Tampa)	41	$35
Atlanta, GA	39	$35
Charlotte, NC	51	$35
Research Triangle (Raleigh, NC)	59	$25
Piedmont/Triad (Winston-Salem, NC)	128	$30
Greenville, SC	54	$30
Memphis, TN	48	$45
Middle Tennessee (Nashville)	102	$45
Virginia (Richmond)	22	$30
Southwestern United States		
Central Arkansas (Little Rock)	82	$60
Central Mississippi (Jackson)	161	$0
Denver, CO	16	$40
Greater Kansas City, KS	87	$0
Baton Rouge, LA	85	$25
Greater New Orleans, LA	61	$20
St. Louis, MO	11	$25
New Mexico (Albuquerque)	83	$25
Central Oklahoma (OK City)	49	$30
Tulsa, OK	34	$25
Austin, TX	20	$25
Greater Houston Area, TX	09	$40
North Texas (Dallas)	12	$30
San Antonio/So. Texas	81	$25
Western United States		
Anchorage, AK	177	$20
Phoenix, AZ	53	$30
Los Angeles, CA	01	$25
Orange County, CA (Anaheim)	79	$30
Sacramento, CA	76	$20
San Francisco, CA	15	$45
San Diego, CA	19	$25
Silicon Valley, CA (Sunnyvale)	62	$25
Hawaii (Honolulu)	71	$30
Boise, ID	42	$30
Willamette Valley, OR (Portland)	50	$30
Utah (Salt Lake City)	04	$30
Mt. Rainier, WA (Olympia)	129	$20
Puget Sound, WA (Seattle)	35	$25
OCEANIA		
Adelaide, Australia	68	$0
Brisbane, Australia	44	$16
Canberra, Australia	92	$15
Melbourne, Australia	47	$25
Perth, Australia	63	$5
Sydney, Australia	17	$30
Auckland, New Zealand	84	$30
Wellington, New Zealand	73	$22
Papua New Guinea	152	$0

⁕Call chapter for information

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

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

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

Your level of purchasing authority
① ☐ Recommend products/services
② ☐ Approve purchase
③ ☐ Recommend and approve purchase

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

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

Primary reason for joining the association *(check one)*
① ☐ Discounts on association products and services
② ☐ Subscription to *IS Control Journal*
③ ☐ Professional advancement/ certification
④ ☐ Access to research, publications, and education
⑨⑨ ☐ Other_____

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

Certified Information Systems Auditor (CISA)

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

The CISA examination content areas include:

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

To earn the CISA designation, candidates are required to:

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

Certified Information Security Manager (CISM)

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

The CISM credential measures expertise in the areas of:

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

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

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

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

CISA®
CERTIFIED INFORMATION SYSTEMS AUDITOR™

CISM
CERTIFIED INFORMATION SECURITY MANAGER™

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

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

GOVERNANCE INSTITUTE™

COBIT®

3rd Edition

Management 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 fulfill 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 1-893209-12-1 (*Management 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 and Investors Group, Canada
Mark Stanley, Sun America Inc., USA

EXPERT PANEL

William Malik, Gartner Group, USA
Jayant Ahuja, PricewaterhouseCoopers, USA
Floris Ampe, PricewaterhouseCoopers, Belgium
Mauro Eidi Villola Assano, BBA Creditanstalt, Brazil
Gary Austin, U.S. General Accounting Office, USA
Efrim J. Boritz, Ph.D, University of Waterloo, Canada
Paul Bull, KPMG, USA
Peter De Koninck, S.W.I.F.T. sc, USA
Ken Devansky, PricewaterhouseCoopers, USA
John Dubiel, Gartner Group, USA
Chris Frost, PricewaterhouseCoopers, United Kingdom
Christopher Fox, PricewaterhouseCoopers, USA
Nils Kandelin, George Mason University, USA
Werner Lippuner, Ernst & Young, USA
Stuart Macgregor, South African Breweries, South Africa
Mario Micallef, National Australia Bank, Australia
Prataprai Oak, Fidelity Investments, USA
Daniel F. Ramos, SAFE Consulting Group, Argentina
Debra Reddish, PricewaterhouseCoopers, USA
Robert J. Reimer, PricewaterhouseCoopers, Canada
Gregory Robertson, Northrop Grumman, USA
Susana Sharp, U.S. House of Representatives, USA.
Craig Silverthorne, U.S. House of Representatives, USA
Gustavo A. Solis, Grupo Cynthus, Mexico
William Spernow, Gartner Group, USA
Mike Taylor, City of Dallas, USA
Elia Fernandez Torres, Grupo Cynthus, Mexico
Wim Van Grembergen Ph.D., UFSIA, Belgium
Winifred Whelan, PricewaterhouseCoopers, USA
Marc Wise, PricewaterhouseCoopers, USA
Roberta J. Witty, Gartner Group, USA

RESEARCH AND DEVELOPMENT SUPPORTED AND SPONSORED BY

PRICEWATERHOUSECOOPERS

Gartner

IBM®

SPECIAL THANKS to the National Capital Area Chapter for its contributions to the COBIT *Management Guidelines*.

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 SUMMARY

How do we get Information Technology under control such that it delivers the information the organisation needs? How do we manage the risks and secure the infrastructure we are so dependent on? As with many issues facing management, these broad strategic questions generate the following traditional questions to which we will provide answers:

- What is the issue/problem?
- What is the solution?
- What does it consist of?
- Will it work?
- How do I do it?

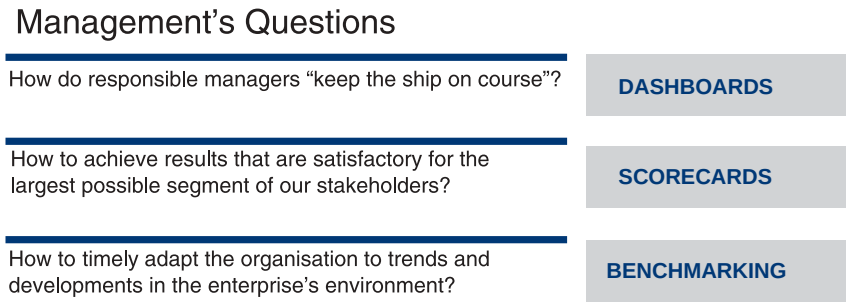
An approach to addressing these issues has been provided by the COBIT *Framework*. COBIT stands for Control Objectives for Information and related Technology and is an open standard for control over information technology, developed and promoted by the IT Governance Institute. This framework identifies 34 information technology (IT) processes, a high-level approach to control over these processes, as well as 318 detailed control objectives and audit guidelines to assess the 34 IT processes. It provides a generally applicable and accepted standard for good IT security and control practices to support management's needs in determining and monitoring the appropriate level of IT security and control for their organisations.

The IT Governance Institute has further built on this with leading-edge research, in cooperation with world-wide industry experts, analysts and academics. This has resulted in the definition of *Management Guidelines* for COBIT, which consist of Maturity Models, Critical Success Factors (CSFs), Key Goal Indicators (KGIs) and Key Performance Indicators (KPIs). This delivers a significantly improved framework responding to management's need for control and measurability of IT by providing management with tools to assess and measure their organisation's IT environment against the 34 IT processes COBIT identifies.

There are numerous changes in IT and in networking that emphasise the need to better manage IT related risks. Dependence on electronic information and IT systems is essential to support critical business processes. Successful businesses need to better manage the complex technology that is pervasive throughout their organisations in order to respond quickly and safely to business needs. 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 in achieving the organisation'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 for 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.

With the increasing interconnection and dependence on IT in our increasingly electronic global economy, overall risk management and assurance are dependent on specific management practices. In our complex environments, management is continuously searching for condensed and timely information in order to make difficult decisions on risk and control, fast and successfully. Here are some traditional questions and the management information toolkit that is used to find the response:



But dashboards need indicators, scorecards need measures and benchmarking needs a scale for comparison. Providing these for information management has been a primary objective in the development of the COBIT *Management Guidelines*.

A basic need for every organisation is to understand the status of its own IT systems and to decide what security and control they should provide. Neither aspect of this issue — understanding of and deciding on the required level of control — is straightforward. To obtain an objective view of an organisation's own level is not easy. What should be measured and how? In addition to the need for measuring where an organisation is, there is the importance of continuous improvement in the areas of IT security and control, and the need for a management toolkit to monitor this improvement. To decide on what is the right level is equally difficult. Senior managers in corporate and public organisations are frequently asked to consider a business case for expenditure to improve the control and security of the information infrastructure. Whilst few would argue that this is not a good thing, all must occasionally ask themselves:

"How far should we go, and is the cost justified by the benefit?"

The response is provided by the COBIT *Management Guidelines* that are generic and action oriented for the purpose of addressing the following types of management concerns:

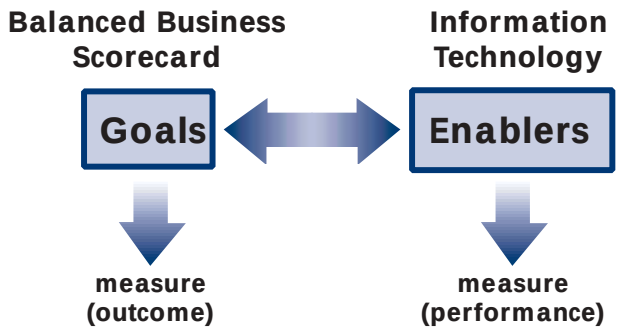
- Performance measurement – What are the indicators of good performance?
- IT control profiling – What's important? What are the Critical Success Factors for control?
- Awareness – What are the risks of not achieving our objectives?
- Benchmarking – What do others do? How do we measure and compare?

An answer to these requirements of determining and monitoring the appropriate IT security and control level is the definition of specific:

- **Benchmarking** of IT control practices (expressed as **Maturity Models**)
- **Performance Indicators** of the IT processes — for their outcome and their performance
- **Critical Success Factors** for getting these processes under control

MANAGEMENT GUIDELINES

The *Management Guidelines* are consistent with and build upon the existing COBIT *Framework*, *Control Objectives* and *Audit Guidelines*. In addition, to help focus on performance management, the principles of the Balanced Business Scorecard[1] were used. They assisted in defining Key Goal Indicators to identify and measure outcomes of processes and Key Performance Indicators to assess how well processes are performing by measuring the enablers of the process. In our information services dominated environment, IT has become the major enabler of the business. Hence, the relationship between business goals with their measures and IT with its goals and measures, is very important and can be portrayed as follows:



In "simple terms," these measures will assist management in monitoring their IT organisation by answering the following questions:

1. What is the management concern?
   Make sure that the enterprise needs are fulfilled.

2. Where is it measured?
   On the Balanced Business Scorecard as a Key Goal Indicator, representing an outcome of the business process.

3. What is the IT concern?
   That the IT processes deliver on a timely basis the right information to the enterprise, enabling the business needs to be fulfilled. This is a Critical Success Factor for the enterprise.

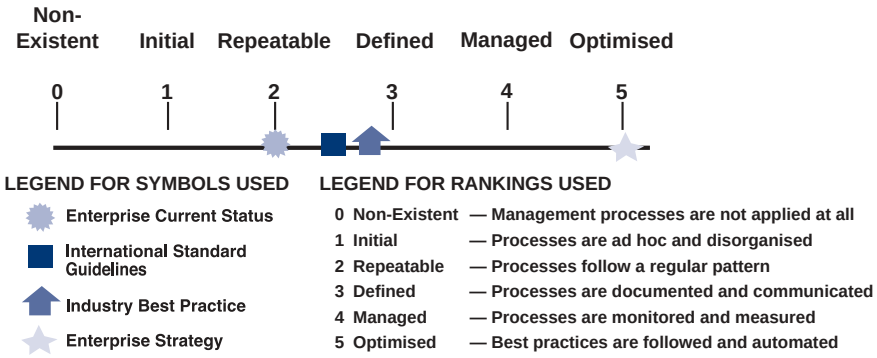
4. Where is that measured?
   On the IT balanced scorecard, as a Key Goal Indicator representing the outcome for IT, which is that information is delivered with the right criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability)

5. What else needs to be measured?
   Whether the outcome is positively influenced by a number of Critical Success Factors that need to be measured as Key Performance Indicators of how well IT is doing.

[1] "The Balanced Business Scorecard — Measurements that Drive Performance," Robert S. Kaplan and David P. Norton, Harvard Business Review, January-February 1992

MATURITY MODELS for control over IT processes consist of developing a method of scoring so that an organisation can grade itself from non-existent to optimised (from 0 to 5). This approach has been derived from the Maturity Model that the Software Engineering Institute defined for the maturity of the software development capability[2]. Against these levels, developed for each of COBIT's 34 IT processes, management can map:

- The current status of the organisation — where the organisation is today
- The current status of (best-in-class in) the industry — the comparison
- The current status of international standards — additional comparison
- The organisation's strategy for improvement — where the organisation wants to be



CRITICAL SUCCESS FACTORS (CSF) define the most important issues or actions for management to achieve control over and within its IT processes. They must be management oriented implementation guidelines and identify the most important things to do, strategically, technically, organisationally or procedurally.

KEY GOAL INDICATORS (KGI) define measures that tell management — after the fact — whether an IT process has achieved its business requirements, usually expressed in terms of information criteria:

- Availability of information needed to support the business needs
- Absence of integrity and confidentiality risks
- Cost-efficiency of processes and operations
- Confirmation of reliability, effectiveness and compliance.

KEY PERFORMANCE INDICATORS (KPI) define measures to determine how well the IT process is performing in enabling the goal to be reached; are lead indicators of whether a goal will likely be reached or not; and are good indicators of capabilities, practices and skills.

In these *Management Guidelines*, Critical Success Factors, Key Goal Indicators and Key Performance Indicators are short and focused, complementing the high-level control guidance provided by the COBIT *Framework* (see Appendix II) which states that IT enables the business by delivering the information the business needs.

[2] "Capability Maturity Model℠ for Software," Version 1.1. Technical Report CMU/SEI-93-TR-024, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, February 1993

In summary, this development has concentrated on the definition of both action-oriented and generic guidelines for management, required to maintain control over the enterprise's information and related processes and technology:

- **MATURITY MODELS** for strategic choice and benchmark comparison.
- **CSF**s for getting these processes under control
- **KGI**s for monitoring achievement of IT process goals
- **KPI**s for monitoring performance within each IT process

In an age of increasing electronic business and technology dependence, organisations will have to demonstrably attain increasing levels of security and control. Every organisation must understand its own performance and must measure its progress. Benchmarking and measuring progress against peers and the enterprise strategy is one way of achieving a competitive level of IT security and control. The COBIT *Management Guidelines* provide management with pragmatic guidance via these maturity models, practical and critical success factors and suggested performance measures, to answer the perpetual question:

"What is the right level of control for my IT such that it supports my enterprise objectives?"

FRAMEWORK

1. MATURITY MODELS

Senior managers in corporate and public organisations are frequently asked to consider a business case for resource expenditures for control over the information infrastructure. While few would argue that this is not a good thing, all must ask themselves:

"How far should we go, and is the cost justified by the benefit?"

To help answer that question, other closely related questions are often asked:

"What internationally recognised standards exist, and how are we placed in relation to them?"

"What are other people doing, and how are we placed in relation to them?"

"What is regarded as industry best practice, and how are we placed with regard to that best practice?"

"Based upon these external comparisons, can we be said to be taking 'reasonable' precautions to safeguard our information assets?"

It has usually been difficult to supply meaningful answers to these questions, because the tools required to make the necessary evaluations have not been available.

IT management is constantly on the lookout for benchmarking and self-assessment tools in response to the need to know what to do in an efficient manner. Starting from COBIT's processes and high-level control objectives, the process owner should be able to incrementally benchmark against that control objective. This provides for three needs:

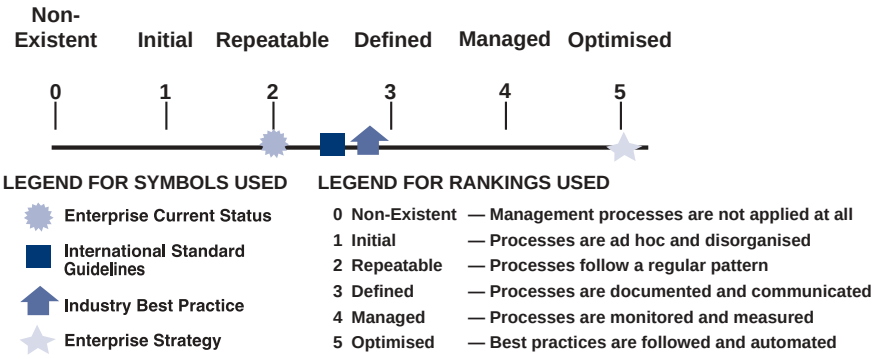
(1) a relative measure of where the organisation is
(2) a manner to efficiently decide where to go
(3) a tool for measuring progress against the goal.

The COBIT *Framework* defines 34 IT processes within an IT environment (see Appendix II). For each process there is one high-level control statement and between 3 and 30 detailed control objectives. The process owner should be able to determine the level of adherence to the control objectives either as a quick self-assessment or as a reference in conjunction with an independent review. Any of these assessments management may wish to put in context by comparison to the industry and environment they are in or in comparison to where international standards and regulations are evolving (i.e., emerging future expectations). To make the results easily usable in management briefings, where they will be presented as a means to support the business case for future plans, a graphical presentation method needs to be provided.

The approach to Maturity Models for control over IT processes consists of developing a method of scoring so that an organisation can grade itself from non-existent to optimised (from 0 to 5). This approach is based on the Maturity Model that the Software Engineering Institute defined for the maturity of the software development capability. Whatever the model, the scales should not be too granular, as that would render the system difficult to use and suggest a precision that is not justifiable.

In contrast, one should concentrate on maturity levels based on a set of conditions that can be unambiguously met. Against levels developed for each of COBIT's 34 IT processes, management can map:

- The current status of the organisation — where the organisation is today
- The current status of (best-in-class in) the industry — the comparison
- The current status of international standard guidelines — additional comparison
- The organisation's strategy for improvement — where the organisation wants to be



For each of the 34 IT processes, there is an incremental measurement scale, based on a rating of "0" through "5." The scale is associated with generic qualitative maturity model descriptions ranging from "Non Existent" to "Optimised" as follows:

Generic Maturity Model

0 Non-Existent. Complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.

1 Initial. There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are however no standardised processes but instead there are ad hoc approaches that tend to be applied on an individual or case by case basis. The overall approach to management is disorganised.

2 Repeatable. Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely.

3 Defined. Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed. It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised. Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organisations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

COBIT is a general framework aimed at IT management and as such these scales need to be practical to apply and reasonably easy to understand. However, the topics of risk and appropriate control in IT management processes are inherently subjective and imprecise and do not need the more mechanistic approach as found in the maturity models for software engineering.

The advantage of a Maturity Model approach is that it is relatively easy for management to place themselves on the scale and appreciate what is involved if they need to improve performance. The scale includes 0 to 5 because it is quite possible that no process exists at all. The 0-5 scale is based on a simple maturity scale showing how a process evolves from non-existent to optimised. Because they are management processes, increased maturity and capability is also synonymous with increased risk management and increased efficiency.

The Maturity Model is a way of measuring how well developed management processes are. How well developed they should be depends on the business needs as mentioned above. The scales are just practice examples for a given management process showing typical schemes for each level of maturity. The Information Criteria contained in the COBIT *Framework* (see Appendix II) help to make sure that we focus on the right management aspects when describing actual practice. For example, planning and organising focuses on the management goals of effectiveness and efficiency, whereas ensuring systems security will focus on the management of confidentiality and integrity.

The Maturity Model scales will help professionals explain to managers where IT management shortcomings exist and set targets for where they need to be by comparing their organisation's control practices to the best practice examples. The right maturity level will be influenced by the enterprise's business objectives and operating environment. Specifically, the level of control maturity will depend on the enterprise's dependence on IT, the technology sophistication and, most importantly, the value of its information.

A strategic reference point for an organisation to improve security and control could also consist of looking at emerging international standards and best-in-class practices. The emerging practices of today may become the expected level of performance of tomorrow and is therefore useful for planning where an organisation wants to be over time.

The Maturity Models are built up starting from the generic qualitative model (see above) to which practices and principles from the following domains are added in increasing manner through the levels:

- Understanding and awareness of risks and control issues
- Training and communication applied on the issues
- Process and practices that are implemented
- Techniques and automation to make processes more effective and efficient
- Degree of compliance to internal policy, laws and regulations
- Type and extent of expertise employed.

The following table describes this increasing application of practices over the levels for the different topics. Together with the qualitative model, it constitutes a generic maturity model applicable to most IT processes.

	Understanding and Awareness	Training and Communication	Process and Practices	Techniques and Automation	Compliance	Expertise
1	Recognition	Sporadic communication on issues	Ad hoc approach to process and practice			
2	Awareness	Communication on the overall issue and needs	Similar/common, but intuitive process emerges	Common tools are appearing	Inconsistent monitoring on isolated issues	
3	Understanding of need to act	Informal training supports individual initiatives	Practices are defined, standardised and documented; sharing of better practices begins	Tool set is standardised; currently available practices are used and enforced	Inconsistent monitoring; measurement emerges; balanced score card adopted occasionally; root cause analysis is intuitive	Involvement of IT specialists in business processes
4	Understand full requirements	Formal training supports a managed program	Process ownership and responsibilities are set; process is sound and complete; internal best practices are applied	Mature techniques are used; standard tools are enforced; limited tactical use of technology	Balanced scorecards are used in some areas; exceptions are noted; root cause analysis is standardised	Involvement of all internal domain experts
5	Advanced, forward-looking understanding	Training and communications support external best practices and use leading edge concepts	Best external practices are applied	Sophisticated techniques are deployed; extensive optimised use of technology	Balanced scorecard is globally applied; exceptions are consistently noted and acted upon; root cause analysis is always applied	Use of external experts and industry leaders for guidance

In summary, Maturity Models:

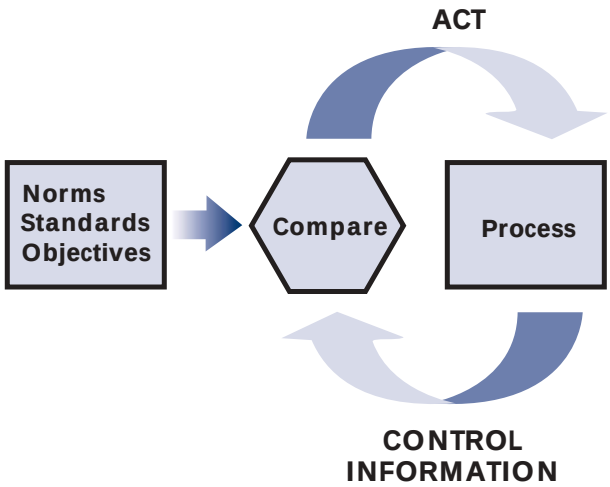
- Refer to business requirements and the enabling aspects at the different maturity levels
- Are a scale that lends itself to pragmatic comparison
- Are a scale where the difference can be made measurable in an easy manner
- Are recognisable as a “profile” of the enterprise relative to IT governance, security and control
- Help setting “As-Is” and “To-Be” positions relative to IT governance, security and control maturity
- Lend themselves to do gap analysis to determine what needs to be done to achieve a chosen level
- Avoid, where possible, discrete levels that create thresholds that are difficult to cross
- Increasingly apply critical success factors
- Are not industry specific nor always applicable, the type of business defines what is appropriate.

2. CRITICAL SUCCESS FACTORS

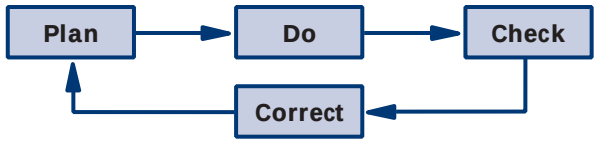
Critical Success Factors provide management with guidance for implementing control over IT and its processes. They are the most important things to do that contribute to the IT process achieving its goals. They are activities that can be of a strategic, technical, organisational, process or procedural nature. They are usually dealing with capabilities and skills and have to be short, focussed and action oriented, leveraging the resources that are of primary importance in the process under consideration.

Guidance can be obtained from the standard Control Model below. It follows the principles we all know when setting the room temperature (*standard*) for the heating system (*process*) which will constantly check (*compare*) ambient room temperature (*control information*) and will signal (*act*) the heating system to provide more heat. This model and its principles identify a number of Critical Success Factors that usually apply to all processes as they deal with what is the standard, who sets it, who controls or needs to act, etc.:

- Defined and documented processes
- Defined and documented policies
- Clear accountabilities
- Strong support/commitment of management
- Appropriate communication to concerned internal and external persons
- Consistent measurement practices.



It should also be noted that these control principles are needed at different levels, i.e., at strategic, tactical and administrative levels. There are usually four types of activities at each level that logically follow each other: planning, doing, checking and correcting. The feedback and control loop mechanisms between the levels should be considered. For example, « doing » at the strategic level feeds « planning » at the tactical, or « checking » at the administrative level is consolidated in the « checking » at the tactical layer, etc.

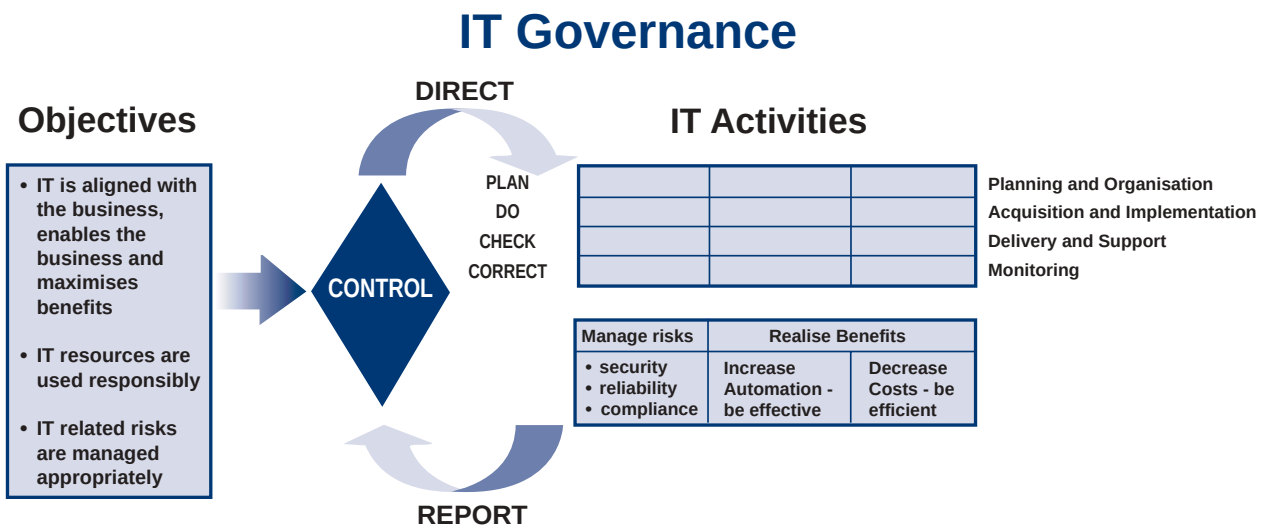


Further guidance in developing critical success factors can be obtained by examining the objectives and monitoring guidelines of the *IT Governance Framework*. IT governance is the responsibility of executives and shareholders. It is a system of control that ensures that the business objectives are achieved. This usually consists of directing the organisation's IT endeavours after reviewing its reported performance against some simple norms that call for:

- IT to be aligned with the business
- IT to enable the business and maximise its benefits
- IT resources to be used responsibly
- IT related risks to be managed appropriately.

As for the standard control model, this will usually happen at different layers, with team leaders reporting to and receiving direction from their managers, with managers reporting up to the executive and the executive to the Board of Directors. Also, reports that indicate deviation from targets will usually already include recommendations for action to be endorsed.

The illustration below presents conceptually the interaction of objectives and IT activities from an IT governance perspective. The IT activities are depicted here with the generic management activities of plan, do, check and correct. With the advent of the COBIT *Control Framework* (see Appendix II), the emerging manner to represent information technology is to use the four COBIT domains of Planning and Organisation; Acquisition and Implementation; Delivery and Support; and Monitoring.



From the standard control model and from the IT Governance Framework, a number of Critical Success Factors can be deduced that apply to most IT processes:

1. Applying to IT in general

- IT processes are defined and aligned with the IT strategy and the business goals
- The customers of the process and their expectations are known
- Processes are scalable and their resources are appropriately managed and leveraged
- The required quality of staff (training, transfer of information, morale, etc.) and availability of skills (recruit, retain, retrain) exist.
- IT performance is measured in financial terms, in relation to customer satisfaction, for process effectiveness and for future capability. IT management is rewarded based on these measures.
- A continuous quality improvement effort is applied.

2. Applying to most IT processes

- All process stakeholders (users, management, etc.) are aware of the risks, of the importance of IT and the opportunities it can offer, and provide strong commitment and support
- Goals and objectives are communicated across all disciplines and understood; it is known how processes implement and monitor objectives, and who is accountable for process performance
- People are goal-focused and have the right information on customers, on internal processes and on the consequences of their decisions
- A business culture is established, encouraging cross-divisional co-operation, teamwork and continuous process improvement
- There is integration and alignment of major processes, e.g., change, problem and configuration management
- Control practices are applied to increase efficient and optimal use of resources and improve the effectiveness of processes.

3. Applying to IT governance

- Control practices are applied to increase transparency, reduce complexity, promote learning, provide flexibility and scalability, and avoid breakdowns in internal control and oversight
- The application of practices that enable sound oversight: a control environment and culture; a code of conduct; risk assessment as a standard practice; self-assessments; formal compliance on adherence to established standards; monitoring and follow up of control deficiencies and risk
- IT governance is recognised and defined, and its activities are integrated into the enterprise governance process, giving clear direction for IT strategy, a risk management framework, a system of controls and a security policy
- IT governance focuses on major IT projects, change initiatives and quality efforts, with awareness of major IT processes, the responsibilities and the required resources and capabilities
- An audit committee is established to appoint and oversee an independent auditor, drive the IT audit plan and review the results of audits and 3rd party opinions.

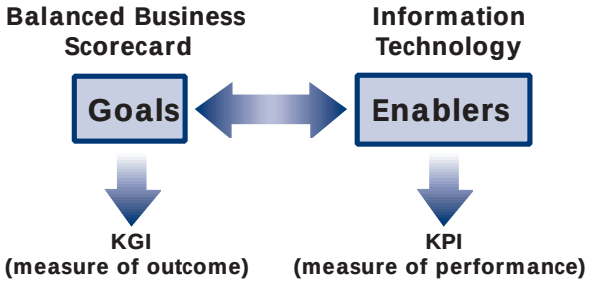
In summary, Critical Success Factors are:

- ◆ Essential enablers focused on the process or supporting environment
- ◆ A thing or a condition that is required for optimal success or an activity recommended for optimal success
- ◆ The most important things to do to increase the probability of success of the process
- ◆ Observable — usually measurable — characteristics of the organisation and process
- ◆ Either strategic, technological, organisational or procedural in nature
- ◆ Focused on obtaining, maintaining and leveraging capability and skills
- ◆ Expressed in terms of the process, not necessarily the business.

3. KEY GOAL INDICATORS

A Key Goal Indicator, representing the process goal, is a measure of "what" has to be accomplished. It is a measurable indicator of the process achieving its goals, often defined as a target to achieve.

By comparison, a Key Performance Indicator, which will be addressed in the next section, is a measure of "how well" the process is performing. This relationship is best illustrated below by a concept of the Balanced Business Scorecard, which also looks for measures of outcome of the goal and for measures of performance relative to the enablers that will make it possible for the goal to be achieved. And in this context we need to remember that IT is a major enabler of the business.

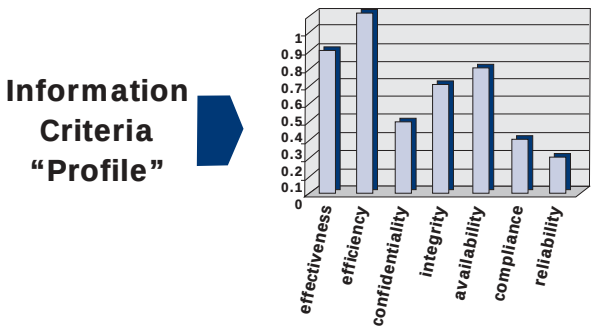


IT, as one of the major enablers of the business, will have its own scorecard. As an enabler, its measures will be performance indicators, i.e., how well is the enabler performing such that it can give an indication that the business goal will be achieved. It should also be noted that performance measures relative to the business become goal measures for IT, i.e., the Balanced Business Scorecards are cascaded (see Appendix III).

But how are the business and IT goals and measures linked? The COBIT *Framework* expresses the objectives for IT in terms of the information criteria that the business needs in order to achieve the business objectives, which will usually be expressed in terms of:

- Availability of systems and services
- Absence of integrity and confidentiality risks
- Cost-efficiency of processes and operations
- Confirmation of reliability, effectiveness and compliance.

The goal for IT can then be expressed as delivering the information that the business needs in line with these criteria. These information criteria are provided in the *Management Guidelines* with an indication whether they have primary or secondary importance for the process under review. In practice, the information criteria profile of an enterprise would be more specific.



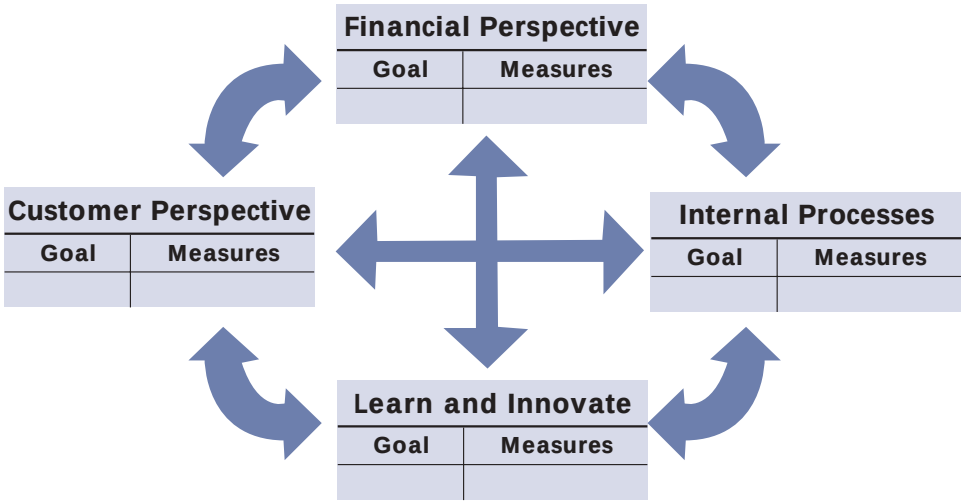
The degree of importance of each of the above information criteria is a function of the business and the environment the enterprise operates in. The previous drawing is only an example. Each organisation will have to decide how important each of the information criteria is for its business. As such, the profile also expresses the enterprise's position on risk. It should be noted, however, that the importance of the information criteria may also change for each process where possibly different objectives apply. Nonetheless, the goal for the IT organisation is to deliver the information that the business needs to accomplish its goals, according to the information criteria profile.

The relative importance of information criteria implies that a selection may need to be taken from the extensive lists of best practices that COBIT provides: the Considerations in the COBIT *Framework* (see Appendix II); the *Control Objectives*; or even the Critical Success Factors of these *Management Guidelines*.

To better understand the goal and performance indicators, we also looked at the four dimensions of the Balanced Business Scorecard:

- **Financial** — How do shareholders look at us? (i.e., deliver against budget)
- **Customer** — How do customers see us? (e.g., customer satisfaction, on time delivery, service value)
- **Internal process** — How do we look at ourselves? (i.e., process orientation and quality)
- **Learning/innovation** — Can we continue to improve and create values? (i.e., employee knowledge and technical infrastructure).

Key Goal Indicators for IT are business driven and usually provide the measures needed to support the financial and customer dimensions of the enterprise Balanced Business Scorecard, which is depicted in the following diagram. Key Performance Indicators, as we will see in the next section, focus on the other two dimensions of the Balanced Business Scorecard: internal processes and innovation. Financial results and customer satisfaction are typically measures of the business goal being achieved and measured *after-the-fact*. On the other hand, process excellence and ability to learn and innovate are indicators of how well an organisation is performing and gives an indication of the probability of achieving success *before-the-fact*.



Key Goal Indicators are 'LAG' indicators, as they can only be measured after the fact, as opposed to Key Performance Indicators which are 'LEAD' indicators giving an indication of success before the fact. They can also be expressed negatively, i.e., in terms of the impact of not reaching the goal. The Substantiating Risk section of the COBIT *Audit Guidelines* gives examples for each of the 34 IT Processes of what can go wrong if the IT process is not adequately controlled.

Key Goal Indicators should not be vague, but measurable as a number or percentage. These measures should show that information and technology are contributing to the mission and strategy of the organisation. Because goals and targets are specific to the enterprise and its environment, many Key Goal Indicators have been expressed with a direction, e.g., increased availability, decreased cost. In practice, management will have to set specific targets which need to be met, taking into account past performance and future goals.

To illustrate the previous points, a set of generic Key Goal Indicators is listed below that is usually applicable to all IT processes:

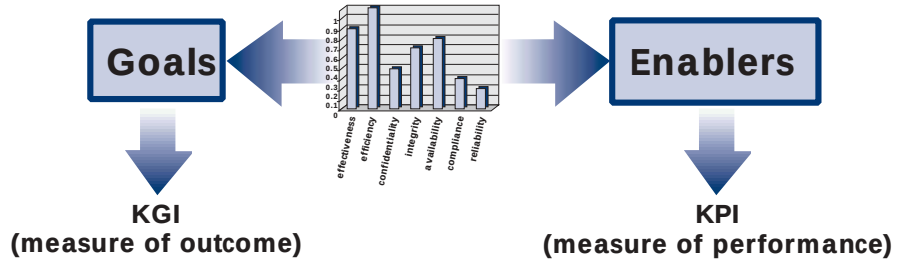
- Achieving targeted return on investment or business value benefits
- Enhanced performance management
- Reduced IT risks
- Productivity improvements
- Integrated supply chains
- Standardised processes
- Boost of service delivery (sales)
- Reaching new and satisfying existing customers
- Creation of new service delivery channels
- Availability of bandwidth, computing power and IT delivery mechanisms fitting the business, and their uptime and downtime
- Meeting requirements and expectations of the customer of the process on budget and on time
- Number of customers and cost per customer served
- Adherence to industry standards.

In summary, Key Goal Indicators are:

- A representation of the process goal, i.e., a measure of "what," or a target to achieve
- The description of the outcome of the process and therefore 'LAG' indicators, i.e., measurable after the fact
- Immediate indicators of the successful completion of the process or indirect indicators of the value the process delivered to the business
- Possibly descriptions of a measure of the impact of not reaching the process goal
- Focused on the customer and financial dimensions of the Balanced Business Scorecard
- IT oriented but business driven
- Expressed in precise, measurable terms wherever possible
- Focused on those information criteria that have been identified as most importance for this process.

4. KEY PERFORMANCE INDICATORS

Key Performance Indicators are measures that tell management that an IT process is achieving its business requirements by monitoring the performance of the enablers of that IT process. Building on the Balanced Business Scorecard principles, the relationship between Key Performance Indicators and Key Goal Indicators is as follows:



Key Performance Indicators are short, focused and measurable indicators of *performance* of the enabling factors of the IT processes, indicating how well the process enables the goal to be reached. While Key Goal Indicators focus on «what», the Key Performance Indicators are concerned with «how». They will often be a measure of a Critical Success Factor and, when monitored and acted upon, will identify opportunities for the improvement of the process. These improvements should positively influence the outcome and, as such, Key Performance Indicators have a cause-effect relationship with the Key Goal Indicators of the process.

In some cases, composite measures are suggested for Key Performance Indicators and, in a few cases, for Key Goal Indicators as well. An example could be a measure for the adequacy of the IT organisation that tracks, as one number, IT staff's business focus, morale and job satisfaction. Or, for example the quality index of a plan by monitoring as one number, its timeliness, completeness and structured approach.

While Key Goal Indicators are business driven, Key Performance Indicators are process oriented and will often express how well the processes and the organisation leverage and manage the needed resources. Similar to Key Goal Indicators, they are often expressed as a number or percentage. A good 'acid' test of a Key Performance Indicators is to see whether it really does predict success or failure of the process goal and whether or not it assists management in improving the process.

A set of generic Key Performance Indicators is listed below that is usually applicable to all IT processes:

1. Applying to IT in general

- Reduced cycle times (i.e., responsiveness of IT production and development)
- Increased quality and innovation
- Utilisation of communications bandwidth and computing power
- Service availability and response times
- Satisfaction of stakeholders (survey and number of complaints)
- Number of staff trained in new technology and customer service skills.

2. Applying to most IT processes

- Improved cost-efficiency of the process (cost vs. deliverables)
- Staff productivity (number of deliverables) and morale (survey)
- Amount of errors and rework.

3. Applying to IT governance

- Benchmark comparisons
- Number of non-compliance reportings.

In summary, Key Performance Indicators:

- ◆ Are a measure of how well the process is performing
- ◆ Predict the probability of success or failure in the future, i.e., are 'LEAD' indicators
- ◆ Are process oriented, but IT driven
- ◆ Focus on the process and learning dimensions of the Balanced Business Scorecard
- ◆ Are expressed in precisely measurable terms
- ◆ Will help in improving the IT process when measured and acted upon
- ◆ Focus on those resources identified as the most important for this process.

5. CONCLUSION

To get Information Technology under control such that IT is aligned with the business and enables it by delivering the information the organisation needs, a number of management tools have been provided in these *Management Guidelines*. The relationship between the Critical Success Factors, the Maturity Models, the Key Performance Indicators and the Key Goal Indicators can be expressed as:

"CSFs are the most important things you need to do based on the choices made in the Maturity Model, whilst monitoring through KPIs whether you will likely reach the goals set by the KGIs."

However, it needs to be emphasised that these guidelines remain generic, generally applicable and do not provide industry specific measures. Organisations will in many cases need to customise this general set of directions to their own environment.

Starting from the COBIT *Framework*, the application of international standards and guidelines, and research into best practices have led to the development of the *Control Objectives*. *Audit Guidelines* have been developed to assess whether these *Control Objectives* are appropriately implemented. However, management needs a similar application of the *Framework* so it can self-assess and make choices for control implementation and improvements over its information and related technology.

That is the main purpose of the *Management Guidelines*, developed with the help of world-wide experts in the field of IT governance, performance management, and information security and control. They provide a set of tools to assist management in responding to the question:

"What is the right level of control for my IT such that it supports my enterprise objectives?"

PLANNING AND ORGANISATION

PO1	Define a Strategic IT Plan
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Organisation and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage Human Resources
PO8	Ensure Compliance with External Requirements
PO9	Assess Risks
PO10	Manage Projects
PO11	Manage Quality

ACQUISITION AND IMPLEMENTATION

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Develop and Maintain Procedures
AI5	Install and Accredit Systems
AI6	Manage Changes

DELIVERY AND SUPPORT

DS1	Define and Manage Service Levels
DS2	Manage Third-Party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Assist and Advise Customers
DS9	Manage the Configuration
DS10	Manage Problems and Incidents
DS11	Manage Data
DS12	Manage Facilities
DS13	Manage Operations

MONITORING

M1	Monitor the Processes
M2	Assess Internal Control Adequacy
M3	Obtain Independent Assurance
M4	Provide for Independent Audit

The following pages provide detailed *Management Guidelines* for each of the 34 COBIT processes and Appendix I provides guidance on how to read them.

PLANNING & ORGANISATION

Control over the IT process **Define a Strategic IT Plan** with the business goal of *striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment*

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

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*

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

Information Criteria
P effectiveness
S efficiency
confidentiality
integrity
availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Percent of IT and business strategic plans that are aligned and cascaded into long- and short-range plans leading to individual responsibilities
- Percent of business units that have clear, understood and current IT capabilities
- Management survey determines clear link between responsibilities and the business and IT strategic goals
- Percent of business units using strategic technology covered in the IT strategic plan
- Percent of IT budget championed by business owners
- Acceptable and reasonable number of outstanding IT projects

Critical Success Factors

- The planning process provides for a prioritisation scheme for the business objectives and quantifies, where possible, the business requirements
- Management buy-in and support is enabled by a documented methodology for the IT strategy development, the support of validated data and a structured, transparent decision-making process
- The IT strategic plan clearly states a risk position, such as leading edge or road-tested, innovator or follower, and the required balance between time-to-market, cost of ownership and service quality
- All assumptions of the strategic plan have been challenged and tested
- The processes, services and functions needed for the outcome are defined, but are flexible and changeable, with a transparent change control process
- A reality check of the strategy by a third party has been conducted to increase objectivity and is repeated at appropriate times
- IT strategic planning is translated into roadmaps and migration strategies

Key Performance Indicators

- Currency of IT capabilities assessment (number of months since last update)
- Age of IT strategic plan (number of months since last update)
- Percent of participant satisfaction with the IT strategic planning process
- Time lag between change in the IT strategic plans and changes to operating plans
- Index of participants involved in strategic IT plan development, based on size of effort, ratio of involvement of business owners to IT staff and number of key participants
- Index of quality of the plan, including timelines of development effort, adherence to structured approach and completeness of plan

PO1 Maturity Model

Control over the IT process **Define a Strategic IT Plan** with the business goal of *striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment*

0 Non-existent IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

1 Initial / Ad Hoc The need for IT strategic planning is known by IT management, but there is no structured decision process in place. IT strategic planning is performed on an as needed basis in response to a specific business requirement and results are therefore sporadic and inconsistent. IT strategic planning is occasionally discussed at IT management meetings, but not at business management meetings. The alignment of business requirements, applications and technology takes place reactively, driven by vendor offerings, rather than by an organisation-wide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 Repeatable but Intuitive IT strategic planning is understood by IT management, but is not documented. IT strategic planning is performed by IT management, but only shared with business management on an as needed basis. Updating of the IT strategic plan occurs only in response to requests by management and there is no proactive process for identifying those IT and business developments that require updates to the plan. Strategic decisions are driven on a project-by-project basis, without consistency with an overall organisation strategy. The risks and user benefits of major strategic decisions are being recognised, but their definition is intuitive.

3 Defined Process A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach, which is documented and known to all staff. The IT planning process is reasonably sound and ensures that appropriate planning is likely to be performed. However, discretion is given to individual managers with respect to implementation of the process and there are no procedures to examine the process on a regular basis. The overall IT strategy includes a consistent definition of risks that the organisation is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly drive the acquisition of new products and technologies.

4 Managed and Measurable IT strategic planning is standard practice and exceptions would be noticed by management. IT strategic planning is a defined management function with senior level responsibilities. With respect to the IT strategic planning process, management is able to monitor it, make informed decisions based on it and measure its effectiveness. Both short-range and long-range IT planning occurs and is cascaded down into the organisation, with updates done as needed. The IT strategy and organisation-wide strategy are increasingly becoming more coordinated by addressing business processes and value-added capabilities and by leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for balancing the internal and external resources required in system development and operations. Benchmarking against industry norms and competitors is becoming increasingly formalised.

5 Optimised IT strategic planning is a documented, living process, is continuously considered in business goal setting and results in discernable business value through investments in IT. Risk and value added considerations are continuously updated in the IT strategic planning process. There is an IT strategic planning function that is integral to the business planning function. Realistic long-range IT plans are developed and constantly being updated to reflect changing technology and business-related developments. Short-range IT plans contain project task milestones and deliverables, which are continuously monitored and updated, as changes occur. Benchmarking against well-understood and reliable industry norms is a well-defined process and is integrated with the strategy formulation process. The IT organisation identifies and leverages new technology developments to drive the creation of new business capabilities and improve the competitive advantage of the organisation.

Control over the IT process **Define the Information Architecture** with the business goal of *optimising the organisation of the information systems*

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 business information model and ensuring appropriate systems are defined to optimise the use of this information*

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

Information Criteria
P effectiveness
S efficiency
S confidentiality
S integrity
availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
people
✓ applications
technology
facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Faster application development
- Decreased time to market for major information systems
- Implementation of defined confidentiality, availability and integrity requirements
- Reduction of data redundancy
- Increased interoperability between systems and applications
- Percent of the corporate data dictionary available to users in an automated manner

Critical Success Factors

- A corporate data administration function is established, at a high enough level, with sufficient authority to administer the corporate data model and information standards
- Information architectural standards are documented, communicated and complied with
- The data model is simple and clear to all
- A corporate data model representing the business is defined and drives the information architecture
- Data ownership is allocated and accepted
- Data and data models are kept current
- An automated repository is used to ensure consistency between the components of the information systems infrastructure, such as information architecture, data dictionaries, applications, data syntax, classification schemes and security levels
- Understanding information requirements sufficiently enough in advance

Key Performance Indicators

- Percent of IT budget assigned to information architecture development and maintenance
- Number of application changes occurring to realign with the data model
- Percent of information integrity requirements documented in the data classification scheme
- Number of application and system incidents caused by inconsistencies in the data model
- Amount of rework caused by inconsistencies in the data model
- Number of errors attributed to the lack of currency of the information architecture
- Time lag between changes in the information architecture and applications

PO2 Maturity Model

Control over the IT process **Define the Information Architecture** with the business goal of *optimising the organisation of the information systems*

0 Non-existent There is no awareness of the importance of the information architecture for the organisation. The knowledge, expertise and responsibilities necessary to develop this architecture do not exist in the organisation.

1 Initial / Ad Hoc Management recognises the need for an information architecture, but has not formalised either a process or a plan to develop one. Isolated and reactive development of components of an information architecture is occurring. There are isolated and partial implementations of data diagrams, documentation, and data syntax rules. The definitions address data, rather than information, and are driven by application software vendor offerings. There is inconsistent and sporadic communication of the need for an information architecture.

2 Repeatable but Intuitive There is an awareness of the importance of an information architecture for the organisation. A process emerges and similar, though informal and intuitive, procedures are followed by different individuals within the organisation. There is no formal training and people obtain their skills through hands-on experience and repeated application of techniques. Tactical requirements drive the development of information architecture components by individuals.

3 Defined Process The importance of the information architecture is understood and accepted, and responsibility for its delivery is assigned and clearly communicated. Related procedures, tools and techniques, although not sophisticated, have been standardised and documented and are part of informal training activities. Basic information architecture policies have been developed including some strategic requirements, but compliance with policies, standards and tools is not consistently enforced. A formally defined data administration function is in place, setting organisation-wide standards and is beginning to report on the delivery and use of the information architecture. Organisation-wide automated data administration tools are emerging, but the processes and rules used are defined by database software vendor offerings.

4 Managed and Measurable The development and enforcement of the information architecture is fully supported by formal methods and techniques. The process is responsive to changes and business needs. Accountability for the performance of the architecture development process is enforced and success of the information architecture is being measured. Formal training activities are defined, documented and consistently applied. Supporting automated tools are widespread, but are not yet integrated. Internal best practices are shared and introduced to the process. Basic metrics have been identified and a measurement system is in place. The information architecture definition process is proactive and focused on addressing future business needs. The data administration organisation is actively involved in all application development efforts to ensure consistency. An automated repository is fully implemented and more complex data models are being implemented to leverage the information content of the databases. Executive information systems and decision support systems are leveraging the available information.

5 Optimised The information architecture is consistently enforced at all levels and its value to the business is continually stressed. IT personnel have the expertise and skills necessary to develop and maintain a robust and responsive information architecture that reflects all the business requirements. The information provided by the information architecture is consistently and extensively applied. Extensive use is made of industry best practices in the development and maintenance of the information architecture including a continuous improvement process. The strategy for leveraging information through data warehousing and data mining technologies is defined. The information architecture is continuously improving and takes into consideration non-traditional information on processes, organisations and systems.

Control over the IT process **Determine Technological Direction** with the business goal of *taking advantage of available and emerging technology to drive and make possible the business strategy*

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

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*

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

Information Criteria
P effectiveness
S efficiency
confidentiality
integrity
availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
people
applications
✓ technology
✓ facilities
data

(✓) applicable to

Critical Success Factors

- Business technology reports are disseminated to business units
- Technology changes are pro-actively monitored for threats and opportunities, with clearly assigned responsibilities and with a defined process that uses proven and reliable resources
- Monitoring results are evaluated at senior management levels and actions are agreed upon and integrated into the IT infrastructure plan, while maintaining alignment with the IT strategic plan
- A research, prototyping and testing facility is set up focusing on demonstrating business value and on identifying constraints and opportunities, rather than technological proficiency
- Technology infrastructure planning is translated into plans for technology acquisition, staff training and recruitment, with regard for technology usage policies and standards
- Roadmaps and migration strategies exist to take the organisation from the current state to the future state of IT infrastructure
- Technology direction and planning assumptions are reassessed independently at appropriate times
- The IT infrastructure plan is regularly assessed for contingency aspects
- An open exchange on technology developments and good relationships with vendors and third parties promotes industry watch functions and benchmarking

Key Goal Indicators

- Number of technology solutions that are not aligned with the business strategy
- Percent of non-compliant technology projects planned
- Number of non-compatible technologies and platforms
- Decreased number of technology platforms to maintain
- Reduced applications deployment effort and time-to-market
- Increased interoperability between systems and applications

Key Performance Indicators

- Percent of IT budget assigned to technology infrastructure and research
- Number of months since the last technology infrastructure review
- Business functions' satisfaction with the timely identification and analysis of technological opportunities
- Percent of technological domains within the technology infrastructure plan that have sub-plans specifying current state, vision state and implementation roadmaps
- Average length of time between the identification of potentially relevant new technology and the decision as to what to do with that technology

PO3 Maturity Model

Control over the IT process **Determine Technological Direction** with the business goal of *taking advantage of available and emerging technology to drive and enable business strategy*

0 Non-existent There is no awareness of the importance of technology infrastructure planning for the entity. The knowledge and expertise necessary to develop such a technology infrastructure plan does not exist. There is a lack of understanding that planning for technological change is critical to effectively allocate resources.

1 Initial / Ad Hoc Management recognises the need for technology infrastructure planning, but has not formalised either a process or plan. Technology component developments and emerging technology implementations are ad-hoc and isolated. There is a reactive and operationally focused approach to planning. Technology directions are driven by the often-contradictory product evolution plans of hardware, systems software and applications software vendors. Communication of the potential impact of changes in technology is inconsistent.

2 Repeatable but Intuitive There is implicit understanding of the need for and importance of technology planning. This need and importance is communicated. Planning is, however, tactical and focused on generating technical solutions to technical problems, rather than on the use of technology to meet business needs. Evaluation of technological changes is left to different individuals who follow intuitive, but similar processes. There is no formal training and communication of roles and responsibilities. Common techniques and standards are emerging for the development of infrastructure components.

3 Defined Process Management is aware of the importance of the technology infrastructure plan. The technology infrastructure plan development process is reasonably sound and is aligned with the IT strategic plan. There is a defined, documented and well-communicated technology infrastructure plan, but it is inconsistently applied. The technology infrastructure direction includes an understanding on where the organisation wants to lead or lag in the use of technology, based on risks and alignment with the organisation strategy. Key vendors are selected based on the understanding of their long-term technology and product development plans, consistent with the organisation direction.

4 Managed and Measurable IT staff have the expertise and skills necessary to develop a technology infrastructure plan. There is formal and specialised training for technology research. The potential impact of changing and emerging technologies is taken into account and validated. Management can identify deviations from the plan and anticipate problems. Responsibility for the development and maintenance of a technology infrastructure plan has been assigned. The process is sophisticated and responsive to change. Internal best practices have been introduced into the process. The human resources strategy is aligned with the technology direction, to ensure that IT staffs can manage technology changes. Migration plans for introducing new technologies are defined. Outsourcing and partnering are being leveraged to access necessary expertise and skills.

5 Optimised A research function exists to review emerging and evolving technologies and benchmark the organisation against industry norms. The direction is guided by industry and international standards and developments, rather than driven by technology vendors. The potential business impact of technological change is reviewed at senior management levels and the decisions to act reflect the contribution of human and technological influences on information solutions. There is formal executive approval of new and changed technological directions. Participation in industry standards setting bodies and vendor user groups is formalised. The entity has a robust technology infrastructure plan that reflects the business requirements, is responsive and can be modified to reflect changes in the business environment. There is a continuous and enforced improvement process in place. Industry best practices are extensively used in determining the technical direction.

Control over the IT process **Define the IT Organisation and Relationships** with the business goal of *delivering the right IT services*

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

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*

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

Information Criteria
P effectiveness
S efficiency
confidentiality
integrity
availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
applications
technology
facilities
data

(✓) applicable to

Critical Success Factors

- The IT organisation communicates its goals and results at all levels
- IT is organised to be involved in all decision processes, respond to key business initiatives and focus on all corporate automation needs
- The IT organisational model is aligned with the business functions and adapts rapidly to changes in the business environment
- Through encouraging and promoting the taking of responsibility, an IT organisation develops and grows individuals and heightens collaboration
- There are clear command and control processes, with segregation where needed, specialisation where required and empowerment where beneficial
- The IT organisation properly positions security, internal control and quality functions, and adequately balances supervision and empowerment
- The IT organisation is flexible to adapt to risk and crisis situations and moves from a hierarchical model, when all is well, to a team-based model when pressure mounts, empowering individuals in times of crisis
- Strong management control is established over the outsourcing of IT services, with a clear policy, and awareness of the total cost of outsourcing
- Essential IT functions are explicitly identified in the organisation model, with clearly specified roles and responsibilities

Key Goal Indicators

- Number of delayed business projects due to IT organisational inertia or unavailability of necessary capabilities
- Number of core IT activities outside of the IT organisation that are not approved or are not subject to IT organisational standards
- Number of business units supported by the IT organisation
- Survey rating of IT staff's business focus, morale and job satisfaction
- Percent utilisation of IT personnel on IT processes that produce direct business benefits

Key Performance Indicators

- Age of organisational change, including reorganisation or organisational reassessment
- Number of organisational assessment recommendations not acted upon
- Percent of IT organisational functions which are mapped into the business organisational structure
- Number of IT units with business objectives directly cascaded into individual roles and responsibilities
- Percent of roles with documented position descriptions
- Average lag time between change in business direction and the reflection of the change in the IT organisational structure
- Percent of essential functions which are explicitly identified in the organisational model with clear roles and responsibilities

PO4 Maturity Model

Control over the IT process **Define the IT Organisation and Relationships** with the business goal of *delivering the right IT services*

0 Non-existent The IT organisation is not effectively established to focus on the achievement of business objectives.

1 Initial / Ad Hoc IT activities and functions are reactive and inconsistently implemented. There is no defined organisational structure, roles and responsibilities are informally assigned, and no clear lines of responsibilities exist. The IT function is considered a support function, without an overall organisation perspective.

2 Repeatable but Intuitive There is an implicit understanding of the need for of an IT organisation; however, roles and responsibilities are neither formalised nor enforced. The IT function is organised to respond tactically, but inconsistently, to customer needs and vendor relationships. The need for a structured organisation and vendor management is communicated, but decisions are still dependent on the knowledge and skills of key individuals. There is an emergence of common techniques to manage the IT organisation and vendor relationships.

3 Defined Process Defined roles and responsibilities for the IT organisation and third parties exist. The IT organisation is developed, documented, communicated and aligned with the IT strategy. Organisational design and the internal control environment are defined. There is formalisation of relationships with other parties, including steering committees, internal audit and vendor management. The IT organisation is functionally complete; however, IT is still more focused on technological solutions rather than on using technology to solve business problems. There are definitions of the functions to be performed by IT personnel and of those which will be performed by users.

4 Managed and Measurable The IT organisation is sophisticated, proactively responds to change and includes all roles necessary to meet business requirements. IT management, process ownership, accountability and responsibility are defined and balanced. Essential IT staffing requirements and expertise needs are satisfied. Internal best practices have been applied in the organisation of the IT functions. IT management has the appropriate expertise and skills to define, implement and monitor the preferred organisation and relationships. Measurable metrics to support business objectives and user defined critical success factors are standardised. Skill inventories are available to support project staffing and professional development. The balance between the skills and resources available internally and those needed from external organisations is defined and enforced.

5 Optimised The IT organisational structure appropriately reflects the business needs by providing services aligned with strategic business processes, rather than with isolated technologies. The IT organisational structure is flexible and adaptive. There is a formal definition of relationships with users and third parties. Industry best practices are deployed. The process to develop and manage the organisational structure is sophisticated, followed and well managed. Extensive internal and external technical knowledge is utilised. There is extensive use of technology to assist in the monitoring of organisational roles and responsibilities. IT leverages technology to support complex, geographically distributed and virtual organisations. There is a continuous improvement process in place.

Control over the IT process **Manage the IT Investment** with the business goal of *ensuring funding and controlling disbursement of financial resources*

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

is enabled by *a periodic investment and operational budget established and approved by the business*

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

Information Criteria	
P	effectiveness
P	efficiency
	confidentiality
	integrity
	availability
	compliance
S	reliability

(**P**) primary (**S**) secondary

IT Resources	
✓	people
✓	applications
✓	technology
✓	facilities
	data

(✓) applicable to

Critical Success Factors

- All IT related costs are identified and classified
- An effective IT asset inventory that facilitates accurate cost measurement is maintained
- Formal investment criteria are defined for decision making in a responsive approval process, adaptable to the type of project
- An IT delivery plan is defined, providing context so that a clear view exists of on-going work and investments, technology life cycles and technology component reusability
- An investment decision-making process is defined and considers short- and long-term impacts, cross-divisional impacts, business justification, benefit realisation, strategic contribution, and compliance with the technology architecture and direction
- To allow for clear choices based on impacts, measurable benefits, time-frames and feasibility, investment decisions need to be presented with options and alternatives
- IT budgets and investments are aligned with the IT strategy and business plans
- Expenditure approval authority is clearly delegated
- Budgets that cover end-to-end expenditures have identifiable and accountable owners and are timely and closely tracked in an automated manner
- Clear management accountability for realising forecasted benefits and a process to track and report on benefits realisation exist, eliminating cross-subsidies
- There are clear management accountabilities for realising and tracking forecasted benefits
- Decision makers consider the full impact, including complete life-cycle and adverse effects, on other business units

Key Goal Indicators

- Percent of IT investments meeting or exceeding expected benefits, based on return on investment and user satisfaction
- Actual IT expenses as percent of total organisation expenses vs. target
- Actual IT expenses as a percent of revenues vs. target
- Percent of business owner IT budgets met
- Absence of project delays caused by lags in investment decisions or unavailablity of funding

Key Performance Indicators

- Percent of projects using the standard IT investment and budget models
- Percent of projects with business owners
- Months since last review of budgets
- Time lag between deviation occurrence and reporting
- Percent of project files containing investment evaluations
- Number of projects where business benefits are not verified post-facto
- Number of projects revealing investment or resource conflicts after approval
- Number of instances and time-lag in delayed use of new technology

PO5 Maturity Model

Control over the IT process **Manage the IT Investment** with the business goal of *ensuring funding and controlling disbursement of financial resources*

0 Non-existent There is no awareness of the importance of IT investment selection and budgeting. There is no tracking or monitoring of IT investments and expenditures.

1 Initial / Ad Hoc The organisation recognises the need for managing the IT investment, but this need is communicated inconsistently. There is no formal allocation of responsibility for IT investment selection and budget development. Perceived significant expenditures require supporting justifications. Isolated implementations of IT investment selection and budgeting occur, with informal documentation. IT investments are justified on an ad hoc basis. Reactive and operationally focused budgeting decisions occur.

2 Repeatable but Intuitive There is an implicit understanding of the need for IT investment selection and budgeting. The need for a selection and budgeting process is communicated. Compliance is dependent on the initiative of individuals in the organisation. There is an emergence of common techniques to develop components of the IT budget. Reactive and tactical budgeting decisions occur. Expectations based on trends in technology are beginning to be stated and their impact on productivity and system life cycles are starting to be considered in investment decisions.

3 Defined Process The IT investment selection and budgeting processes are reasonably sound and cover key business and technology issues. Investment selection and policy is defined, documented and communicated. The IT budget is aligned with the strategic IT and business plans. The budgeting and IT investment selection processes are formalised, documented and communicated. Informal self-training is occurring. Formal approval of IT investment selections and budgets is taking place. The balance between the investments in human resources, hardware, systems software and application software is defined and agreed upon in order to leverage technological developments and the availability and productivity of IT professionals.

4 Managed and Measurable Responsibility and accountability for investment selection and budgeting is assigned to a specific individual. Budget variances are identified and resolved. IT staff have the expertise and skills necessary to develop the IT budget and recommend appropriate IT investments. Formal costing analyses are performed covering direct and indirect costs of existing operations, as well as of proposed investments, using total cost of ownership concepts. A proactive and standardised process for budgeting is used. The shift in development and operating costs from hardware and software to systems integration and IT human resources is recognised in the investment plans.

5 Optimised Benefits and returns are calculated in both financial and non-financial terms. Industry best practices are used to benchmark costs and identify approaches to increase the effectiveness of investments. Analysis of technological developments is used in the investment selection and budgeting process. There is a continuous improvement process in place. Investment decisions incorporate price/performance improvement trends, supported by new technologies and products. Funding alternatives are formally investigated and evaluated within the context of the organisation's existing capital structure, using formal evaluation methods. There is proactive identification of variances. An analysis of the long-term cost of ownership is incorporated in the investment decisions. The investment process recognises the need to support long-term strategic initiatives by creating new business opportunities through the use of technology. The organisation has a well-understood investment risk policy regarding the lead or lag use of technology in developing new business opportunities or operational efficiencies.

Control over the IT process **Communicate Management Aims and Direction** with the business goal of *ensuring user awareness and understanding of those aims*

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

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*

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

Information Criteria
P effectiveness
efficiency
confidentiality
integrity
availability
S compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
applications
technology
facilities
data

(✓) applicable to

Critical Success Factors

- Policy enforcement is considered and decided upon at the time of policy development
- A confirmation process is in place to measure awareness, understanding and compliance with policies
- Well-defined and clearly articulated mission statements and policies are available
- Information control policies are aligned with the overall strategic plans
- Management endorses and is committed to the information control policies, stressing the need for communication, understanding and compliance
- Management is leading by example
- There is practical guidance with respect to implementation of policies and procedures
- Diverse attention-catching methods are used to repeatedly communicate important messages
- Information control policies are current and up-to-date
- There is a consistently applied policy development framework that guides formulation, roll out, understanding and compliance

Key Goal Indicators

- Percent of IT plans and policies covering mission, vision, goals, values, and code of conduct which are developed and documented
- Percent of IT plans and policies which are communicated to all stakeholders
- Percent of the organisation that has been trained in policies and procedures
- Improved measure of user awareness based on regular surveys
- Number of policies and procedures addressing information control

Key Performance Indicators

- Time lag between policy approval and communication to users
- Frequency of communications
- Age of specific information policy documents (number of months since last update)
- Percent of budget assigned to information policy development and implementation
- Percent of policies that have associated operational procedures to ensure that they are carried out

PO6 Maturity Model

Control over the IT process **Communicate Management Aims and Direction** with the business goal of *ensuring user awareness and understanding of those aims*

0 Non-existent Management has not established a positive information control environment. There is no recognition of the need to establish a set of policies, procedures, standards, and compliance processes.

1 Initial / Ad Hoc Management is reactive in addressing the requirements of the information control environment. Policies, procedures and standards are developed and communicated on an ad-hoc, as needed basis, driven primarily by issues. The development, communication and compliance processes are informal and inconsistent.

2 Repeatable but Intuitive Management has an implicit understanding of the needs and requirements of an effective information control environment. However, practices are informal and not consistently documented. Management has communicated the need for control policies, procedures and standards, but development is left to the discretion of individual managers and business areas. Policies and other supporting documents are developed based on individual needs and there is no overall development framework. Quality is recognised as a desirable philosophy to be followed, but practices are left to the discretion of individual managers. Training is carried out on an individual, as required basis.

3 Defined Process Management has developed, documented and communicated a complete information control and quality management environment that includes a framework for policies, procedures and standards. The policy development process is structured, maintained and known to staff, and the existing policies, procedures and standards are reasonably sound and cover key issues. Management has addressed the importance of IT security awareness and has initiated awareness programmes. Formal training is available to support the information control environment but is not rigorously applied. There is inconsistent monitoring of compliance with the control policies and standards.

4 Managed and Measurable Management accepts responsibility for communicating internal control policies and has delegated responsibility and allocated sufficient resources to maintain the environment in line with significant changes. A positive, proactive information control environment, including a commitment to quality and IT security awareness, has been established. A complete set of policies, procedures and standards has been developed, maintained and communicated and is a composite of internal best practices. A framework for roll out and subsequent compliance checks has been established.

5 Optimised The information control environment is aligned with the strategic management framework and vision and is frequently reviewed, updated and continuously improved. Internal and external experts are assigned to ensure that industry best practices are being adopted with respect to control guidance and communication techniques. Monitoring, self-assessment and communication processes are pervasive within the organisation. Technology is used to maintain policy and awareness knowledge bases and to optimise communication, using office automation and computer based training tools.

Control over the IT process **Manage Human Resources** with the business goal of *acquiring and maintaining a motivated and competent workforce and maximising personnel contributions to the IT processes*

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

is enabled by *sound, fair and transparent personnel management practices to recruit, hire, vet, compensate, train, appraise, promote and dismiss*

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

Information Criteria
P effectiveness
P efficiency
confidentiality
integrity
availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
applications
technology
facilities
data

(✓) applicable to

Key Goal Indicators

- Age of IT human resources management plan defined by number of months since last update
- Percent of IT staff that meet the competency profile for their role within the organisation
- Percent utilisation of IT personnel on IT processes which provide direct business benefits
- IT personnel turnover rate
- Percent achievement of staffing complement
- Average length of time, in months, that IT personnel jobs are open

Key Performance Indicators

- Time lag between changes in the IT strategic plan and the IT human resources management plan
- Percent of IT personnel with completed professional development plans
- Percent of IT personnel with documented and validated performance reviews
- Percent of training time per person
- Percent of critical personnel cross-trained and assigned back-up personnel
- Number of projects delayed or cancelled due to lack of IT personnel resources
- Percent of the human resources budget assigned to the development and maintenance of the IT human resources management plan
- Percent of IT personnel positions with documented job descriptions and hiring qualifications

Critical Success Factors

- A framework exists for the development and maintenance of an IT human resources management plan
- Management supports and is committed to the IT human resources management plan
- There is consistency between the IT strategic plan and the IT human resources management plan
- Sufficient and appropriately skilled resources are allocated to the development of the IT human resources management plan
- Appropriate ongoing IT and orientation training resources are allocated to fulfil the needs of the IT human resources management plan
- Succession plans consider single points of dependency to avoid leaving expertise gaps
- Job rotation for career development is implemented

PO7 Maturity Model

Control over the IT process **Manage Human Resources** with the business goal of *maximising personnel contributions to the IT processes*

0 **Non-existent** There is no awareness about the importance of aligning IT human resources management with the technology planning process for the organisation. There is no person or group formally responsible for IT human resources management.

1 **Initial / Ad Hoc** Management recognises the need for IT human resources management, but has not formalised a process or plan. The IT human resources management process is informal and has a reactive and operationally focused approach to the hiring and managing of IT personnel. Awareness is developing concerning the impact that rapid business and technology changes and increasingly complex solutions have on the need for new skills and competence levels.

2 **Repeatable but Intuitive** There is implicit understanding of the need for IT human resources management. There is a tactical approach to the hiring and managing of IT personnel, driven by project-specific needs, rather than by a technology direction and an understood balance of internal and external availability of skilled staff. Informal training takes place for new personnel, who then receive training on an as required basis.

3 **Defined Process** The process for managing IT human resources has been developed and there is a defined and documented IT human resources management plan. There is a strategic approach to the hiring and managing of IT personnel. There is a formal training plan designed to meet the needs of IT human resources. A rotational program, designed to expand both technical and business management skills, is established.

4 **Managed and Measurable** Responsibility for the development and maintenance of an IT human resources management plan has been assigned to a specific individual with the requisite expertise and skills necessary to develop and maintain the plan. The process is responsive to change. The organisation has standardised measures that allow it to identify deviations from the plan, with specific emphasis on managing IT personnel growth and turnover. Compensation scale analysis is performed periodically to ensure that salaries are competitive with those in comparable IT organisations. IT human resources management is proactive, taking into account career path development.

5 **Optimised** The organisation has an effective IT human resources management plan that meets the business requirements for IT and the business it supports. IT human resources management is integrated with technology planning, ensuring optimum development and use of available IT skills. Components of IT human resources management are consistent with industry best practices, such as compensation, performance reviews, participation in industry forums, transfer of knowledge, training and mentoring. Training programs are developed for all new technology standards and products prior to their deployment in the organisation. Technology is used in providing skills, training and competence requirement information in easily accessible databases, to assist the IT human resources management process. Incentive programs are defined and enforced for IT management, similar to those available for other senior management of the organisation, to reward those meeting IT performance goals.

Control over the IT process **Ensure Compliance with External Requirements** with the business goal of *meeting legal, regulatory and contractual obligations*

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

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

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

Information Criteria	
P	effectiveness
	efficiency
	confidentiality
	integrity
	availability
P	compliance
S	reliability

(**P**) primary (**S**) secondary

IT Resources	
✓	people
✓	applications
	technology
	facilities
✓	data

(✓) applicable to

Key Goal Indicators

- Number of external legal, regulatory or contractual issues arising
- Average age of external legal, regulatory or contractual open issues
- Cost of non-compliance, such as settlements or fines

Critical Success Factors

- Policies and procedures relating to compliance with external requirements have been documented and communicated
- A monitoring function reviews compliance
- An inventory of corrective actions needed to meet external requirements is maintained
- Follow-up processes to resolve external compliance issues are defined
- Information is available to determine the cost of compliance with external requirements
- Effective internal audits covering compliance are performed

Key Performance Indicators

- Frequency of compliance reviews
- Number of exceptions identified in compliance reviews
- Average time lag between identification of external compliance issues and resolution

PO8 Maturity Model

Control over the IT process **Ensure Compliance with External Requirements** with the business goal of *meeting legal, regulatory and contractual obligations*

0 Non-existent There is little awareness of external requirements that affect IT, with no process regarding compliance with regulatory, legal and contractual requirements.

1 Initial / Ad Hoc There is awareness of regulation, contract and legal compliance impacting the organisation. Informal processes are followed to maintain compliance, but only as the need arises in new projects or in response to audits or reviews.

2 Repeatable but Intuitive There is an understanding for the need to comply with external requirements and the need is communicated. Where compliance has become a recurring requirement, as in financial regulations or privacy legislation, individual compliance procedures have been developed and are followed on a year-to-year basis. There is, however, no overall scheme in place ensuring that all compliance requirements are met. It is likely, therefore, that exceptions will occur and that new compliance needs will only be dealt with on a reactive basis. There is high reliance on the knowledge and responsibility of individuals and errors are likely. There is informal training regarding external requirements and compliance issues.

3 Defined Process Policies, procedures and processes have been developed, documented and communicated to ensure compliance with regulations and with contractual and legal obligations. These are not always followed and some may be out-of-date or impractical to implement. There is little monitoring performed and there are compliance requirements that have not been addressed. Training is provided in external legal and regulatory requirements affecting the organisation and the defined compliance processes. Standard pro-forma contracts and legal processes exist to minimise the risks associated with contractual liability.

4 Managed and Measurable There is full understanding of issues and exposures from external requirements and the need to ensure compliance at all levels. There is a formal training scheme that ensures that all staff are aware of their compliance obligations. Responsibilities are clear and process ownership is understood. The process includes a review of the environment to identify external requirements and on-going changes. There is a mechanism in place to monitor non-compliance with external requirements, enforce internal practices and implement corrective action. Non-compliance issues are analysed for root-causes in a standard manner, with the objective to identify sustainable solutions. Standardised internal best practices are utilised for specific needs such as standing regulations and recurring service contracts.

5 Optimised There is a well-organised, efficient and enforced process for complying with external requirements, based on a single central function that provides guidance and co-ordination to the whole organisation. There is extensive knowledge of the applicable external requirements, including their future trends and anticipated changes, and the need for new solutions. The organisation takes part in external discussions with regulatory and industry groups to understand and influence external requirements affecting them. Best practices have been developed ensuring efficient compliance with external requirements, resulting in very few cases of compliance exceptions. A central, organisation-wide tracking system exists, enabling management to document the workflow and to measure and improve the quality and effectiveness of the compliance monitoring process. An external requirements self-assessment process is implemented and has been refined to a level of best practice. The organisation's management style and culture relating to compliance are sufficiently strong and processes are developed well enough for training to be limited to new personnel and whenever there is a significant change.

Control over the IT process **Assess Risks** with the business goal of *supporting management decisions in achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors*

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

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*

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

Information Criteria
P effectiveness
S efficiency
P confidentiality
P integrity
P availability
S compliance
S reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Increased degree of awareness of the need for risk assessments
- Decreased number of incidents caused by risks identified after the fact
- Increased number of identified risks that have been sufficiently mitigated
- Increased number of IT processes that have formal documented risk assessments completed
- Appropriate percent or number of cost effective risk assessment measures

Critical Success Factors

- There are clearly defined roles and responsibilities for risk management ownership and management accountability
- A policy is established to define risk limits and risk tolerance
- The risk assessment is performed by matching vulnerabilities, threats and the value of data
- Structured risk information is maintained, fed by incident reporting
- Responsibilities and procedures for defining, agreeing on and funding risk management improvements exist
- Focus of the assessment is primarily on real threats and less on theoretical ones
- Brainstorming sessions and root cause analyses leading to risk identification and mitigation are routinely performed
- A reality check of the strategy is conducted by a third party to increase objectivity and is repeated at appropriate times

Key Performance Indicators

- Number of risk management meetings and workshops
- Number of risk management improvement projects
- Number of improvements to the risk assessment process
- Level of funding allocated to risk management projects
- Number and frequency of updates to published risk limits and policies
- Number and frequency of risk monitoring reports
- Number of personnel trained in risk management methodology

PO9 Maturity Model

Control over the IT process **Assess Risks** with the business goal of *supporting management decisions in achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors*

0 Non-existent Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and with development project uncertainties. Risk management has not been identified as relevant to acquiring IT solutions and delivering IT services.

1 Initial / Ad Hoc The organisation is aware of its legal and contractual responsibilities and liabilities, but considers IT risks in an ad hoc manner, without following defined processes or policies. Informal assessments of project risk take place as determined by each project. Risk assessments are not likely to be identified specifically within a project plan or to be assigned to specific managers involved in the project. IT management does not specify responsibility for risk management in job descriptions or other informal means. Specific IT-related risks such as security, availability and integrity are occasionally considered on a project-by-project basis. IT-related risks affecting day-to-day operations are infrequently discussed at management meetings. Where risks have been considered, mitigation is inconsistent.

2 Repeatable but Intuitive There is an emerging understanding that IT risks are important and need to be considered. Some approach to risk assessment exists, but the process is still immature and developing. The assessment is usually at a high-level and is typically applied only to major projects. The assessment of on-going operations depends mainly on IT managers raising it as an agenda item, which often only happens when problems occur. IT management has not generally defined procedures or job descriptions dealing with risk management.

3 Defined Process An organisation-wide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training. Decisions to follow the process and to receive training are left to the individual's discretion. The methodology is convincing and sound, and ensures that key risks to the business are likely to be identified. Decisions to follow the process are left to individual IT managers and there is no procedure to ensure that all projects are covered or that the ongoing operation is examined for risk on a regular basis.

4 Managed and Measurable The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management. It is likely that IT risk management is a defined management function with senior level responsibility. The process is advanced and risk is assessed at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the IT environment which could significantly affect the risk scenarios, such as an increased threat from the network or technical trends that affect the soundness of the IT strategy. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. Senior management and IT management have determined the levels of risk that the organisation will tolerate and have standard measures for risk/return ratios. Management budgets for operational risk management projects to reassess risks on a regular basis. A risk management database is established.

5 Optimised Risk assessment has developed to the stage where a structured, organisation-wide process is enforced, followed regularly and well managed. Risk brainstorming and root cause analysis, involving expert individuals, are applied across the entire organisation. The capturing, analysis and reporting of risk management data are highly automated. Guidance is drawn from leaders in the field and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted and extensively involves the users of IT services.

Control over the IT process **Manage Projects** with the business goal of *setting priorities and delivering on time and within budget*

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

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*

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

Information Criteria
P effectiveness
P efficiency
confidentiality
integrity
availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
data

(✓) applicable to

Critical Success Factors

- Experienced and skilled project managers are available
- An accepted and standard programme management process is in place
- There is senior management sponsorship of projects, and stakeholders and IT staff share in the definition, implementation and management of projects
- There is an understanding of the abilities and limitations of the organisation and the IT function in managing large, complex projects
- An organisation-wide project risk assessment methodology is defined and enforced
- All projects have a plan with clear traceable work breakdown structures, reasonably accurate estimates, skill requirements, issues to track, a quality plan and a transparent change process
- The transition from the implementation team to the operational team is a well-managed process
- A system development life cycle methodology has been defined and is used by the organisation

Key Goal Indicators

- Increased number of projects completed on time and on budget
- Availability of accurate project schedule and budget information
- Decrease in systemic and common project problems
- Improved timeliness of project risk identification
- Increased organisation satisfaction with project delivered services
- Improved timeliness of project management decisions

Key Performance Indicators

- Increased number of projects delivered in accordance with a defined methodology
- Percent of stakeholder participation in projects (involvement index)
- Number of project management training days per project team member
- Number of project milestone and budget reviews
- Percent of projects with post-project reviews
- Average number of years of experience of project managers

PO10 Maturity Model

Control over the IT process **Manage Projects** with the business goal of *setting priorities and delivering on time and within budget*

0 Non-existent Project management techniques are not used and the organisation does not consider business impacts associated with project mismanagement and development project failures.

1 Initial / Ad Hoc The organisation is generally aware of the need for projects to be structured and is aware of the risks of poorly managed projects. The use of project management techniques and approaches within IT is a decision left to individual IT managers. Projects are generally poorly defined and do not incorporate business and technical objectives of the organisation or the business stakeholders. There is a general lack of management commitment and project ownership and critical decisions are made without user management or customer input. There is little or no customer and user involvement in defining IT projects. There is no clear organisation within IT projects and roles and responsibilities are not defined. Project schedules and milestones are poorly defined. Project staff time and expenses are not tracked and compared to budgets.

2 Repeatable but Intuitive Senior management has gained and communicated an awareness of the need for IT project management. The organisation is in the process of learning and repeating certain techniques and methods from project to project. IT projects have informally defined business and technical objectives. There is limited stakeholder involvement in IT project management. Some guidelines have been developed for most aspects of project management, but their application is left to the discretion of the individual project manager.

3 Defined Process The IT project management process and methodology have been formally established and communicated. IT projects are defined with appropriate business and technical objectives. Stakeholders are involved in the management of IT projects. The IT project organisation and some roles and responsibilities are defined. IT projects have defined and updated milestones, schedules, budget and performance measurements. IT projects have formal post system implementation procedures. Informal project management training is provided. Quality assurance procedures and post system implementation activities have been defined, but are not broadly applied by IT managers. Policies for using a balance of internal and external resources are being defined.

4 Managed and Measurable Management requires formal and standardised project metrics and "lessons learned" to be reviewed following project completion. Project management is measured and evaluated throughout the organisation and not just within IT. Enhancements to the project management process are formalised and communicated, and project team members are trained on all enhancements. Risk management is performed as part of the project management process. Stakeholders actively participate in the projects or lead them. Project milestones, as well as the criteria for evaluating success at each milestone, have been established. Value and risk are measured and managed prior to, during and after the completion of projects. Management has established a programme management function within IT. Projects are defined, staffed and managed to increasingly address organisation goals, rather than only IT specific ones.

5 Optimised A proven, full life-cycle project methodology is implemented and enforced, and is integrated into the culture of the entire organisation. An on-going programme to identify and institutionalise best practices has been implemented. There is strong and active project support from senior management sponsors as well as stakeholders. IT management has implemented a project organisation structure with documented roles, responsibilities and staff performance criteria. A long-term IT resources strategy is defined to support development and operational outsourcing decisions. An integrated programme management office is responsible for projects from inception to post implementation. The programme management office is under the management of the business units and requisitions and directs IT resources to complete projects. Organisation-wide planning of projects ensures that user and IT resources are best utilised to support strategic initiatives.

Control over the IT process **Manage Quality** with the business goal of *meeting the IT customer requirements*

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

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

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

Information Criteria	
P	effectiveness
P	efficiency
	confidentiality
P	integrity
	availability
	compliance
S	reliability

(**P**) primary (**S**) secondary

IT Resources	
✓	people
✓	applications
✓	technology
✓	facilities
	data

(✓) applicable to

Key Goal Indicators

- Number of IT processes and projects that satisfy stakeholder requirements
- Increased rating for customer satisfaction with services rendered
- Number of IT processes and projects formally signed off by quality assurance without significant rework
- Decreased number of quality defects
- Decreased number of non-compliance reports against quality standards

Critical Success Factors

- A clearly defined and agreed upon development process has been created to perform quality assurance
- Quality is defined by the organisation with clear roles for the quality assurance processes and quality control procedures
- A quality assurance program has been implemented with well defined, measurable quality standards and quality control processes have been defined, resourced and aligned
- There is continuous improvement and a defined knowledge base for processes and metrics
- There is a quality education and training programme
- Stakeholders are involved in the quality assurance programme
- A positive quality culture is consistently promoted by all layers of management
- Awareness exists that quality standards should equally apply to processes and projects where reliance is placed on third parties
- Every delivery process needs to have proper quality assurance criteria
- Emphasis is provided on training IT and end user staff in testing methods and techniques

Key Performance Indicators

- Number of IT processes and projects with active quality assurance management participation
- Number of documented quality assurance monitoring and testing activities
- Number of quality assurance peer reviews
- Number of IT processes and projects that have been benchmarked
- Number of meetings between stakeholders and developers
- Average number of training days in quality management
- Number of projects with documented and measured quality criteria

PO11 Maturity Model

Control over the IT process **Manage Quality** with the business goal of *meeting the IT customer requirements*

0 **Non-existent** The organisation lacks a quality assurance planning process and a system development life cycle methodology. Senior management and IT staff do not recognise that a quality program is necessary. Projects and operations are never reviewed for quality.

1 **Initial / Ad Hoc** There is a management awareness of the need for quality assurance. Individual expertise drives quality assurance, when it occurs. Quality assurance activities that do occur are focused on IT project and process-oriented initiatives, not on organisation-wide processes. IT projects and operations are not generally measured for quality, but management makes informal judgements on quality.

2 **Repeatable but Intuitive** Basic quality metrics have been defined and could be repeated from project to project within the IT organisation. A programme is being established for managing quality assurance activities within IT. IT management planning and monitoring practices are established over quality assurance activities, but are not broadly enforced. Common tools and practices for quality management are emerging. Quality satisfaction surveys are occasionally conducted.

3 **Defined Process** IT management is building a knowledge base for quality metrics. There is a defined quality assurance process that has been communicated by management and involves both IT and end-user management. An education and training program has been instituted to teach all levels of the organisation about quality. Quality awareness is high throughout the organisation. Tools and practices are being standardised and root cause analysis is occasionally applied. A standardised program for measuring quality is in place and well structured. Quality satisfaction surveys are consistently conducted.

4 **Managed and Measurable** The organisation continuously and consistently measures quality of processes, services, products and projects. Quality assurance is addressed in all processes, including those processes with reliance on third parties. A standardised knowledge base is being established for quality metrics. Quality satisfaction surveying is an ongoing process and leads to root cause analysis. Cost/benefit analysis methods are used to justify quality assurance initiatives. Responsibilities and accountability are increasingly being defined for organisation-wide business processes and not only for IT processes. Benchmarking against industry and competitor norms is increasingly being performed.

5 **Optimised** Quality awareness is very high within the whole organisation. Quality assurance is integrated and enforced in all IT activities. Quality assurance processes are flexible and adaptable to changes in the IT environment. All quality problems are analysed for root causes. Quality satisfaction surveys are an essential part of a continuous improvement process. The knowledge base is enhanced with external best practices. Benchmarking against external standards is routinely being performed. The quality assurance of IT processes is fully integrated with the assurance over business processes to ensure that the products and services of the entire organisation have a competitive advantage.

This page intentionally left blank

ACQUISITION & IMPLEMENTATION

Control over the IT process **Identify Automated Solutions** with the business goal of *ensuring an effective and efficient approach to satisfy the user requirements*

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

is enabled by *an objective and clear identification and analysis of the alternative opportunities measured against user requirements*

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

Information Criteria	
P	effectiveness
S	efficiency
	confidentiality
	integrity
	availability
	compliance
	reliability

(**P**) primary (**S**) secondary

IT Resources	
	people
✓	applications
✓	technology
✓	facilities
	data

(✓) applicable to

Critical Success Factors

- There is good knowledge of the solutions available in the market
- Practices are defined to address not only soundness of design and robustness of functionality, but also: operability, including performance, scalability and integration; acceptability, covering administration, maintenance and support; and sustainability, in respect of cost, productivity and appearance
- Criteria for consideration of in-house development, purchased solutions and outsourcing options are defined
- There is a general acquisition and implementation method or system development life cycle methodology that is clear, understood and accepted
- There is a transparent, fast and efficient process for planning, initiation and approval of solutions
- Key users are identified to support the solution analysis and recommendation
- Solutions are constructed from pre-defined components
- A structured requirements analysis process is implemented
- There is a clear definition of supplier responsibilities
- Use proven technology as a matter of principle and new technology only where needed, justified by a business case
- There is awareness of the total cost of ownership of the solution
- Security and control requirements are considered early on

Key Goal Indicators

- Number or percent of projects restarted or redirected
- Number or backlog of non-addressed solutions
- Number or percent of solutions signed off by the chief technology officer or architect as in line with the IT strategy and IT architecture
- Number or percent of solutions signed off by user as fully meeting user requirements
- Number or percent of solutions that fully consider alternatives, feasibility and risk
- Percent of implemented solutions formally approved by business owners and by IT

Key Performance Indicators

- Time lag between requirement definition and identification of a solution
- Number or percent of solutions returned from acceptance testing
- Lag time before approval of identified solution
- Number of projects involving users in requirements definition and solution selection
- Number of solutions subsequently affected by significant change requests due to functional changes

AI1 Maturity Model

Control over the IT process **Identify Automated Solutions** with the business goal of *ensuring the best approach to satisfy the user requirement*

0 Non-existent The organisation does not require the identification of functional and operational requirements for development, implementation or modification of solutions, such as system, service, infrastructure, software and data. The organisation does not maintain an awareness of available technology solutions potentially relevant to its business.

1 Initial / Ad Hoc There is an awareness of the need to define requirements and identify technology solutions. However, approaches are inconsistent and not based on any specific acquisition and implementation methodology. Individual groups tend to meet to discuss needs informally and requirements are usually not documented. Solutions are identified by individuals based on limited market awareness, or in response to vendor offerings. There is little or no structured analysis or research of available technology.

2 Repeatable but Intuitive There is no formally defined acquisition and implementation methodology, but requirements tend to be defined in a similar way across the business due to common practices within IT. Solutions are identified informally based on the internal experience and knowledge of the IT function. The success of each project depends on the expertise of a few key IT individuals and the quality of documentation and decision making varies considerably.

3 Defined Process The organisation has established an acquisition and implementation methodology, which requires a clear and structured approach in determining IT solutions to satisfy business requirements. The approach requires the consideration of alternatives evaluated against user requirements, technological opportunities, economic feasibility, risk assessments and other factors. The process is not, however, always followed for every project and depends on decisions made by the individual staff involved, the amount of management time committed and the size and priority of the original business requirement. Typically, the process is bypassed or considered to be impractical.

4 Managed and Measurable The organisation has established an acquisition and implementation methodology, which has evolved to the point where it is unusual for it not to be applied. Documentation is of a good quality and each stage is properly approved. Requirements are well articulated and in accordance with pre-defined structures. The methodology forces proper consideration of solution alternatives and analysis of costs and benefits enabling informed choices to be made. The methodology is clear, defined, generally understood and measurable. Therefore, exceptions can be easily determined and corrected by management. Solutions respond efficiently to user requirements and there is awareness that forward looking solutions can improve business processes and the competitive solution.

5 Optimised The organisation's acquisition and implementation methodology has been subjected to continuous improvement and has kept in step with changes in technology. It has flexibility, allowing it to handle the range of projects from large-scale, organisation-wide applications to specific tactical projects. The methodology is supported by internal and external knowledge databases containing reference materials on technology solutions. The methodology itself produces computer based documentation in a pre-defined structure that makes production and maintenance very efficient. The organisation is often able to identify new opportunities to utilise technology to gain competitive advantage, influence business process re-engineering and improve overall efficiency.

AI2 Acquisition & Implementation
Acquire and Maintain Application Software

COBIT

Control over the IT process **Acquire and Maintain Application Software** with the business goal of *providing automated functions which effectively support the business process*

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

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

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

Information Criteria	
P	effectiveness
P	efficiency
	confidentiality
S	integrity
	availability
S	compliance
S	reliability

(**P**) primary (**S**) secondary

IT Resources	
	people
✓	applications
	technology
	facilities
	data

(✓) applicable to

Key Goal Indicators

- Number of applications delivered on time, meeting specifications and in line with the IT architecture
- Number of applications without integration problems during implementation
- Cost of maintenance per application below the set level
- Number of production problems, per application, causing visible downtime or service degradation
- Number of solutions not consistent with the currently approved IT strategy
- Reduced ratio of maintenance efforts relative to new development

Critical Success Factors

- The acquisition and implementation methodology is strongly supported by senior management
- Acquisition practices are clear, understood and accepted
- There is a formal, accepted, understood and enforced acquisition and implementation methodology
- An appropriate set of automated support tools is available, saving time on software selection by focusing on the best of breed
- There is separation between development and testing activities
- Key requirements are prioritised in view of possible scope reductions, if time, quality or cost cannot be compromised
- The approach taken and effort committed are related to the business relevance of the application
- The degree and form of documentation required is agreed upon and followed in the implementation
- Compliance with corporate IT architecture is monitored, including a formal process for approving deviations

Key Performance Indicators

- Ratio of actual maintenance cost per application versus the application portfolio average
- Average time to deliver functionality, based on measures such as function point or modules
- Number of change requests related to bugs, critical errors and new functional specifications
- Number of production problems or disfunctionality per application and per maintenance change
- Number of deviations from standard procedures, such as undocumented applications, unapproved design and testing reduced to meet deadlines
- Number of returned modules or level of rework required after acceptance testing
- Time lag to analyse and fix problems
- Number or percent of application software effectively documented for maintenance

AI2 Maturity Model

Control over the IT process **Acquire and Maintain Application Software** with the business goal of *providing automated functions which effectively support the business process*

0 Non-existent There is no process for designing and specifying applications. Typically, applications are obtained based on vendor driven offerings, brand recognition or IT staff familiarity with specific products, with little or no consideration of actual requirements.

1 Initial / Ad Hoc There is an awareness that a process for acquiring and maintaining applications is required. Approaches, however, vary from project to project without any consistency and typically in isolation from other projects. The organisation is likely to have acquired a variety of individual solutions and now suffers legacy problems and inefficiencies with maintenance and support. The business users are unable to gain much advantage from IT investments.

2 Repeatable but Intuitive There are similar processes for acquiring and maintaining applications, but they are based on the expertise within the IT function, not on a documented process. The success rate with applications depends greatly on the in-house skills and experience levels within IT. Maintenance is usually problematic and suffers when internal knowledge has been lost from the organisation.

3 Defined Process There are documented acquisition and maintenance processes. An attempt is made to apply the documented processes consistently across different applications and projects, but they are not always found to be practical to implement or reflective of current technology solutions. They are generally inflexible and hard to apply in all cases, so steps are frequently bypassed. As a consequence, applications are often acquired in a piecemeal fashion. Maintenance follows a defined approach, but is often time-consuming and inefficient.

4 Managed and Measurable There is a formal, clear and well-understood system acquisition and implementation methodology and policy that includes a formal design and specification process, criteria for acquisition of application software, a process for testing and requirements for documentation, ensuring that all applications are acquired and maintained in a consistent manner. Formal approval mechanisms exist to ensure that all steps are followed and exceptions are authorised. The methods have evolved so that they are well suited to the organisation and are likely to be positively used by all staff, and applicable to most application requirements.

5 Optimised Application software acquisition and maintenance practices are in line with the agreed processes. The approach is component based, with pre-defined, standardised applications matched to business needs. It is usual for organisation-wide approaches to be taken. The acquisition and maintenance process is well advanced, enables rapid deployment and allows for high responsiveness, as well as flexibility, in responding to changing business requirements. The application software acquisition and implementation process has been subjected to continuous improvement and is supported by internal and external knowledge databases containing reference materials and best practices. The methodology creates computer based documentation in a pre-defined structure that makes production and maintenance very efficient.

Control over the IT process **Acquire and Maintain Technology Infrastructure** with the business goal of *providing the appropriate platforms for supporting business applications*

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

is enabled by *judicious hardware acquisition, standardising on software, assessment of hardware and software performance, and consistent system administration*

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

Information Criteria	
P	effectiveness
P	efficiency
	confidentiality
S	integrity
	availability
	compliance
	reliability

(**P**) primary (**S**) secondary

IT Resources	
	people
	applications
✓	technology
	facilities
	data

(✓) applicable to

Critical Success Factors

- The acquisition and implementation methodology is strongly supported by senior management
- Acquisition practices are clear, understood and accepted
- There is ease of integration across different technology platforms
- Well articulated business strategy and related architectural requirements are defined and supported by senior management
- An up-to-date inventory of hardware and software infrastructure is available
- Relationships with vendors are well developed
- The ability exists to adequately establish the cost of overlap between different technology platforms
- Policies are defined to promote well considered choices between internal development, leveraging external infrastructures and outsourcing
- The selection process focuses on using reusable components
- Policies are defined to manage dependencies on single source suppliers
- There is coordination with the change management processes and systems
- A well defined life cycle methodology is used to select, acquire, maintain and remove infrastructure technology
- Acquisition duly considers performance and capacity requirements by integrating with capacity and performance management processes
- An appropriate set of automated support tools is available, saving time on selection by focusing on the best of breed

Key Goal Indicators

- Reduced number of platforms diverging from the agreed technology infrastructure
- Number of delays in systems implementation due to inadequate infrastructure
- Reduced ratio of maintenance efforts relative to new development
- Reduction of time to market of systems due to a predefined and flexible infrastructure
- Reduced downtime of infrastructure
- Reduced number of systems with serious interoperability problems
- Number of application performance problems related to inadequacies in the technology infrastructure

Key Performance Indicators

- Reduced number of different platforms
- Age of platforms
- Number of shared functions and resources
- Number and frequency of changes
- Number of breakdowns due to a lack of preventive maintenance
- Number of breakdowns due to system software changes
- Costs, based on effort and lapsed time, for major modification to system software or infrastructure

AI3 Maturity Model

Control over the IT process **Acquire and Maintain Technology Infrastructure** with the business goal of *providing the appropriate platforms for supporting business applications*

0 Non-existent Technology architecture is not recognised as a sufficiently important topic to be addressed.

1 Initial / Ad Hoc Changes to infrastructure are made for every new application without any overall plan. Although there is an awareness that the IT infrastructure is important, there is no consistent overall approach.

2 Repeatable but Intuitive There is a consistency between tactical approaches, when acquiring and maintaining the IT infrastructure; it is, however, not based on any defined strategy and does not consider the needs of the business applications that must be supported.

3 Defined Process A clear, defined and generally understood process for administering the IT infrastructure emerges. It supports the needs of critical business applications and is aligned to IT and business strategy. However, it is not possible to determine that the process is consistently applied and it is therefore not likely that the infrastructure fully supports the needs of the business applications. Outsourcing all or some of the IT infrastructure usually occurs in reaction to problems or specific opportunities.

4 Managed and Measurable The acquisition and maintenance process for technology infrastructure has developed to the point where it works well for most situations, is followed consistently within IT and is component based and focused on reusability. Attempts to make changes to the infrastructure without following agreed defined processes would be detected and prevented. It is likely that the IT infrastructure adequately supports the business applications. The process is well organised, but often reactive rather than proactive. The cost and lead-time to achieve the expected level of scalability, flexibility and integration is not optimised. Outsourcing all or some of the IT infrastructure is part of the tactical plan.

5 Optimised The acquisition and maintenance process for technology infrastructure is proactive and closely aligned with critical business applications and the technology architecture. Best practices regarding technology solutions are followed and the organisation is aware of the latest platform developments and management tools, including organisation-wide approaches and the need for increasing levels of reliability, availability and network security. Costs are reduced by rationalising and standardising infrastructure components and by using automation. The organisation maintains a high-level of technical awareness and can identify optimum ways to proactively improve performance, including consideration of outsourcing options. It is able to monitor and measure the performance of its existing infrastructure for timely detection of problems. The IT infrastructure is seen as the key enabler to leveraging the use of IT. Single-source supplier risks are actively managed.

Control over the IT process **Develop and Maintain Procedures** with the business goal of *ensuring the proper use of the applications and the technological solutions put in place*

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

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

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

Information Criteria
P effectiveness
P efficiency
confidentiality
S integrity
availability
S compliance
S reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
data

(✓) applicable to

Key Goal Indicators

- Number of applications where IT procedures are seamlessly integrated into business processes
- Number of technical solutions not adequately documented, including lack of user manuals, operations manuals and training materials
- Composite metric of the level of satisfaction with training material, user and operational documentation
- Reduced cost of producing and maintaining user documentation, operational procedures and training materials
- Proficiency levels of system users based on the percent of availability used

Critical Success Factors

- Well-defined service level agreements exist, with clear links to documentation standards
- The infrastructure and organisation are designed to promote and share user documentation, technical procedures and training material between trainers, help desk and user groups
- User training in use of procedures is integrated with the organisation and IT training plans
- Inventories of business processes, business procedures and IT procedures are maintained using automated tools
- The development process ensures the use of standard operating procedures and a standard look and feel
- A standard framework for documentation and procedures is defined and monitored
- Knowledge management, workflow techniques and automated tools are used to develop, distribute and maintain procedures

Key Performance Indicators

- Level of training attendance of users and operators for each application
- Accuracy of change requests and completeness of user documentation, IT procedures and training materials
- Time lag between changes and updates of training, procedures and documentation materials
- Satisfaction survey index with regard to training material, user procedures and operations procedures
- Reduction in number of training calls handled by the help desk
- Number of incidents caused by deficient documentation
- Number of applications with adequate user training

AI4 Maturity Model

Control over the IT process **Develop and Maintain Procedures** with the business goal of *ensuring the proper use of the applications and the technological solutions put in place*

0 Non-existent There is no process in place with regard to the production of user documentation, operations manuals and training material. The only materials that exist are those supplied with purchased products.

1 Initial / Ad Hoc The organisation is aware that a process addressing documentation is needed. Documentation is occasionally produced, but is dispersed in the organisation, inconsistent and only available to limited groups. Much of the documentation and procedures are out of date, and there is virtually no integration of procedures across different systems and business units. Training materials tend to be one-off schemes with variable quality, usually of a generic nature and often provided by third parties, without being customised for the organisation.

2 Repeatable but Intuitive Similar approaches are taken with regard to producing procedures and documentation, but they are not based on a structured approach or framework. User and operating procedures are documented, but there is no uniform approach and, therefore, their accuracy and availability relies to a large extent on individuals, rather than on a formal process. Training material is available, but tends also to be produced individually and quality depends on the individuals involved. Actual procedures and quality of user support therefore can vary from poor to very good, with very little consistency and integration across the organisation.

3 Defined Process There is a clearly defined, accepted and understood framework for user documentation, operations manuals and training materials. Procedures are stored and maintained in a formal library and can be accessed by anyone who needs to know. Corrections are made on a reactive basis. Procedures are available off-line and can be accessed and maintained in case of disaster. A process exists that specifies procedure updates and training materials to be an explicit deliverable of a change project. Despite the existence of defined approaches, the actual content varies because there is no control to enforce compliance with standards. Users are informally involved in the process. Automated tools are increasingly used in the generation and distribution of procedures.

4 Managed and Measurable Consistent compliance has improved the defined framework for maintaining procedures and training materials. The approach taken covers all systems and business units, so that processes can be viewed from a business perspective and are integrated to include interdependencies and interfaces. Controls exist to ensure that standards are adhered to and that procedures are developed and maintained for all processes. User feedback is collected and corrective actions are initiated when feedback scores are unacceptable. Hence, documentation and training materials are usually at a predictable, good level of reliability and availability. A formal process for using automated procedure documentation and management is implemented. Automated procedure development is increasingly integrated with application systems development, facilitating consistency and user access.

5 Optimised The process for user and operational documentation is constantly improved through the adoption of new tools or methods. The procedure materials are treated as a constantly evolving knowledge base which is maintained electronically using up-to-date knowledge management, workflow and distribution technologies, making it accessible and easy to maintain. The material is updated to reflect organisational, operational and software changes and is fully integrated into the business processes definition, thus supporting organisation-wide requirements, rather than only IT-oriented procedures.

Control over the IT process **Install and Accredit Systems** with the business goal of *verifying and confirming that the solution is fit for the intended purpose*

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

is enabled by *the realisation of a well-formalised installation, migration, conversion and acceptance plan*

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

Information Criteria
P effectiveness
efficiency
confidentiality
S integrity
S availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Critical Success Factors

- The acquisition and implementation methodology is established and consistently applied
- Resources are available to support a separate test environment and sufficient time is allowed for the test process
- Commitment and involvement of stakeholders is assured in the testing, training and transition processes
- Test data is available and representative of live data in kind and quantity, and the test environment reflects as close as possible the live environment
- A feedback mechanism is implemented for optimising and continuously improving the process
- Stress testing is performed for new systems before they are rolled out and regression testing is conducted for existing systems when changes are implemented
- Procedures for formally certifying and accrediting systems for security are consistently defined and adhered to
- There is clear understanding and verification of operational requirements

Key Goal Indicators

- Reduced number of missed installation and accreditation milestones
- Time to complete the installation and accreditation process, from beginning to the end of the security certification and accreditation process
- Reduced number of operational systems not accredited, in the instance where the process did not occur
- Number of changes to installed systems needed to optimise operations
- Number of changes required following system acceptance testing
- Number of findings during internal or external audits regarding the installation and accreditation process
- Number of changes required to correct problems after solutions are put into production

Key Performance Indicators

- Degree of stakeholder involvement in the installation and accreditation process
- Number of automated installation and accreditation processes
- Frequency of reporting of lessons learned
- Reported user satisfaction with the installation and accreditation process (lessons learned)
- Number of findings during the quality assurance review of installation and accreditation functions
- Reusability of the test platform

AI5 Maturity Model

Control over the IT process **Install and Accredit Systems** with the business goal of *verifying and confirming that the solution is fit for the intended purpose*

0 Non-existent There is a complete lack of formal installation or accreditation processes and senior management or IT staff does not recognise the need to verify that solutions are fit for the intended purpose.

1 Initial / Ad Hoc There is an awareness of the need to verify and confirm that implemented solutions serve the intended purpose. Testing is performed for some projects, but the initiative for testing is left to the individual project teams and the approaches taken vary. Formal accreditation and sign-off is rare or non-existent.

2 Repeatable but Intuitive There is some consistency between the testing and accreditation approaches, but they are not based on any methodology. The individual development teams normally decide the testing approach and there is usually an absence of integration testing. There is an informal approval process, not necessarily based on standardised criteria. Formal accreditation and sign-off is inconsistently applied.

3 Defined Process A formal methodology relating to installation, migration, conversion and acceptance is in place. However, management does not have the ability to assess compliance. IT installation and accreditation processes are integrated into the system life cycle and automated to some extent. Training, testing and transition to production status and accreditation are likely to vary from the defined process, based on individual decisions. The quality of systems entering production is inconsistent, with new systems often generating a significant level of post-implementation problems.

4 Managed and Measurable The procedures are formalised and developed to be well organised and practical with defined test environments and accreditation procedures. In practice, all major changes to systems follow this formalised approach. Evaluation of meeting user requirements is standardised and measurable, producing metrics that can be effectively reviewed and analysed by management. The quality of systems entering production is satisfactory to management, with reasonable levels of post-implementation problems. Automation of the process is ad hoc and project dependent. Neither post-implementation evaluations nor continuous quality reviews are consistently employed, although management may be satisfied with the current level of efficiency. The test system adequately reflects the live environment. Stress testing for new systems and regression testing for existing systems is applied for major projects.

5 Optimised The installation and accreditation processes have been refined to a level of best practice, based on the results of continuous improvement and refinement. IT installation and accreditation processes are fully integrated into the system life cycle and automated when advisable, facilitating the most efficient training, testing and transition to production status of new systems. Well-developed test environments, problem registers and fault resolution processes ensure efficient and effective transition to the production environment. Accreditation takes place usually with limited rework and post implementation problems are normally limited to minor corrections. Post-implementation reviews are also standardised, with lessons learned channelled back into the process to ensure continuous quality improvement. Stress testing for new systems and regression testing for amended systems is consistently applied.

AI6 Acquisition & Implementation
Manage Changes

Control over the IT process **Manage Changes** with the business goal of *minimising the likelihood of disruption, unauthorised alterations and errors*

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

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*

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

Information Criteria
P effectiveness
P efficiency
confidentiality
P integrity
P availability
compliance
S reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Critical Success Factors

- Change policies are clear and known and they are rigorously and systematically implemented
- Change management is strongly integrated with release management and is an integral part of configuration management
- There is a rapid and efficient planning, approval and initiation process covering identification, categorisation, impact assessment and prioritisation of changes
- Automated process tools are available to support workflow definition, pro-forma workplans, approval templates, testing, configuration and distribution
- Expedient and comprehensive acceptance test procedures are applied prior to making the change
- A system for tracking and following individual changes, as well as change process parameters, is in place
- A formal process for hand-over from development to operations is defined
- Changes take the impact on capacity and performance requirements into account
- Complete and up-to-date application and configuration documentation is available
- A process is in place to manage co-ordination between changes, recognising interdependencies
- An independent process for verification of the success or failure of change is implemented
- There is segregation of duties between development and production

Key Goal Indicators

- Reduced number of errors introduced into systems due to changes
- Reduced number of disruptions (loss of availability) caused by poorly managed change
- Reduced impact of disruptions caused by change
- Reduced level of resources and time required as a ratio to number of changes
- Number of emergency fixes

Key Performance Indicators

- Number of different versions installed at the same time
- Number of software release and distribution methods per platform
- Number of deviations from the standard configuration
- Number of emergency fixes for which the normal change management process was not applied retroactively
- Time lag between the availability of the fix and its implementation
- Ratio of accepted to refused change implementation requests

AI6 Maturity Model

Control over the IT process **Manage Changes** with the business goal of *minimising the likelihood of disruption, unauthorised alterations and errors*

0 **Non-existent** There is no defined change management process and changes can be made with virtually no control. There is no awareness that change can be disruptive for both IT and business operations, and no awareness of the benefits of good change management.

1 **Initial / Ad Hoc** It is recognised that changes should be managed and controlled, but there is no consistent process to follow. Practices vary and it is likely that unauthorised changes will take place. There is poor or non-existent documentation of change and configuration documentation is incomplete and unreliable. Errors are likely to occur together with interruptions to the production environment caused by poor change management.

2 **Repeatable but Intuitive** There is an informal change management process in place and most changes follow this approach; however, it is unstructured, rudimentary and prone to error. Configuration documentation accuracy is inconsistent and only limited planning and impact assessment takes place prior to a change. There is considerable inefficiency and rework.

3 **Defined Process** There is a defined formal change management process in place, including categorisation, prioritisation, emergency procedures, change authorisation and release management, but compliance is not enforced. The defined process is not always seen as suitable or practical and, as a result, workarounds take place and processes are bypassed. Errors are likely to occur and unauthorised changes will occasionally occur. The analysis of the impact of IT changes on business operations is becoming formalised, to support planned rollouts of new applications and technologies.

4 **Managed and Measurable** The change management process is well developed and consistently followed for all changes and management is confident that there are no exceptions. The process is efficient and effective, but relies on considerable manual procedures and controls to ensure that quality is achieved. All changes are subject to thorough planning and impact assessment to minimise the likelihood of post-production problems. An approval process for changes is in place. Change management documentation is current and correct, with changes formally tracked. Configuration documentation is generally accurate. IT change management planning and implementation is becoming more integrated with changes in the business processes, to ensure that training, organisational changes and business continuity issues are addressed. There is increased co-ordination between IT change management and business process re-design.

5 **Optimised** The change management process is regularly reviewed and updated to keep in line with best practices. Configuration information is computer based and provides version control. Software distribution is automated and remote monitoring capabilities are available. Configuration and release management and tracking of changes is sophisticated and includes tools to detect unauthorised and unlicensed software. IT change management is integrated with business change management to ensure that IT is an enabler in increasing productivity and creating new business opportunities for the organisation.

This page intentionally left blank

DELIVERY & SUPPORT

Control over the IT process **Define and Manage Service Levels** with the business goal of *establishing a common understanding of the level of service required*

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

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*

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

Information Criteria
P effectiveness
P efficiency
S confidentiality
S integrity
S availability
S compliance
S reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Sign-off by strategic business unit that service levels are aligned with key business objectives
- Customer satisfaction that the service level meets expectations
- Actual to budget cost ratio in line with service levels
- Percent of all critical business processes relying on IT covered by service level agreements
- Percent of service level agreements reviewed at the agreed interval or following major change
- Service level partners sign off service level monitoring information provided
- Percent of IT services which meet service level agreements

Critical Success Factors

- Service levels are expressed in end-user business terms, wherever possible
- Root cause analysis is performed when service levels breaches occur
- Skills and tools are available to provide useful and timely service level information
- The reliance of critical business processes on IT is defined and is covered by service level agreements
- IT management accountabilities and responsibilities are linked to service levels
- The IT organisation can identify sources of cost variances
- Detailed and consistent explanations for cost variances are provided
- A system for tracking and following individual changes is available

Key Performance Indicators

- Time lag of resolution of a service level change request
- Frequency of customer satisfaction surveys
- Time lag to resolve a service level issue
- Number of times that root cause analysis of service level procedure and subsequent resolution is completed within required period
- Significance of amount of additional funding needed to deliver the defined service level

DS1 Maturity Model

Control over the IT process **Define and Manage Service Levels** with the business goal of *establishing a common understanding of the level of service required*

0 Non-existent Management has not recognised the need for a process for defining service levels. Accountabilities and responsibilities for monitoring them are not assigned.

1 Initial / Ad Hoc There is awareness of the need to manage service levels, but the process is informal and reactive. The responsibility and accountability for monitoring performance is informally defined. Performance measurements are qualitative, with imprecisely defined goals. Performance reporting is infrequent and inconsistent.

2 Repeatable but Intuitive There are agreed-upon service level agreements, but they are informal and not revisited. Service level reporting is incomplete, irrelevant or misleading and dependent on the skills and initiative of individual managers. A service level co-ordinator is appointed with defined responsibilities, but not sufficient authority. The service level agreement compliance process is voluntary and not enforced.

3 Defined Process Responsibilities are well defined, but with discretionary authority. The service level agreement development process is in place with checkpoints for reassessing service levels and customer satisfaction. Service levels criteria are defined and agreed upon with users, with an increased level of standardisation. Service level shortfalls are identified, but resolution planning is still informal. The relationship between the funding provided and the expected service levels is being increasingly formalised. Service level is increasingly based on industry benchmarks and may not address organisation-specific needs.

4 Managed and Measurable Service levels are increasingly defined in the system requirements definition phase and incorporated into the design of the application and operational environments. Customer satisfaction is routinely measured and assessed. Performance measures are increasingly reflecting end-user needs, rather than only IT goals. User service levels measurement criteria are becoming standardised and reflective of industry norms. Root cause analysis is performed when service levels are not met. The reporting system for monitoring service levels is becoming increasingly automated. Operational and financial risks associated with not meeting agreed-upon service levels are defined and clearly understood.

5 Optimised Service levels are continuously reevaluated to ensure alignment of IT and business objectives, while taking advantage of technology advances and improvements in product price/performance ratios. All service level processes are subject to continuous improvement processes. Criteria for defining service levels are defined based on business criticality and include availability, reliability, performance, growth capacity, user support, continuity planning and security considerations. Customer satisfaction levels are monitored and enforced. Expected service levels are evaluated against industry norms, but also reflect the specific strategic goals of business units. IT management has the resources and accountability needed to meet service level performance targets and the executive compensation is structured to provide incentives for meeting the organisation goals.

Control over the IT process **Manage Third-party Services** with the business goal of *ensuring that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements*

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

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

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

Information Criteria
P effectiveness
P efficiency
S confidentiality
S integrity
S availability
S compliance
S reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Critical Success Factors

- Clearly-defined service requirements and performance measures exist
- The organisation retains accountability and control, and proactively manages external services
- The service provider has a mechanism in place to report on performance measures
- Third-party providers have a quality assurance programme in place
- All deliverables, including operational and performance requirements, are sufficiently defined and understood by all parties
- Effective change procedures for service requirements and performance measures are implemented
- Contracts are subject to successful legal review and sign-off
- There is provision for adequate management and administration, addressing financial, operations, legal and control issues
- The application of mutually agreed service level agreements is based on agreed upon associated rewards and penalties
- An internal contract manager is the single point of contact with the third party
- A Request for Proposal (RFP) process exists, with pre-established and agreed evaluation criteria
- A process is in place for classifying service problems based on their importance and the required responses

Key Goal Indicators

- Percent of service providers with formally agreed objectives
- Percent of significant agreements for which service provider qualification reviews are undertaken
- Percent of service providers that are formally qualified
- Number of third-party contractors with well-defined goals and expected deliverables
- Mutual satisfaction with the ongoing relationship
- Number of third-party contractors not meeting objectives or service levels
- Number and cost of disputes with third parties flowing from inadequate agreements or lack of performance against adequate agreements

Key Performance Indicators

- Number and frequency of review meetings
- Number of contract amendments
- Frequency of service level reports
- Number of outstanding issues
- Time lag for clearing issues
- Percent of contracts outstanding for legal review
- Time lag since the last contract review against market conditions
- Number of service contracts not using standard terms and conditions or approved exceptions

DS2 Maturity Model

Control over the IT process **Manage Third-party Services** with the business goal of *ensuring that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements*

0 **Non-existent** Responsibilities and accountabilities are not defined. There are no formal policies and procedures regarding contracting with third-parties. Third-party services are neither approved nor reviewed by management. There are no measurement activities and no reporting by third parties. In the absence of a contractual obligation for reporting, senior management is not aware of the quality of the service delivered.

1 **Initial / Ad Hoc** Management is aware of the need to have documented policies and procedures for third-party service procurement, including having signed contracts. There are no standard terms of agreement. Measurement of the service provided is informal and reactive. Practices are dependent on the experience of the individual and the commercial effectiveness of the supplier.

2 **Repeatable but Intuitive** The process for overseeing third-party service providers and the delivery of services is informal. A signed, pro-forma contract is used with standard vendor terms and conditions and description of services to be provided. Measurements are taken, but are not relevant. Reports are available, but do not support business objectives.

3 **Defined Process** Well documented procedures are in place to govern third-party procurement, with clear processes ensuring proper vetting and negotiating with vendors. The relationship with the third-party is purely a contractual one. The nature of the services to be provided is detailed in the contract and includes operational, legal and control requirements. Oversight responsibility for third-party-service delivery is assigned. Contractual terms are based on standardised templates. The business risk associated with the contract is assessed and reported.

4 **Managed and Measurable** Formal and standardised criteria are established for defining scope of work, services to be provided, deliverables, assumptions, time scales, costs, billing arrangements, responsibilities, business terms and conditions. Responsibilities for contract and vendor management are assigned. Vendor qualifications and capabilities are verified. Requirements are defined and linked to business objectives. A process exists to review service performance against contractual terms, providing input to current and future third-party service delivery. Transfer pricing models are used in the procurement process. All interested parties are aware of service, cost and milestone expectations.

5 **Optimised** The jointly signed contract is reviewed periodically after work starts. Responsibility for quality assurance of service delivery and vendor support is assigned. Evidence of compliance with operational, legal and control contract provisions is monitored and corrective action is enforced. The third party is subject to independent periodic review, with feedback based on the nature of the review. Selected measurements vary dynamically in response to changing business conditions. Measures support early detection of problems. Comprehensive, defined reporting is linked to the third-party compensation process. Reporting provides early warning of potential problems to facilitate timely resolution.

Control over the IT process **Manage Performance and Capacity** with the business goal of *ensuring that the adequate capacity is available and that best and optimal use is made of it to meet required performance needs*

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

is enabled by *data collection, analysis and reporting on resource performance, application sizing and workload demand*

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

Information Criteria	
P	effectiveness
P	efficiency
	confidentiality
	integrity
S	availability
	compliance
	reliability

(**P**) primary (**S**) secondary

IT Resources	
	people
✓	applications
✓	technology
✓	facilities
	data

(✓) applicable to

Key Goal Indicators

- Number of end-business processes suffering interruptions or outages caused by inadequate IT capacity and performance
- Number of critical business processes not covered by a defined service availability plan
- Percent of critical IT resources with adequate capacity and performance capability, taking account of peak loads

Critical Success Factors

- The performance and capacity implications of IT service requirements for all critical business processes are clearly understood
- Performance requirements are included in all IT development and maintenance projects
- Capacity and performance issues are dealt with at all appropriate stages in the system acquisition and deployment methodology
- The technology infrastructure is regularly reviewed to take advantage of cost/performance ratios and enable the acquisition of resources providing maximum performance capability at the lowest price
- Skills and tools are available to analyse current and forecasted capacity
- Current and projected capacity and usage information is made available to users and IT management in an understandable and usable form

Key Performance Indicators

- Number of down-time incidents caused by insufficient capacity or processing performance
- Percent of capacity remaining at normal and peak loads
- Time taken to resolve capacity problems
- Percent of unplanned upgrades compared with total number of upgrades
- Frequency of capacity adjustments to meet changing demands

DS3 Maturity Model

Control over the IT process **Manage Performance and Capacity** with the business goal of *ensuring that the adequate capacity is available and that best and optimal use is made of it to meet required performance needs*

0 Non-existent Management has not recognised that key business processes may require high levels of performance from IT or that the overall business need for IT services may exceed capacity. There is no capacity planning process in place.

1 Initial / Ad Hoc Performance and capacity management is reactive and sporadic. Users often have to devise work-arounds for performance and capacity constraints. There is very little appreciation of the IT service needs by the owners of the business processes. IT management is aware of the need for performance and capacity management, but the action taken is usually reactive or incomplete. The planning process is informal.

2 Repeatable but Intuitive Business management is aware of the impact of not managing performance and capacity. For critical areas, performance needs are generally catered for, based on assessment of individual systems and the knowledge of support and project teams. Some individual tools may be used to diagnose performance and capacity problems, but the consistency of results is dependent on the expertise of key individuals. There is no overall assessment of the IT infrastructure's performance capability or consideration of peak and worst-case loading situations. Availability problems are likely to occur in an unexpected and random fashion and take considerable time to diagnose and correct.

3 Defined Process Performance and capacity requirements are defined as steps to be addressed at all stages of the systems acquisition and deployment methodology. There are defined service level requirements and metrics that can be used to measure operational performance. It is possible to model and forecast future performance requirements. Reports can be produced giving performance statistics. Problems are still likely to occur and be time consuming to correct. Despite published service levels, end users will occasionally feel sceptical about the service capability.

4 Managed and Measurable Processes and tools are available to measure system usage and compare it to defined service levels. Up-to-date information is available, giving standardised performance statistics and alerting incidents such as insufficient capacity or throughput. Incidents caused by capacity and performance failures are dealt with according to defined and standardised procedures. Automated tools are used to monitor specific resources such as disk storage, network servers and network gateways. There is some attempt to report performance statistics in business process terms, so that end users can understand IT service levels. Users feel generally satisfied with current service capability and are demanding new and improved availability levels.

5 Optimised The performance and capacity plans are fully synchronised with the business forecasts and the operational plans and objectives. The IT infrastructure is subject to regular reviews to ensure that optimum capacity is achieved at the lowest possible cost. Advances in technology are closely monitored to take advantage of improved product performance. The metrics for measuring IT performance have been fine-tuned to focus on key areas and are translated into KGIs, KPIs and CFSs for all critical business processes. Tools for monitoring critical IT resources have been standardised, wherever possible, across platforms and linked to a single organisation-wide incident management system. Monitoring tools increasingly can detect and automatically correct performance problems, e.g., allocating increased storage space or re-routing network traffic. Trends are detected showing imminent performance problems caused by increased business volumes, enabling planning and avoidance of unexpected incidents. Users expect 24x7x365 availability.

Control over the IT process **Ensure Continuous Service** with the business goal of *making sure IT services are available as required and ensuring a minimum business impact in the event of a major disruption*

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

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*

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

Information Criteria
P effectiveness
S efficiency
confidentiality
integrity
P availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- No incidents causing public embarrassment
- Number of critical business processes relying on IT that have adequate continuity plans
- Regular and formal proof that the continuity plans work
- Reduced downtime
- Number of critical infrastructure components with automatic availability monitoring

Critical Success Factors

- A no-break power system is installed and regularly tested
- Potential availability risks are proactively detected and addressed
- Critical infrastructure components are identified and continuously monitored
- Continuous service provision is a continuum of advance capacity planning, acquisition of high-availability components, needed redundancy, existence of tested contingency plans and the removal of single points of failure
- Action is taken on the lessons learned from actual downtime incidents and test executions of contingency plans
- Availability requirements analysis is performed regularly
- Service level agreements are used to raise awareness and increase co-operation with suppliers for continuity needs
- The escalation process is clearly understood and based on a classification of availability incidents
- The business costs of interrupted service are specified and quantified where possible, providing the motivation to develop appropriate plans and arrange for contingency facilities

Key Performance Indicators

- Number of outstanding continuous service issues not resolved or addressed
- Number and extent of breaches of continuous service, using duration and impact criteria
- Time lag between organisational change and continuity plan update
- Time to diagnose an incident and decide on continuity plan execution
- Time to normalise the service level after execution of the continuity plan
- Number of proactive availability fixes implemented
- Lead time to address continuous service short-falls
- Frequency of continuous service training provided
- Frequency of continuous service testing

DS4 Maturity Model

Control over the IT process **Ensure Continuous Service** with the business goal of *making sure IT services are available as required and ensuring a minimum business impact in the event of a major disruption*

0 **Non-existent**. There is no understanding of the risks, vulnerabilities and threats to IT operations or the impact of loss of IT services to the business. Service continuity is not considered as needing management attention.

1 **Initial / Ad Hoc** Responsibilities for continuous service are informal, with limited authority. Management is becoming aware of the risks related to and the need for continuous service. The focus is on the IT function, rather than on the business function. Users are implementing work-arounds. The response to major disruptions is reactive and unprepared. Planned outages are scheduled to meet IT needs, rather than to accommodate business requirements.

2 **Repeatable but Intuitive** Responsibility for continuous service is assigned. The approaches to continuous service are fragmented. Reporting on system availability is incomplete and does not take business impact into account. There are no documented user or continuity plans, although there is commitment to continuous service availability and its major principles are known. A reasonably reliable inventory of critical systems and components exists. Standardisation of continuous service practices and monitoring of the process is emerging, but success relies on individuals.

3 **Defined Process** Accountability is unambiguous and responsibilities for continuous service planning and testing are clearly defined and assigned. Plans are documented and based on system criticality and business impact. There is periodic reporting of continuous service testing. Individuals take the initiative for following standards and receiving training. Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.

4 **Managed and Measurable** Responsibilities and standards for continuous service are enforced. Responsibility for maintaining the continuous service plan is assigned. Maintenance activities take into account the changing business environment, the results of continuous service testing and best internal practices. Structured data about continuous service is being gathered, analysed, reported and acted upon. Training is provided for continuous service processes. System redundancy practices, including use of high-availability components, are being consistently deployed. Redundancy practices and continuous service planning influence each other. Discontinuity incidents are classified and the increasing escalation path for each is well known to all involved.

5 **Optimised** Integrated continuous service processes are proactive, self-adjusting, automated and self-analytical and take into account benchmarking and best external practices. Continuous service plans and business continuity plans are integrated, aligned and routinely maintained. Buy-in for continuous service needs is secured from vendors and major suppliers. Global testing occurs and test results are fed back as part of the maintenance process. Continuous service cost effectiveness is optimised through innovation and integration. Gathering and analysis of data is used to identify opportunities for improvement. Redundancy practices and continuous service planning are fully aligned. Management does not allow single points of failure and provides support for their remedy. Escalation practices are understood and thoroughly enforced.

Control over the IT process **Ensure Systems Security** with the business goal of *safeguarding information against unauthorised use, disclosure or modification, damage or loss*

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

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

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

Information Criteria	
	effectiveness
	efficiency
P	confidentiality
P	integrity
S	availability
S	compliance
S	reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Critical Success Factors

- An overall security plan is developed that covers the building of awareness, establishes clear policies and standards, identifies a cost-effective and sustainable implementation, and defines monitoring and enforcement processes
- There is awareness that a good security plan takes time to evolve
- The corporate security function reports to senior management and is responsible for executing the security plan
- Management and staff have a common understanding of security requirements, vulnerabilities and threats, and they understand and accept their own security responsibilities
- Third-party evaluation of security policy and architecture is conducted periodically
- A "building permit" programme is defined, identifying security baselines that have to be adhered to
- A "drivers licence" programme is in place for those developing, implementing and using systems, enforcing security certification of staff
- The security function has the means and ability to detect, record, analyse significance, report and act upon security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring
- A centralised user management process and system provides the means to identify and assign authorisations to users in a standard and efficient manner
- A process is in place to authenticate users at reasonable cost, light to implement and easy to use

Key Goal Indicators

- No incidents causing public embarrassment
- Immediate reporting on critical incidents
- Alignment of access rights with organisational responsibilities
- Reduced number of new implementations delayed by security concerns
- Full compliance, or agreed and recorded deviations from minimum security requirements
- Reduced number of incidents involving unauthorised access, loss or corruption of information

Key Performance Indicators

- Reduced number of security-related service calls, change requests and fixes
- Amount of downtime caused by security incidents
- Reduced turnaround time for security administration requests
- Number of systems subject to an intrusion detection process
- Number of systems with active monitoring capabilities
- Reduced time to investigate security incidents
- Time lag between detection, reporting and acting upon security incidents
- Number of IT security awareness training days

DS5 Maturity Model

Control over the IT process **Ensure Systems Security** with the business goal of *safeguarding information against unauthorised use, disclosure or modification, damage or loss*

0 Non-existent The organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process to IT security breaches. There is a complete lack of a recognisable system security administration process.

1 Initial / Ad Hoc The organisation recognises the need for IT security, but security awareness depends on the individual. IT security is addressed on a reactive basis and not measured. IT security breaches invoke "finger pointing" responses if detected, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator with no management authority. Security awareness is fragmented and limited. IT security information is generated, but is not analysed. Security solutions tend to respond reactively to IT security incidents and by adopting third-party offerings, without addressing the specific needs of the organisation. Security policies are being developed, but inadequate skills and tools are still being used. IT security reporting is incomplete, misleading or not pertinent.

3 Defined Process Security awareness exists and is promoted by management. Security awareness briefings have been standardised and formalised. IT security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for IT security are assigned, but not consistently enforced. An IT security plan exists, driving risk analysis and security solutions. IT security reporting is IT focused, rather than business focused. Ad hoc intrusion testing is performed.

4 Managed and Measurable Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Security awareness briefings have become mandatory. User identification, authentication and authorisation are being standardised. Security certification of staff is being established. Intrusion testing is a standard and formalised process leading to improvements. Cost/benefit analysis, supporting the implementation of security measures, is increasingly being utilised. IT security processes are co-ordinated with the overall organisation security function. IT security reporting is linked to business objectives.

5 Optimised IT security is a joint responsibility of business and IT management and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimised and included in a verified security plan. Security functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. IT security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analysed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and pro-active identification of risk is the basis for continuous improvements. Security processes and technologies are integrated organisation wide.

Control over the IT process **Identify and Allocate Costs** with the business goal of *ensuring a correct awareness of the costs attributable to IT services*

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

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*

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

Information Criteria	
	effectiveness
P	efficiency
	confidentiality
	integrity
	availability
	compliance
P	reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Continued cost optimisation of information services by the IT function
- Continued cost optimisation of information services by users
- Increased ratio of proven benefits to actual costs of IT services
- Index of efficiency, based on a comparison of internal with external provider costs
- Business management understanding/acceptance of IT costs and service levels

Critical Success Factors

- End-users, business process owners and the IT organisation share a common understanding of costing requirements and cost allocation
- Direct and indirect costs are identified, captured, reported and analysed in a timely and automated manner
- Costs are charged back on the basis of utilisation and recorded in charge-back principles that are formally accepted and regularly re-assessed
- Cost reporting is used by all parties to review budget performance, to identify cost optimisation opportunities and to benchmark performance against reliable sources
- There is a direct link between the cost of the service and the service level agreements
- The results of cost allocation and optimisation are used to verify benefit realisation and are fed back into the next budget cycle

Key Performance Indicators

- Percentage of variance between budgets, forecasts and actual costs
- Percentage reduction in information service rates
- Percentage increase in optimisation of user service requests
- Percentage increase in optimisation of IT resources usage
- Number of cost optimisation initiatives

DS6 Maturity Model

Control over the IT process **Identify and Allocate Costs** with the business goal of *ensuring a correct awareness of the costs attributable to IT services*

0 Non-existent There is a complete lack of any recognisable process for identifying and allocating costs with respect to information services provided. The organisation has not even recognised that there is an issue to be addressed with respect to cost accounting and there is no communication about the issue.

1 Initial / Ad Hoc There is a general understanding of the overall costs for information services, but there is no breakdown of costs per user, department, groups of users, service functions, projects or deliverables. There is virtually no cost monitoring, with only aggregate cost reporting to management. There is no charge-back process or system in place to bill users for costs incurred in delivering information services.

2 Repeatable but Intuitive There is overall awareness of the need to identify and allocate costs. Cost allocation is based on informal or rudimentary cost assumptions, e.g., hardware costs, and there is virtually no linking to value drivers. Cost allocation processes are repeatable and some of them begin to be monitored. There is no formal training and communication on standard cost identification and allocation procedures. Responsibility is not assigned.

3 Defined Process There is a defined and documented information services cost model. The model is institutionalised and communicated, and informal training is established. An appropriate level of awareness exists of the costs attributable to information services. An automated cost accounting system exists, but is focused on the information services function rather than on business processes.

4 Managed and Measurable Information services cost management responsibilities and accountabilities are defined and fully understood at all levels and are supported by formal training. Direct and indirect costs are identified and reported in a timely and automated manner to management, business process owners and users. Generally, there is cost monitoring and evaluation, and actions are taken when processes are not working effectively or efficiently. Action is taken in many, but not all cases. Cost management processes are continuously being improved and enforce best internal practice. Information services cost reporting is linked to business objectives and service level agreements. There is involvement of all required internal cost management experts.

5 Optimised Costs of services provided are identified, captured, summarised and reported to management, business process owners and users. Costs are identified as chargeable items and support a charge-back system that appropriately bills users for services provided, based on utilisation. Cost details support service level agreements. There is strong monitoring and evaluation of costs of services, where variances from budget amounts are identified and discrepancies are detailed and appropriately acted upon. Cost figures obtained are used to verify benefit utilisation and are used in the organisation's budgeting process. Information services cost reporting provides early warning of changing business requirements through intelligent reporting systems. A variable cost model is utilised, derived from volumes processed for each service provided. Cost management has been refined to a level of best practices, based on the result of continuous improvement and maturity modelling with other organisations. External experts are leveraged and benchmarks are used for cost management guidance.

Control over the IT process **Educate and Train Users** with the business goal of *ensuring that users are making effective use of technology and are aware of the risks and responsibilities involved*

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

is enabled by *a comprehensive training and development plan*

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

Information Criteria
P effectiveness
S efficiency
confidentiality
integrity
availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
applications
technology
facilities
data

(✓) applicable to

Key Goal Indicators

- Measured improvement in employee optimisation of IT resources to maximise business value
- Measured improvement in employee awareness of ethical conduct requirements, system security principles and performance of duties in an ethical and secure manner
- Measured improvement in security practices to protect against harm from failures affecting availability, confidentiality and integrity
- Number of help desk calls for training or to answer questions
- Increased user satisfaction with roll out of new technologies

Critical Success Factors

- A comprehensive education and training program, focused on individual and corporate needs, is in place
- The education and training programs are supported by budgets, resources, facilities and trainers
- Training and education are critical components of the employee career paths
- Employees and managers identify and document training needs
- Needed training is provided in a timely manner
- There is senior management support to ensure that employees perform their duties in an ethical and secure manner
- Employees receive system security practices training in protecting against harm from failures affecting availability, confidentiality and integrity
- Corporate policy requires that all employees receive a basic training program covering ethical conducts, system security practices and permitted use of IT resources
- There is management acceptance that training costs are investments in lowering the total costs of technology ownership

Key Performance Indicators

- Percentage of employees trained
- Age of employee training curricula
- Time lag between identification of training need and the delivery of the training
- Number of training alternatives available to employees from in-house and third-party sources
- Percentage of employees trained in ethical conduct requirements
- Number of identified employee ethical violations
- Percentage of employees trained in security practices
- Number of identified security incidents related to employees
- Increased identification and documentation of training needs and delivery of timely training

DS7 Maturity Model

Control over the IT process **Educate and Train Users** with the business goal of *ensuring that users are making effective use of technology and are aware of the risks and responsibilities involved*

0 Non-existent There is a complete lack of any training and education program. The organisation has not even recognised there is an issue to be addressed with respect to training and there is no communication on the issue.

1 Initial / Ad Hoc There is evidence that the organisation has recognised the need for a training and education program, but there are no standardised processes. In the absence of an organised program, employees have been identifying and attending training courses on their own. Some of these training courses have addressed the issues of ethical conduct, system security awareness and security practices. The overall management approach lacks any cohesion and there is only sporadic and inconsistent communication on issues and approaches to address training and education.

2 Repeatable but Intuitive There is awareness of the need for a training and education program and for associated processes throughout the organisation. Training is beginning to be identified in the individual performance plans of employees. Processes have developed to the stage where informal training and education classes are taught by different instructors, while covering the same subject matter with different approaches. Some of the classes address the issues of ethical conduct and system security awareness and practices. There is high reliance on the knowledge of individuals. However, there is consistent communication on the overall issues and the need to address them.

3 Defined Process The training and education program has been institutionalised and communicated, and employees and managers identify and document training needs. Training and education processes have been standardised and documented. Budgets, resources, facilities and trainers are being established to support the training and education program. Formal classes are given to employees in ethical conduct and in system security awareness and practices. Most training and education processes are monitored, but not all deviations are likely to be detected by management. Analysis of training and education problems is only occasionally applied.

4 Managed and Measurable There is a comprehensive training and education program that is focused on individual and corporate needs and yields measurable results. Responsibilities are clear and process ownership is established. Training and education is a component of employee career paths. Management supports and attends training and educational sessions. All employees receive ethical conduct and system security awareness training. All employees receive the appropriate level of system security practices training in protecting against harm from failures affecting availability, confidentiality and integrity. Management monitors compliance by constantly reviewing and updating the training and education program and processes. Processes are under improvement and enforce best internal practices.

5 Optimised Training and education result in an improvement of individual performance. Training and education are critical components of the employee career paths. Sufficient budgets, resources, facilities and instructors are provided for the training and education programs. Processes have been refined and are under continuous improvement, taking advantage of best external practices and maturity modelling with other organisations. All problems and deviations are analysed for root causes and efficient action is expediently identified and taken. There is a positive attitude with respect to ethical conduct and system security principles. IT is used in an extensive, integrated and optimised manner to automate and provide tools for the training and education program. External training experts are leveraged and benchmarks are used for guidance.

Control over the IT process **Assist and Advise Customers** with the business goal of *ensuring that any problem experienced by the user is appropriately resolved*

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

is enabled by *a help desk facility which provides first-line support and advice*

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

Information Criteria
P effectiveness
P efficiency
confidentiality
integrity
availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
technology
facilities
data

(✓) applicable to

Critical Success Factors

- Up-to-date and easily accessible Frequently Asked Questions (FAQs) and their answers are available
- Knowledgeable and customer-oriented support staff resolve problems in close co-operation with the problem management staff
- All user inquiries are consistently and thoroughly registered by the help desk
- User inquiries that cannot be resolved in a timely manner are appropriately escalated
- The clearance of user inquiries is monitored
- User questions are resolved in a timely manner
- Those user inquiries that cannot be resolved in a timely manner are investigated and acted upon
- Management monitors trends to identify root causes in a proactive manner and follows up with analysis and the development of sustainable solutions
- Corporate policies and programs are defined for training users in technology use and security practices
- There is management awareness of the cost of support services and user downtime and of the need to take action on root-cause issues
- Support costs are charged back to the business using simple tools and clear policies

Key Goal Indicators

- Reduced average time to resolve problems
- Reduced repetitive inquiries on solved problems
- Increased user satisfaction with the effectiveness and efficiency of the help desk
- Increased user confidence in the services of the help desk
- Improved efficiency measured by reduced help desk resources in relation to systems supported
- Percent of problems resolved at first contact
- Elapsed time per call

Key Performance Indicators

- Number of repeat inquiries
- Number of escalations
- Number of inquiries
- Time to resolve inquiries
- Reduced trends in user inquiries requiring problem resolution
- Cost per call

DS8 Maturity Model

Control over the IT process **Assist and Advise Customers** with the business goal of *ensuring that any problem experienced by the user is appropriately resolved*

0 **Non-existent** There is no support to resolve user questions and problems. There is a complete lack of a help desk function. The organisation has not recognised there is an issue to be addressed.

1 **Initial / Ad Hoc** The organisation has recognised that a process supported by tools and personnel is required in order to respond to user queries and manage problem resolution. There is, however, no standardised process and only reactive support is provided. Management does not monitor user queries, problems or trends. There is no escalation process to ensure that problems are resolved.

2 **Repeatable but Intuitive** There is organisational awareness of the need for a help desk function. Assistance is available on an informal basis through a network of knowledgeable individuals. These individuals have some common tools available to assist in problem resolution. There is no formal training and communication on standard procedures, and responsibility is left to the individual. However, there is consistent communication on the overall issues and the need to address them.

3 **Defined Process** The need for a help desk function is recognised and accepted. Procedures have been standardised and documented and informal training is occurring. It is, however, left to the individual to get training and to follow the standards. Frequently Asked Questions (FAQs) and user guidelines are developed, but individuals must find them and may not follow them. Queries and problems are tracked on a manual basis and individually monitored, but a formal reporting system does not exist. Problem escalation is just emerging. The timely response to queries and problems is not measured and problems may go unresolved.

4 **Managed and Measurable** There is a full understanding of the benefits of a help desk at all levels of the organisation and the function has been established in appropriate organisational units. The tools and techniques are automated with a centralised knowledge base of problems and solutions. The help desk staff closely interacts with the problem management staff. The responsibilities are clear and effectiveness is monitored. Procedures for communicating, escalating, and resolving problems are established and communicated. Help desk personnel are trained and processes are improved through the use of task-specific software. Root causes of problems are identified and trends are reported, resulting in timely correction of problems. Processes are under improvement and enforce best internal practice.

5 **Optimised** The help desk function is established, well organised and takes on a customer service orientation, by being knowledgeable, customer focussed and helpful. Extensive, comprehensive FAQs are an integral part of the knowledge base. Tools are in place to enable a user to self-diagnose and resolve problems. IT is used to create, manage and improve access to automated knowledge bases that support problem resolution. Advice is consistent and problems are resolved quickly within a structured escalation process. Management utilises a pro-active notification process and trend analysis to prevent and monitor problems. Processes have been refined to the level of best external practices, based on the results of continuous improvement and maturity modelling with other organisations.

Control over the IT process **Manage the Configuration** with the business goal of *accounting for all IT components, prevent unauthorised alteration, verify physical existence and provide a basis for sound change management*

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

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

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

Information Criteria	
P	effectiveness
	efficiency
	confidentiality
	integrity
S	availability
	compliance
S	reliability

(**P**) primary (**S**) secondary

IT Resources	
	people
✓	applications
✓	technology
✓	facilities
	data

(✓) applicable to

Critical Success Factors

- Owners are established for all configuration elements and are responsible for maintaining the inventory and controlling change
- Configuration information is maintained and accessible, based on up-to-date inventories and a comprehensive naming convention
- An appropriate software library structure is in place, addressing the needs of development, testing and production environments
- There exists a release management policy and a system to enforce it
- Record keeping and physical custody duties are kept segregated
- There is integration with procurement and change management processes
- Vendor catalogues and configuration are aligned
- Configuration baselines exist, identifying the minimum standard components and integration requirements, consistency and integration criteria
- An automatic configuration detection and checking mechanism is available
- An automatic distribution and upgrade process is implemented
- There is zero tolerance for illegal software

Key Goal Indicators

- Percent of IT configuration identified and accounted for
- Reduction in number of variances between accounts and physical situation
- Quality index of information, including interrelationships, age, changes applied, status and related problems criteria
- Usage index of information for proactive actions, including preventive maintenance and upgrade criteria

Key Performance Indicators

- Percent of configuration components for which data is kept and updated automatically
- Frequency of physical verifications
- Frequency of exception analysis, addressing redundancy, obsolescence and correction of configuration
- Time lag between modification to the configuration and the update of records
- Number of releases
- Percent of reactionary changes

DS9 Maturity Model

Control over the IT process **Manage the Configuration** with the business goal of *accounting for all IT components, prevent unauthorised alteration, verify physical existence and provide a basis for sound change management*

0 **Non-existent** Management does not have an appreciation of the benefits of having a process in place that is capable of reporting on and managing the IT infrastructure, for either hardware or software configurations.

1 **Initial / Ad Hoc** The need for configuration management is recognised. Basic configuration management tasks, such as maintaining inventories of hardware and software, are performed on an individual basis. No standard practices are applied.

2 **Repeatable but Intuitive** Management is aware of the benefits of controlling the IT configuration but there is implicit reliance on technical personnel knowledge and expertise. Configuration management tools are being employed to a certain degree, but differ among platforms. Moreover, no standard working practices have been defined. Configuration data content is limited and not used by interrelated processes, such as change management and problem management.

3 **Defined Process** The need for accurate and complete configuration information is understood and enforced. The procedures and working practices have been documented, standardised and communicated, but training and application of the standards is up to the individual. In addition, similar configuration management tools are being implemented across platforms. Deviations from procedures are unlikely to be detected and physical verifications are performed inconsistently. Some automation occurs to assist in tracking equipment and software changes. Configuration data is being used by interrelated processes.

4 **Managed and Measurable** The need to manage the configuration is recognised at all levels of the organisation and best practices continue to evolve. Procedures and standards are communicated and incorporated into training and deviations are monitored, tracked and reported. Automated tools are utilised, such as 'push' technology, to enforce standards and improve stability. Configuration management systems do cover most of the IT infrastructure and allow for proper release management and distribution control. Exception analysis, as well as physical verifications, are consistently applied and their root causes are investigated.

5 **Optimised** All infrastructure components are managed within the configuration management system, which contains all necessary information about components and their interrelationships. The configuration data is aligned with vendor catalogues. Interrelated processes are fully integrated and use as well as update configuration data. Baseline audit reports provide essential hardware and software data for repair, service, warranty, upgrade and technical assessments of each individual unit. Authorised software installation rules are enforced. Management forecasts repairs and upgrades from analysis reports providing scheduled upgrades and technology refreshment capabilities. Asset tracking and monitoring of individual workstations protects assets and prevents theft, misuse and abuse.

Control over the IT process **Manage Problems and Incidents** with the business goal of *ensuring that problems and incidents are resolved, and the cause investigated to prevent any recurrence*

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

is enabled by *a problem management system which records and progresses all incidents*

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

Information Criteria
P effectiveness
P efficiency
confidentiality
integrity
S availability
compliance
reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- A measured reduction of the impact of problems and incidents on IT resources
- A measured reduction in the elapsed time from initial symptom report to problem resolution
- A measured reduction in unresolved problems and incidents
- A measured increase in the number of problems avoided through pre-emptive fixes
- Reduced time lag between identification and escalation of high-risk problems and incidents

Critical Success Factors

- There is clear integration of problem management with availability and change management
- Accessibility to configuration data, as well as the ability to keep track of problems for each configuration component, is provided
- An accurate means of communicating problem incidents, symptoms, diagnosis and solutions to the proper support personnel is in place
- Accurate means exist to communicate to users and IT the exceptional events and symptoms that need to be reported to problem management
- Training is provided to support personnel in problem resolution techniques
- Up-to-date roles and responsibilities charts are available to support incident management
- There is vendor involvement during problem investigation and resolution
- Post-facto analysis of problem handling procedures is applied

Key Performance Indicators

- Elapsed time from initial symptom recognition to entry in the problem management system
- Elapsed time between problem recording and resolution or escalation
- Elapsed time between evaluation and application of vendor patches
- Percent of reported problems with already known resolution approaches
- Frequency of coordination meetings with change management and availability management personnel
- Frequency of component problem analysis reporting
- Reduced number of problems not controlled through formal problem management

DS10 Maturity Model

Control over the IT process **Manage Problems and Incidents** with the business goal of *ensuring that problems and incidents are resolved, and the cause investigated to prevent any recurrence*

0 **Non-existent** There is no awareness of the need for managing problems and incidents. The problem-solving process is informal and users and IT staff deal individually with problems on a case-by-case basis.

1 **Initial / Ad Hoc** The organisation has recognised that there is a need to solve problems and evaluate incidents. Key knowledgeable individuals provide some assistance with problems relating to their area of expertise and responsibility. The information is not shared with others and solutions vary from one support person to another, resulting in additional problem creation and loss of productive time, while searching for answers. Management frequently changes the focus and direction of the operations and technical support staff.

2 **Repeatable but Intuitive** There is a wide awareness of the need to manage IT related problems and incidents within both the business units and information services function. The resolution process has evolved to a point where a few key individuals are responsible for managing the problems and incidents occurring. Information is shared among staff; however, the process remains unstructured, informal and mostly reactive. The service level to the user community varies and is hampered by insufficient structured knowledge available to the problem solvers. Management reporting of incidents and analysis of problem creation is limited and informal.

3 **Defined Process** The need for an effective problem management system is accepted and evidenced by budgets for the staffing, training and support of response teams. Problem solving, escalation and resolution processes have been standardised, but are not sophisticated. Nonetheless, users have received clear communications on where and how to report on problems and incidents. The recording and tracking of problems and their resolutions is fragmented within the response team, using the available tools without centralisation or analysis. Deviations from established norms or standards are likely to go undetected.

4 **Managed and Measurable** The problem management process is understood at all levels within the organisation. Responsibilities and ownership are clear and established. Methods and procedures are documented, communicated and measured for effectiveness. The majority of problems and incidents are identified, recorded, reported and analysed for continuous improvement and are reported to stakeholders. Knowledge and expertise are cultivated, maintained and developed to higher levels as the function is viewed as an asset and major contributor to the achievement of IT objectives. The incident response capability is tested periodically. Problem and incident management is well integrated with interrelated processes, such as change, availability and configuration management, and assists customers in managing data, facilities and operations.

5 **Optimised** The problem management process has evolved into a forward-looking and proactive one, contributing to the IT objectives. Problems are anticipated and may even be prevented. Knowledge is maintained, through regular contacts with vendors and experts, regarding patterns of past and future problems and incidents. The recording, reporting and analysis of problems and resolutions is automated and fully integrated with configuration data management. Most systems have been equipped with automatic detection and warning mechanism, which are continuously tracked and evaluated.

Control over the IT process **Manage Data** with the business goal of *ensuring that data remains complete, accurate and valid during its input, update and storage*

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

is enabled by *an effective combination of application and general controls over the IT operations*

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

Information Criteria	
	effectiveness
	efficiency
	confidentiality
P	integrity
	availability
	compliance
P	reliability

(**P**) primary (**S**) secondary

IT Resources	
	people
	applications
	technology
	facilities
✓	data

(✓) applicable to

Critical Success Factors

- Data entry requirements are clearly stated, enforced and supported by automated techniques at all levels, including database and file interfaces
- The responsibilities for data ownership and integrity requirements are clearly stated and accepted throughout the organisation
- Data accuracy and standards are clearly communicated and incorporated into the training and personnel development processes
- Data entry standards and correction are enforced at the point of entry
- Data input, processing and output integrity standards are formalised and enforced
- Data is held in suspense until corrected
- Effective detection methods are used to enforce data accuracy and integrity standards
- Effective translation of data across platforms is implemented without loss of integrity or reliability to meet changing business demands
- There is a decreased reliance on manual data input and re-keying processes
- Efficient and flexible solutions promote effective use of data
- Data is archived and protected and is readily available when needed for recovery

Key Goal Indicators

- A measured reduction in the data preparation process and tasks
- A measured improvement in the quality, timeline and availability of data
- A measured increase in customer satisfaction and reliance upon the data
- A measured decrease in corrective activities and exposure to data corruption
- Reduced number of data defects, such as redundancy, duplication and inconsistency
- No legal or regulatory data compliance conflicts

Key Performance Indicators

- Percent of data input errors
- Percent of updates reprocessed
- Percent of automated data integrity checks incorporated into the applications
- Percent of errors prevented at the point of entry
- Number of automated data integrity checks run independently of the applications
- Time interval between error occurrence, detection and correction
- Reduced data output problems
- Reduced time for recovery of archived data

DS11 Maturity Model

Control over the IT process **Manage Data** with the business goal of *ensuring that data remains complete, accurate and valid during its input, update and storage*

0 Non-existent Data is not recognised as a corporate resource and asset. There is no assigned data ownership or individual accountability for data integrity and reliability. Data quality and security is poor or non-existent.

1 Initial / Ad Hoc The organisation recognises a need for accurate data. Some methods are developed at the individual level to prevent and detect data input, processing and output errors. The process of error identification and correction is dependent upon manual activities of individuals, and rules and requirements are not passed on as staff movement and turnover occur. Management assumes that data is accurate because a computer is involved in the process. Data integrity and security are not management requirements and, if security exists, it is administered by the information services function.

2 Repeatable but Intuitive The awareness of the need for data accuracy and maintaining integrity is prevalent throughout the organisation. Data ownership begins to occur, but at a department or group level. The rules and requirements are documented by key individuals and are not consistent across the organisation and platforms. Data is in the custody of the information services function and the rules and definitions are driven by the IT requirements. Data security and integrity are primarily the information services function's responsibilities, with minor departmental involvement.

3 Defined Process The need for data integrity within and across the organisation is understood and accepted. Data input, processing and output standards have been formalised and are enforced. The process of error identification and correction is automated. Data ownership is assigned, and integrity and security are controlled by the responsible party. Automated techniques are utilised to prevent and detect errors and inconsistencies. Data definitions, rules and requirements are clearly documented and maintained by a database administration function. Data becomes consistent across platforms and throughout the organisation. The information services function takes on a custodian role, while data integrity control shifts to the data owner. Management relies on reports and analyses for decisions and future planning.

4 Managed and Measurable Data is defined as a corporate resource and asset, as management demands more decision support and profitability reporting. The responsibility for data quality is clearly defined, assigned and communicated within the organisation. Standardised methods are documented, maintained and used to control data quality, rules are enforced and data is consistent across platforms and business units. Data quality is measured and customer satisfaction with information is monitored. Management reporting takes on a strategic value in assessing customers, trends and product evaluations. Integrity of data becomes a significant factor, with data security recognised as a control requirement. A formal, organisation-wide data administration function has been established, with the resources and authority to enforce data standardisation.

5 Optimised Data management is a mature, integrated and cross-functional process that has a clearly defined and well-understood goal of delivering quality information to the user, with clearly defined integrity, availability and reliability criteria. The organisation actively manages data, information and knowledge as corporate resources and assets, with the objective of maximising business value. The corporate culture stresses the importance of high quality data that needs to be protected and treated as a key component of intellectual capital. The ownership of data is a strategic responsibility with all requirements, rules, regulations and considerations clearly documented, maintained and communicated.

Control over the IT process **Manage Facilities** with the business goal of *providing a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards*

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

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

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

Information Criteria	
	effectiveness
	efficiency
	confidentiality
P	integrity
P	availability
	compliance
	reliability

(**P**) primary (**S**) secondary

IT Resources	
	people
	applications
	technology
✓	facilities
	data

(✓) applicable to

Critical Success Factors

- A strategy and standards are defined for all facilities, covering site selection, construction, guarding, personnel safety, mechanical and electrical systems, fire, lightning and flooding protection
- The facilities strategy and standards are aligned with IT services availability targets and information security policies, and integrated with business continuity planning and crisis management
- Facilities are regularly monitored using automated systems with clear tolerances and audit logs, CCTV (Close Circuit Television) and intrusion detection systems where necessary, as well as through physical inspections and audits
- There is strict adherence to preventive maintenance schedules and strict discipline in the housekeeping of facilities
- Physical access is rigourously monitored and based on need-to-be and zoning principles, with identification authorisation and exception procedures where needed
- There are good relationships and exchanges of information with law enforcement, fire brigade and other local authorities
- Clear, concise and up-to-date detection, inspection and escalation procedures exist, supported by a training programme

Key Goal Indicators

- A reduction in the number of facilities and physical security incidents, including theft, damage, disclosure, outage, health and safety problems
- A reduction in the amount of downtime due to outage of utilities
- A measured adherence to applicable laws and regulation
- A measured adherence to insurance policy requirements
- A measured improvement in the cost/risk ratio

Key Performance Indicators

- Complete inventory and maps with identification of single points of failure
- Frequency of training of personnel in safety, facilities and security measures
- Frequency of testing of fire alarm and evacuation plans
- Frequency of physical inspections
- Reduced number of unauthorised accesses to restricted equipment rooms
- Transparent, regular switching to no-break power
- Time lag between recording and closure of physical incidents

DS12 Maturity Model

Control over the IT process **Manage Facilities** with the business goal of *providing a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards*

0 Non-existent There is no awareness of the need to protect the facilities or the investment in computing resources. Environmental factors, including fire protection, dust, power and excessive heat and humidity, are neither monitored nor controlled.

1 Initial / Ad Hoc The organisation has recognised a business requirement to provide a suitable physical surrounding which protects the resources and personnel against man-made and natural hazards. No standard procedures exist and the management of facilities and equipment is dependent upon the skills and abilities of key individuals. Housekeeping is not reviewed and people move within the facilities without restriction. Management does not monitor the facility environmental controls or the movement of personnel.

2 Repeatable but Intuitive The awareness of the need to protect and control the physical computing environment is recognised and evident in the allocation of budgets and other resources. Environmental controls are implemented and monitored by the operations personnel. Physical security is an informal process, driven by a small group of employees possessing a high-level of concern about securing the physical facilities. The facilities maintenance procedures are not well documented and rely upon the best practices of a few individuals. The physical security goals are not based on any formal standards and management does not ensure that security objectives are achieved.

3 Defined Process The need to maintain a controlled computing environment is understood and accepted within the organisation. The environmental controls, preventive maintenance and physical security are budget items approved and tracked by management. Access restrictions are applied, with only approved personnel being allowed access to the computing facilities. Visitors are logged and sometimes escorted, depending upon the responsible individual. The physical facilities are low profile and not readily identifiable. Civil authorities monitor compliance with health and safety regulations. The risks are insured, but no effort is made to optimise the insurance costs.

4 Managed and Measurable The need to maintain a controlled computing environment is fully understood, as evident in the organisational structure and budget allocations. Environmental and physical security requirements are documented and access is strictly controlled and monitored. Responsibility and ownership have been established and communicated. The facilities staff has been fully trained in emergency situations, as well as in health and safety practices. Standardised control mechanisms are in place for restricting access to facilities and addressing environmental and safety factors. Management monitors the effectiveness of controls and the compliance with established standards. The recoverability of computing resources is incorporated into an organisational risk management process. Plans are developed for the entire organisation, regular and integrated testing occurs and lessons learned are incorporated into plan revisions. The integrated information is used to optimise insurance coverage and related costs.

5 Optimised There is a long-term plan for the facilities required to support the organisation's computing environment. Standards are defined for all facilities, covering site selection, construction, guarding, personnel safety, mechanical and electrical systems, fire, lighting and flooding protection. All facilities are inventoried and classified according to the organisation's ongoing risk management process. Access is strictly controlled on a job-need basis, monitored continuously and visitors are escorted at all times. The environment is monitored and controlled through specialised equipment and equipment rooms become 'unmanned'. Preventive maintenance programs enforce a strict adherence to schedules and regular tests are applied to sensitive equipment. The facilities strategy and standards are aligned with IT services availability targets and integrated with business continuity planning and crisis management. Management reviews and optimises the facilities on a continual basis, capitalising on opportunities to improve the business contribution.

Control over the IT process **Manage Operations** with the business goal of *ensuring that important IT support functions are performed regularly and in an orderly fashion*

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

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

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

Information Criteria	
P	effectiveness
P	efficiency
	confidentiality
S	integrity
S	availability
	compliance
	reliability

(**P**) primary (**S**) secondary

IT Resources	
✓	people
✓	applications
	technology
✓	facilities
✓	data

(✓) applicable to

Critical Success Factors

- Operations instructions are well defined, according to agreed-upon standards, and with provision of clear cut-off and restart points
- There is a high degree of standardisation of operations
- There is close co-ordination with related processes, including problem and change management functions, and availability and continuity management
- There is a high degree of automation of operations tasks
- Operational processes are re-engineered to work effectively with automated tools
- Rationalisation and standardisation of systems management tools is implemented
- Input and output handling is, as much as possible, confined to the users
- Changes to job schedules are strictly controlled
- There are strict acceptance procedures for new job schedules, including documentation delivered
- Preventive maintenance schemes are in place
- Service support agreements with vendors are defined and enforced
- Clear and concise detection, inspection and escalation procedures are established

Key Goal Indicators

- A measured reduction in delays and deviations from schedules
- A measured completion of output media produced and delivered to the proper destination
- A measure of resources available on time and on schedule
- A measured reduction in operations related errors
- A reduced amount of scheduled as well as unscheduled downtime due to operations interventions
- A reduced overall cost of operation in relation to the overall processing load

Key Performance Indicators

- A measured completion of the computing process at various stages
- A measured reduction in operator intervention
- Reduced number of problems, delays and deviations
- Reduced number of reruns and restarts
- Reduced amount of unplanned maintenance
- Reduced number of unscheduled jobs and events
- Increased number of user controlled parameter settings
- Measured congruence between user demand and availability of resource capacity
- Frequency of analysis and reporting conducted to monitor operations performance
- Frequency of back-up check-ups
- Average age of equipment

DS13 Maturity Model

Control over the IT process **Manage Operations** with the business goal of *ensuring that important IT support functions are performed regularly and in an orderly fashion*

0 **Non-existent** The organisation does not devote time and resources to the establishment of basic IT support and operations activities.

1 **Initial / Ad Hoc** The organisation recognises the need for structuring the IT support functions. However, no standard procedures are established and the operations activities are reactive in nature. The majority of operations are not formally scheduled and processing requests are accepted without prior validation. Computers supporting the business processes are frequently interrupted, delayed and unavailable. Time is lost while employees wait for resources. Systems are not stable or available and output media sometimes show up in unexpected places or not at all.

2 **Repeatable but Intuitive** The organisation is fully aware of the key role that IT operations activities play in providing IT support functions. In addition, the organisation communicates the need for co-ordination between users and systems operations. Budgets for tools are being allocated on a case-by-case basis. IT support operations are informal and intuitive. There is a high dependence on the skills and abilities of individuals. The instructions of what to do, when and in what order, are not documented. There are no operating standards and no formal operator training exists. Management does not measure the meeting of schedules by IT operations or analyse delays.

3 **Defined Process** The need for computer operations management is understood and accepted within the organisation. Resources have been allocated and some on-the-job training occurs. The repeatable functions are formally defined, standardised, documented and communicated to operations and customer personnel. The events and completed task results are recorded, but reporting to management is limited or non-existent. The use of automated scheduling and other tools is extended and standardised in order to limit operator intervention. Other regular IT support activities are also identified and related tasks are being defined. Strict controls are exercised over putting new jobs in operation and a formal policy is used to reduce the number of unscheduled events. Maintenance and service agreements with vendors are still informal in nature.

4 **Managed and Measurable** The computer operations and support responsibilities are clearly defined and ownership is assigned. Operations are supported through resource budgets for capital expenditures and human resources. Training is formalised and ongoing, as part of career development. Schedules and tasks are documented and communicated, both internal to the IT function and to the business client. It is possible to measure and monitor the daily activities with standardised performance agreements and established service levels. Any deviations from established norms are quickly addressed and corrected. Management monitors the use of computing resources and completion of work or assigned tasks. An on-going effort exists to increase the level of process automation as a means of ensuring continuous improvement. Formal maintenance and service agreements are established with vendors. There is full alignment with problem and availability management processes, supported by an analysis of the causes of errors and failures.

5 **Optimised** IT support operations are effective, efficient and sufficiently flexible to meet service level needs quickly and without loss of productivity. Operational IT management processes are standardised and documented in a knowledge base and is subject to continuous improvement. Automated processes that support systems operate seamlessly and contribute to a stable environment that is transparent to and usable by the user. This allows users to maximise alignment of IT operations with their needs. All problems and failures are analysed to identify the root cause. Regular meetings with change management ensure timely inclusion of changes in production schedules. In co-operation with the vendor, equipment is analysed for age and malfunction symptoms and maintenance is mainly preventive in nature.

This page intentionally left blank

MONITORING

Control over the IT process **Monitor the Processes** with the business goal of *ensuring the achievement of the performance objectives set for the IT processes*

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

is enabled by *the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations*

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

Information Criteria
P effectiveness
P efficiency
S confidentiality
S integrity
S availability
S compliance
S reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Consistent application of the right limited number of performance indicators
- Increased number of process improvement opportunities detected and acted upon
- Satisfaction of management and the governance entity with performance reporting
- Reduced number of outstanding process deficiencies

Critical Success Factors

- Useful, accurate and timely management reports are available
- Processes have defined and understood Key Goal Indicators and Key Performance Indicators
- Measurements of IT performance include financial, operational, customer and organisational learning criteria that ensure alignment with organisation-wide goals and can be integrated with tools such as the IT Balanced Business Scorecard
- There are clearly understood and communicated process objectives
- A framework is established for defining and implementing IT governance reporting requirements
- A knowledge base of historical performance is established

Key Performance Indicators

- Time lag between the process deficiency occurrence and reporting
- Time lag between the reporting of a deficiency and action initiated
- Ratio between process deficiencies reported and deficiencies subsequently accepted as requiring management attention follow-up (noise index)
- Number of processes monitored
- Number of cause and effect relations identified and incorporated in monitoring
- Number of external benchmarks of process effectiveness
- Time lag between business changes and any associated changes to performance indicators
- Number of changes to the set of performance indicators without the business goals changing

M1 Maturity Model

Control over the IT process **Monitor the Processes** with the business goal of *ensuring the achievement of the performance objectives set for the IT processes*

0 Non-existent The organisation has no monitoring process implemented. IT does not independently perform monitoring of projects or processes. Useful, timely and accurate reports are not available. The need for clearly understood process objectives is not recognised.

1 Initial / Ad Hoc Management recognises a need to collect and assess information about monitoring processes. Standard collection and assessment processes have not been identified. Monitoring is implemented and metrics are chosen on a case-by-case basis, according to the needs of specific IT projects and processes. Monitoring is generally implemented reactively to an incident that has caused some loss or embarrassment to the organisation. Monitoring is implemented by the information services function for the benefit of other departments, but is not implemented over IT processes. Process definition and monitoring measures follow traditional financial, operations and internal control approaches, without specifically addressing the needs of the information services function.

2 Repeatable but Intuitive Basic measurements to be monitored have been identified. Collection and assessment methods and techniques have been defined, but the processes have not been adopted across the entire organisation. Planning and management functions are created for assessing monitoring processes, but decisions are made based on the expertise of key individuals. Limited tools are chosen and implemented for gathering information, but may not be used to their full capacity due to a lack of expertise in their functionality. The information services function is managed as a cost centre, without assessing its contribution to the revenue generating entities of the organisation.

3 Defined Process Management has communicated and institutionalised standard monitoring processes. Educational and training programs for monitoring have been implemented. A formalised knowledge base of historical performance information has been developed. Assessment is still performed at the individual IT process and project level and is not integrated among all processes. Tools for monitoring internal IT processes and service levels are being implemented. Measurements of the contribution of the information services function to the performance of the organisation have been defined, using traditional financial and operational criteria. IT-specific performance measurements are defined and implemented, but the non-financial and strategic measurements are still informal. Measures of customer satisfaction and service levels provided to the operating entities of the organisation are being implemented.

4 Managed and Measurable Management has defined the tolerances under which processes must operate. Base-lining of monitoring results is being standardised and normalised. There is integration of metrics across all IT projects and processes. The information services function management reporting systems are formalised and fully automated. Automated tools are integrated and leveraged organisation-wide to collect and monitor operational information on applications, systems and processes. A framework has been defined for identifying strategically oriented KGIs, KPIs and CSFs to measure performance. Criteria for evaluating organisational development based on Maturity Models have been defined. Measurements of the information services function performance include financial, operational, customer and organisational learning criteria that ensure alignment with organisation-wide goals.

5 Optimised A continuous quality improvement process is developed for updating organisation-wide monitoring standards and policies and incorporating industry best practices. All monitoring processes are optimised and support organisation-wide objectives. KGIs, KPIs and CSFs are routinely used to measure performance and are integrated into strategic assessment frameworks such as the IT Balanced Scorecard. Process monitoring and on-going re-design are consistent with plans developed based on process maturity models and with organisation-wide business process improvement plans. Benchmarking against industry and key competitors has become formalised, with well-understood comparison criteria.

Control over the IT process **Assess Internal Control Adequacy** with the business goal of *ensuring the achievement of the internal control objectives set for the IT processes*

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

is enabled by *the commitment to monitoring internal control, assessing their effectiveness, and reporting on them on a regular basis*

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

Information Criteria
P effectiveness
P efficiency
S confidentiality
S integrity
S availability
P compliance
S reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Index of senior management satisfaction and comfort with reporting on internal control monitoring
- Decreased probability of internal control incidents
- Positive external qualification and certification reports
- Number of control improvement initiatives
- Absence of regulatory or legal non-compliance events
- Decreased number of security incidents and quality defects

Critical Success Factors

- Management clearly defines what components of the processes need to be controlled
- Internal control, compliance and internal audit responsibilities are clearly understood
- Competence and authority of the internal control compliance function exist, addressing delegation as appropriate
- A properly defined IT control process framework is in place
- A clear process is used for timely reporting of internal control deficiencies
- Internal control monitoring data is accurate, complete and timely
- There is management commitment to act on internal control deficiencies
- There is alignment with risk assessment and security processes
- A process is in place to support knowledge sharing on internal control incidents and solutions

Key Performance Indicators

- Number and coverage of control self-assessments
- Timeliness between internal control deficiency occurrence and reporting
- Number, frequency and coverage of internal compliance reports
- Number of timely actions on internal control issues
- Number of control improvements stemming from root cause analysis

M2 Maturity Model

Control over the IT process **Assess Internal Control Adequacy** with the business goal of *ensuring the achievement of the internal control objectives set for the IT processes*

0 Non-existent The organisation lacks procedures to monitor the effectiveness of internal controls. Management internal control reporting methods are absent. There is a general unawareness of IT operational security and internal control assurance. Management and employees have an overall lack of awareness of internal controls.

1 Initial / Ad Hoc The organisation has a lack of management commitment for regular operational security and internal control assurance. Individual expertise in assessing internal control adequacy is applied on an ad hoc basis. IT management has not formally assigned responsibility for monitoring effectiveness of internal controls. IT internal control assessments are conducted as part of traditional financial audits, with methodologies and skill sets that do not reflect the needs of the information services function.

2 Repeatable but Intuitive The organisation uses informal control reports to initiate corrective action initiatives. Planning and management processes are defined, but assessment is dependent on the skill sets of key individuals. The organisation has an increased awareness of internal control monitoring. Management has begun to establish basic metrics. Information services management performs monitoring over the effectiveness of critical internal controls on a regular basis. Controls over security are monitored and results are reviewed regularly. Methodologies and tools specific to the IT environment are starting to be used, but not consistently. Skilled IT staff is routinely participating in internal control assessments. Risk factors specific to the IT environment are being defined.

3 Defined Process Management supports and has institutionalised internal control monitoring. Policies and procedures have been developed for assessing and reporting on internal control monitoring activities. A metrics knowledge base for historical information on internal control monitoring is being established. An education and training program for internal control monitoring has been implemented. Peer reviews for internal control monitoring have been established. Self-assessments and internal controls assurance reviews are established over operational security and internal control assurance and involve information services function management working with business managers. Tools are being utilised but are not necessarily integrated into all processes. IT process risk assessment policies are being used within control frameworks developed specifically for the IT organisation. The information system services function is developing its own, technically oriented, IT internal control capabilities.

4 Managed and Measurable Management has established benchmarking and quantitative goals for internal control review processes. The organisation established tolerance levels for the internal control monitoring process. Integrated and increasingly automated tools are incorporated into internal control review processes, with an increased use of quantitative analysis and control. Process-specific risks and mitigation policies are defined for the entire information services function. A formal IT internal control function is established, with specialised and certified professionals utilising a formal control framework endorsed by senior management. Benchmarking against industry standards and development of best practices is being formalised.

5 Optimised Management has established an organisation-wide continuous improvement program that takes into account lessons learned and industry best practices for internal control monitoring. The organisation uses state of the art tools that are integrated and updated, where appropriate. Knowledge sharing is formalised and formal training programs, specific to the information services function, are implemented. IT control frameworks address not only IT technical issues, but are integrated with organisation-wide frameworks and methodologies to ensure consistency with organisation goals.

Control over the IT process **Obtain Independent Assurance** with the business goal of *increasing confidence and trust among the organisation, customers and third-party providers*

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

is enabled by *independent assurance reviews carried out at regular intervals*

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

Information Criteria
P effectiveness
P efficiency
S confidentiality
S integrity
S availability
P compliance
S reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Increased number of accepted opinions on the overall system of internal control for all agreed domains
- Increased number of quality certifications or accreditations for all agreed domains
- Increased number of second opinions reported to the stakeholders for major IT decisions such as going live, contract negotiations, joint ventures and major acquisitions
- Percentage of recommendations closed on time relative to independent internal control reviews, quality certifications or accreditations and second opinions
- Reduced number of failed or reversed major IT decisions
- Index of confidence and trust of stakeholders

Critical Success Factors

- There is continuous alignment with stakeholder needs
- The organisation has defined processes for IT assurance activities, especially overall internal control, certification and major decisions
- Benchmarking of external service providers is routinely performed
- Major IT decisions have an up-front requirements analysis for a third-party assurance opinion
- Prior to obtaining independent assurance, a high-level risk assessment is performed with the key stakeholders
- There is a commitment to leverage independent assurance for sustainable improvement
- Assurance activities are performed in accordance with generally accepted practices, such as SysTrust
- There is a partnership between auditor and auditee, to encourage cooperation

Key Performance Indicators

- Reduced overhead of obtaining assurance and certifications
- Timeliness of assurance reporting
- Timeliness of assurance activities
- Number of assurance processes initiated
- Number of iterations before assurance reports are accepted
- Number of IT decisions requiring assurance where no assurance was sought
- Number of IT decisions not requiring assurance where assurance was sought
- Reduced number of failed or reversed major IT decisions after a positive assurance was obtained

M3 Maturity Model

Control over the IT process **Obtain Independent Assurance** with the business goal of *increasing confidence and trust among the organisation, customers and third-party providers*

0 Non-existent The organisation does not have assurance processes in place. Security policies are not implemented. Service level agreements have not been developed and processes are not measured. Management has not instituted any assurance or certification programs.

1 Initial / Ad Hoc The organisation manages IT processes independently. Certification and assurance processes are in place on an exception basis. Certification and assurance are driven by events such as regulatory changes or requirements or customer demand. The assurance process is conducted reactively by task forces or by technical specialists who do not have specific assurance skills.

2 Repeatable but Intuitive Information services function management has implemented processes for managing assurance activities. Assurance requirements are still linked to business needs and requirements and are driven by the information system services function. Risk management, as part of information services function management, drives certification and assurance programs. The information services function performs risk assessments to identify system level risks. Senior management supports and has committed to independent assurance. Methods and techniques are developed for certification and assurance and are being benchmarked to develop best practices. The process for selecting internal or external resources is being formalised.

3 Defined process The organisation has defined and institutionalised the processes for IT assurance activities and the criteria for using internal and external resources based on the level of expertise, sensitivity and independence required. Assurance processes include legal and regulatory requirements, certification needs, general organisational effectiveness and identification of best practices. Assurance requirements have been developed for IT processes. Management conducts participative reviews of all assurance activities. Management outside of the information services function has proactive involvement in assurance and certification reviews. A knowledge base of certification and assurance best practices has been developed. Key IT processes have been certified.

4 Managed and Measurable Management has implemented assurance processes for ensuring that critical IT processes are identified and have specific assurance plans. IT processes are reviewed in the context of the business process they support. Assurance processes are quantitatively managed and controlled. Management uses what is learned from assurance and certification processes to improve other processes, based on what was learned. The knowledge base is utilised to ensure that best practices are used in new processes and to benchmark other processes. A formal process is in place to ensure the competence of the assurance function by continually evaluating the balance between internally- and externally-available knowledge and skills. Cost/benefit criteria for conducting internal and external-based assessments are defined.

5 Optimised Management has implemented measures to ensure that all critical business processes have assurance processes over the IT infrastructures that support them. The organisation has a continuous improvement program for the assurance and certification processes that reflects industry best practices. Management has developed the ability to quickly integrate the results of assurance and certification activities into organisation-wide processes. The effectiveness of third-party service providers and relationships with business partners are routinely evaluated. There is a formally-defined strategy, supported by senior management, for developing compliance with national and international standards and for obtaining certifications that are seen as providing recognition and a competitive advantage.

Control over the IT process **Provide for Independent Audit** with the business goal of *increasing confidence levels and benefit from best practice advice*

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

is enabled by *independent audits carried out at regular intervals*

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

Information Criteria
P effectiveness
P efficiency
S confidentiality
S integrity
S availability
P compliance
S reliability

(**P**) primary (**S**) secondary

IT Resources
✓ people
✓ applications
✓ technology
✓ facilities
✓ data

(✓) applicable to

Key Goal Indicators

- Increased level of confidence derived from independent audit activities
- Increased adoption of best practices as a result of independent audit advice and recommendations
- Increased value for the money
- Increased level of communication with the audit committee and senior management

Critical Success Factors

- An audit committee that defines and supports an audit mandate that provides for the independence, responsibility, authority and accountability of the audit function
- Risk-based planning is used to identify business and IT activities for initial and cyclical reviews
- The planning and conducting of audits are proactive
- The audit methodology is properly supported by tools and techniques
- Clearly-agreed on practices between management and audit are established for tracking and closing audit recommendations and for reporting on global status
- Auditors perform impact assessments of recommendations, including cost, benefit and risk
- Audits are performed in accordance with generally accepted auditing standards

Key Performance Indicators

- Increased level of satisfaction with the audit function working relationship
- Number of corrective and sustainable actions taken as a result of new audit findings
- Increased number of auditors with professional and technical certifications
- Improved cycle time of the audit process, from planning through reporting

M4 Maturity Model

Control over the IT process **Provide for Independent Audit** with the business goal of *increasing confidence levels and benefit from best practice advice*

0 Non-existent Management is unaware of the importance of an independent audit function and independent audits do not take place.

1 Initial / Ad Hoc An informal IT audit function exists which carries out independent reviews from time to time. There is no overall plan for providing independent audits and no co-ordination between reviews. Independent audit planning, managing and reporting are based on individual expertise. The quality of planning and delivery of audit services is generally poor, with variable results and very limited management involvement.

2 Repeatable but Intuitive Provision of an independent audit function is recognised by management as being potentially useful, but there is no written policy defining its purpose, authority and responsibilities. Senior management has not established an infrastructure and process to ensure that independent audits are performed on a regular basis. Independent audit planning, managing and reporting follows a similar pattern, based on previously gained experience and the expertise of the team members. There is little co-ordination between audits and limited follow-up of previous audit findings. IT management interest and involvement in the audit process is inconsistent and dependent on the perceived quality of the specific audit team.

3 Defined Process A charter for the IT audit function is established by senior management and followed in providing for the independence and authority of the audit function. Audit management has identified and understands the IT environment and initiatives. A process is established for planning and managing audits. Audit staff is expected to comply with auditing standards, but results may be variable. Resolution of audit comments does occur, but often there is poor follow-up and closure. Basic elements of quality assurance are established to assure that practices comply with applicable auditing standards and to improve the effectiveness of audit function activities. The IT, financial and process audit functions are not generally integrated. IT management is aware of the need for independent audits, but is not always satisfied with the quality provided and does not have confidence that the function has adequate knowledge to make valid recommendations.

4 Managed and Measurable Strategic and operational risk-based audit plans are established, based on an assessment of current and future needs. Individual audit plans are developed, based on a cyclical operational plan and resource availability. The audit process can be tailored to specific assignments. A process knowledge base is established and is developed to ensure that quality assessments can be made and useful recommendations are generated. Audits are co-ordinated and integrated with any associated financial and process audits. Results are reported to management and follow-up occurs to ensure that management has taken corrective actions on critical issues identified by the audits. A structured quality assurance function facilitates quantitative management and control of the audit process. The IT audit function participates in the development of corrective actions and in projects to ensure that controls are appropriately built into processes. IT management is usually positively involved in all audits and makes use of audit results to improve performance.

5 Optimised The audit function is capable of rapidly responding to management concerns related to business process and IT control risk issues on a continuous, organisation-wide basis. Audit planning is closely integrated with business and IT strategies. Audit processes are monitored and analysed for improvement in adapting to changing environmental conditions. This includes quantitatively monitoring activities in the auditing community and taking into account state-of-the-art industry best practices and other external trends in adjusting auditing processes. Audit is involved in the development of business plans and in all projects that support business plans, to ensure that the appropriate controls are included into all processes. Audit is consulted on all projects for control and business advice.

This page intentionally left blank

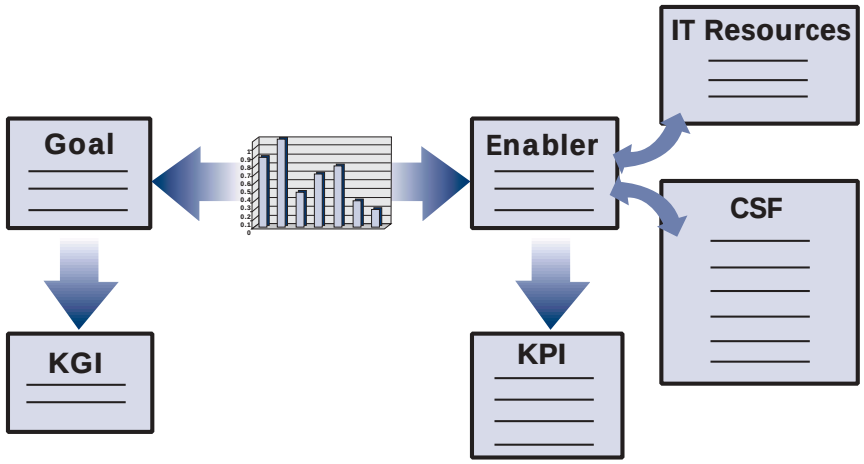
HOW TO USE

1. THE MANAGEMENT GUIDELINES

On the left-hand page, every *Management Guideline* provides a number of elements for each of the 34 COBIT processes:

- Process identification
- Goal statement for the process
- Enabling statement (how to keep the process under control to ascertain whether it achieves its goals)
- IT Resources, with an indication of relevance to this process
- Information Criteria, with an indication of relative importance (P = of primary importance, S = of secondary importance, or blank = less important, not necessarily to be neglected)
- Critical Success Factors
- Key Goal Indicators
- Key Performance Indicators.

These elements are structured as described in the following graphic. The relationship is based on the principles of the Balanced Business Scorecard, linking goals with their outcome measures (KGI) to enablers with their performance measures (KPI). The enablers are made specific and pragmatic with a number of Critical Success Factors and use specific IT Resources.



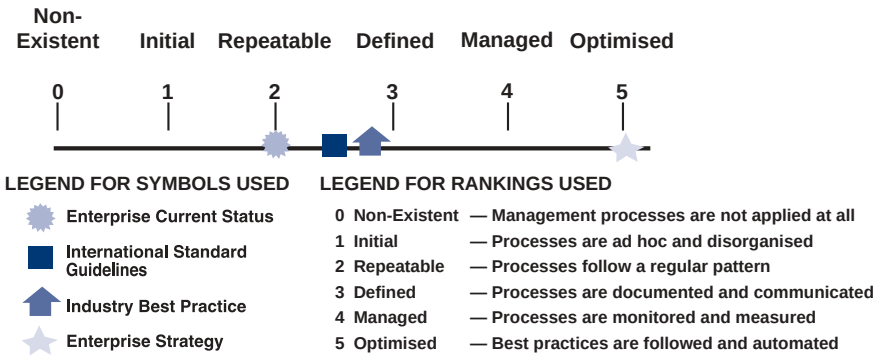
In addition, guidance can be obtained from the Generic Management Guideline (see Appendix IV) and from the IT Governance Guideline (see Appendix V). Both of these will give a quick indication of the high-level requirements to keep an IT process manageable.

Finally, it needs to be noted that these guidelines do not propose that all the practices addressed through CSFs and KPIs need to be applied in all cases. An appropriate selection needs to be made. The Maturity Models (see next section in this Appendix) supplied with each process guideline can help in making that selection. However, in businesses with high reliability requirements for IT and where survival depends on the availability of information, the near global application of the guidelines, at levels 3 or 4 of maturity, would constitute good practice.

2. THE MATURITY MODEL

As a separate tool, a Maturity Model is provided on the right hand page of the *Management Guidelines* for each of the 34 COBIT processes. This tool can be the basis for the following incremental applications:

- A method for self-assessment against the scales, deciding where the organisation is
- A method for using the results of the self-assessment to set targets for future development, based upon where the organisation wants to be on the scale, which is not necessarily at level 5
- A method for planning projects to reach the targets, based upon an analysis of the gaps between those targets and the present status
- A method for prioritising project work based upon project classification and upon an analysis of its beneficial impact against its cost.



2.1. Self-assessment and Goal Identification

For each assessment topic the organisation should use the six-point measurement scale from 0 to 5, to define its estimated position. This can then easily and graphically be compared to the three reference points (targeted performance, international standards and best practice).

An organisation making a self-assessment simply needs to consider each assessment topic in turn, reading the six scale-point descriptors and assessing which one of these six positions best describes the current status of the organisation. The more important the process is for the organisation, the higher one should be on the scale. For example, in a relatively stable commercial environment, the incremental maturity of the 13 IT Processes in the Delivery and Support domain is what differentiates successful organisations from others. On the other hand, in a highly dynamic commercial environment, organisational success, if not survival, is highly dependent on the maturity of the Planning and Organisation and the Acquisition and Implementation domains.

Each benchmark point is strictly incremental and all conditions of the descriptor must be fulfilled to qualify for classification at that level. It should also be noted that there is a difference between measuring capability and measuring performance. For example, acquiring the capability and skills for certain security or control practices is one decision that needs to be made and tracked, but consistent application of the capability, once it has been acquired, needs also to be measured.

The organisation also needs to consider which one of the six descriptors best describes where it would like to go as a result of its IT strategy, with special emphasis on the degree of dependence and value of information in achieving its business requirements. The external benchmarks can be very helpful in forming an opinion as to what realistic level of security and control the organisation requires in relation to its environment and its strategic goals.

2.2. Gap Analysis

In many cases the two self assessment markers (where one is and where one wants to be) will be separated by a gap on the chart, the size of which gives a visual impression of how much work needs to be done to close the gap and hence to achieve the strategic goal. However, this gap also needs to be described in greater detail to facilitate use of the results of the gap analysis to plan a series of projects which will take the organisation towards its strategic goals for security and control of IT.

The gap analysis process will compile a list of all the actions needed to close the gaps between the 'current status' markers and their corresponding 'strategic goal' markers. This list of gaps should then be used to plan a matching list of projects that will carry out these actions. There will probably be a many-to-many mapping between gaps and projects (see diagram below).

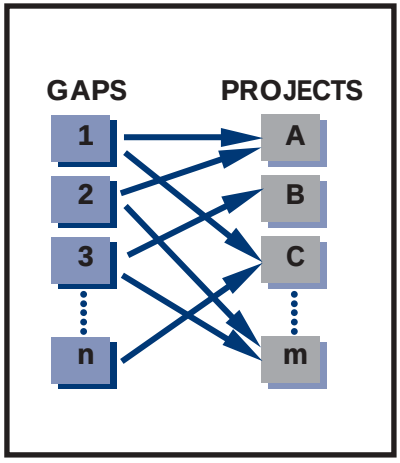
2.3. Project Classification

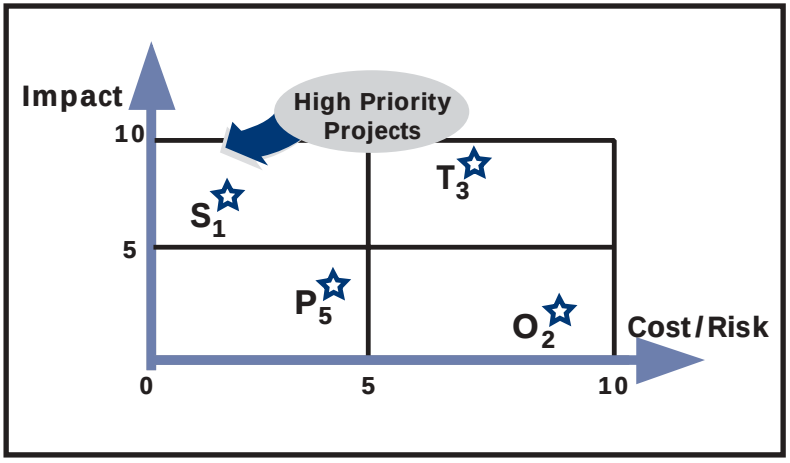
For ease of planning and communication, projects can be classified according to type: Strategic initiatives, Tactical projects, Organisational improvements or Procedural developments. Each project is then tagged with a unique sequential label, for example: S1, T3, O2, P5, as in the diagram below.

2.4. Project Prioritisation

The objective of prioritising projects is to identify those projects where quick wins can be achieved. The best candidates for quick wins are usually those where the gaps are small, where the cost of closing the gap is low, where the risk of project failure is low and where the impact on the business benefits will be greatest.

Projects should therefore be assessed for impact and cost/risk, on a scale of 0 to 10, for each of these variables. The projects can be plotted on a chart which becomes a management decision support tool, showing the relative impacts and costs/risks. Projects that are high impact and low cost/risk are good candidates for selection as quick wins.





This page intentionally left blank

THE COBIT FRAMEWORK

THE NEED FOR CONTROL IN INFORMATION TECHNOLOGY

In recent years, it has become increasingly evident to regulators, lawmakers, users and service providers that there is a need for a reference framework for security and control in IT. Critically important to the success and survival of an organisation is effective management of 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; and
- 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. Truly, information and information systems are pervasive throughout organisations—from the user's platform to local and wide area networks to client servers to mainframe computers. ***Many organisations recognise the potential benefits that technology can yield. Successful organisations, however, understand and manage the risks associated with implementing new technologies.*** Thus, management needs to have an appreciation for and a basic understanding of the risks and constraints of IT in order to provide 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 helps manage risks, it does 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 their 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. This has been illustrated by several recent studies on how auditors judge complex security and control situations in IT—studies that came about almost simultaneously in different corners of the world. 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 fulfill 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.

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, U.S.). 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 that the public accountant provide 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 *Control Objectives* from an auditor's tool to COBIT, a management tool. Further, the development of *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. COBIT is thus the breakthrough IT governance tool that helps management in understanding and managing the risks associated with IT.

Hence, the main objective of the COBIT project is the development of clear policies and good practices for security and control in IT, for endorsement by commercial, governmental and professional organisations, world-at-large. 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 were 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.

Apart from responding to the needs of the immediate audience of senior management, auditors and security and control professionals, COBIT can be used within enterprises by the business process owner in his/her responsibility for control over the information aspects of the process and by those responsible for IT in the enterprise.

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 objective, 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.

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.

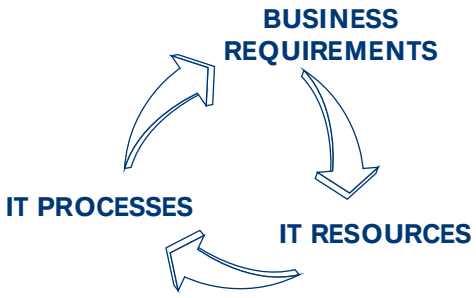
IT Control Objective is defined as a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

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 appropriate 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 & regulations
Security Requirements	Confidentiality Integrity Availability

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

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

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

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

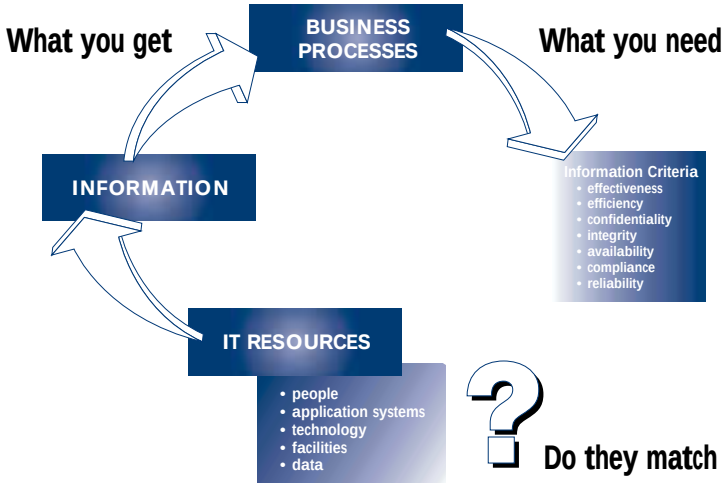
Effectiveness	deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
Efficiency	concerns the provision of information through the optimal (most productive and economical) use of resources.
Confidentiality	concerns the protection of sensitive information from unauthorised disclosure.
Integrity	relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
Availability	relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
Compliance	deals with complying with those laws, regulations and contractual arrangements to which the business process is subject; i.e., externally imposed business criteria.
Reliability of Information	relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

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

Data	are objects in their widest sense (i.e., external and internal), structured and non-structured, graphics, sound, etc.
Application Systems	are understood to be the sum of manual and programmed procedures.
Technology	covers hardware, operating systems, database management systems, networking, multimedia, etc.
Facilities	are all the resources to house and support, information systems.
People	include staff skills, awareness and productivity to plan, organise, acquire, deliver, support and monitor information systems and services.

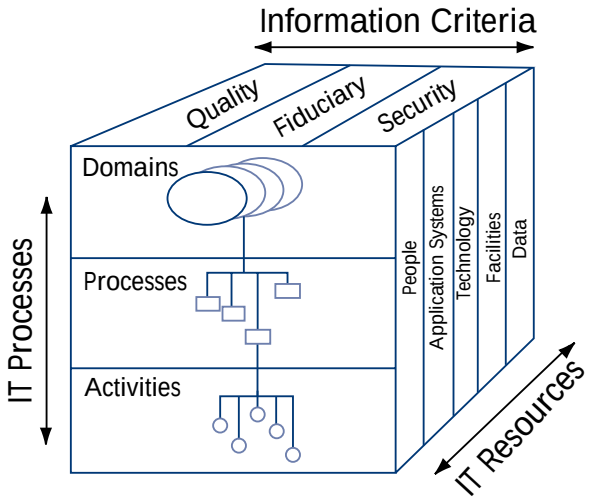
Money or capital was not retained as an IT resource for classification of control objectives because it can be considered as being the investment into any of the above resources. It should also be noted that the *Framework* does not specifically refer to documentation of all material matters relating 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.

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



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

Thus, the conceptual framework can be approached from three vantage points: (1) Information Criteria, (2) IT Resources and (3) IT Processes. For example, managers may want to look with a Quality, Fiduciary or Security interest (included in the *Framework* as seven specific information criteria). An IT manager, on the other hand, may want to consider IT resources for which he/she is accountable. Process owners, IT specialists and users may have a specific interest in particular processes or activities/tasks. Auditors may wish to approach the *Framework* from a control coverage point of view. These three vantage points are depicted in the COBIT Cube.



With the above 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 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 information services 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.

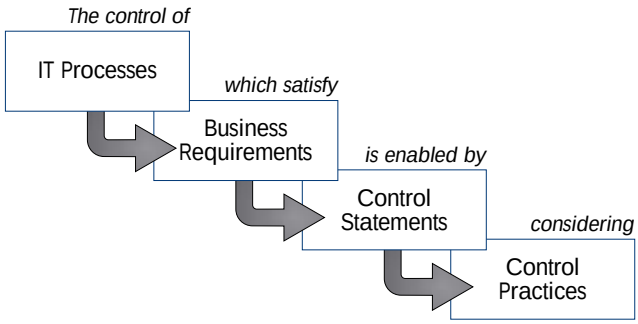
It is clear that all control measures will not necessarily satisfy the different business requirements for information to the same degree.

- **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 only satisfies to a lesser extent or indirectly the information criterion concerned.
- **Blank** could be applicable; however, requirements are more appropriately satisfied by another criteria in this process and/or by another process.

Similarly, not all control measures will 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 the same rigorous process of input from researchers, experts and reviewers, using the strict definitions previously indicated.

HIGH-LEVEL CONTROL OBJECTIVES

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.

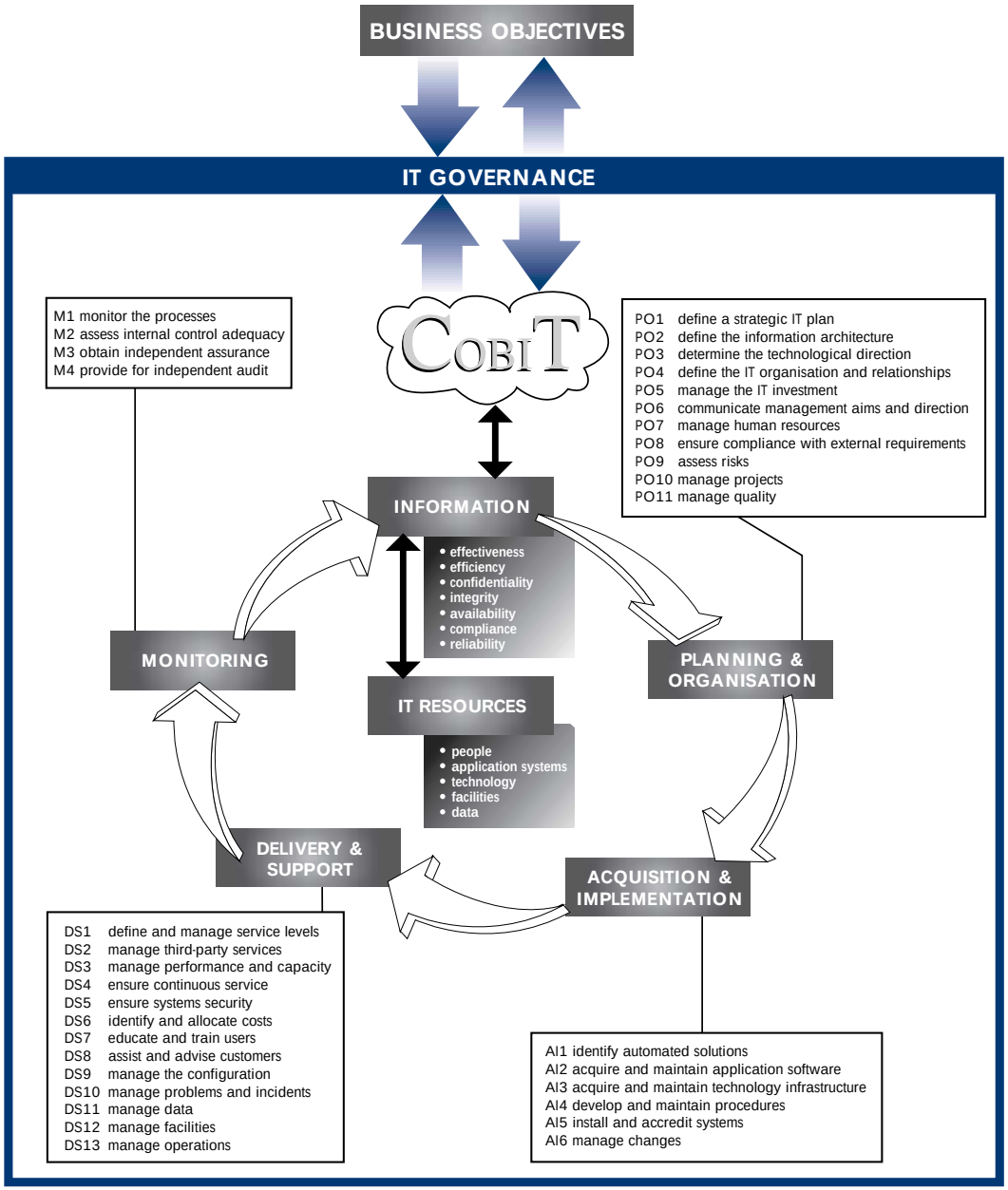


The Control Objectives have been organised by process/activity, to facilitate combined or global approaches, such as installation/implementation of a process, global management responsibilities for a process and the use of IT resources by a process.

The Control Objectives have also been provided with references to IT domains, IT resources and business criteria for information. This allows looking at the IT control requirements from any of three vantage points, as illustrated earlier by the COBIT Cube (see page 109). Each high-level control objective indicates to which domain it belongs, which information criteria are the most and second most important for the process it covers and which resources need management's special attention.

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.

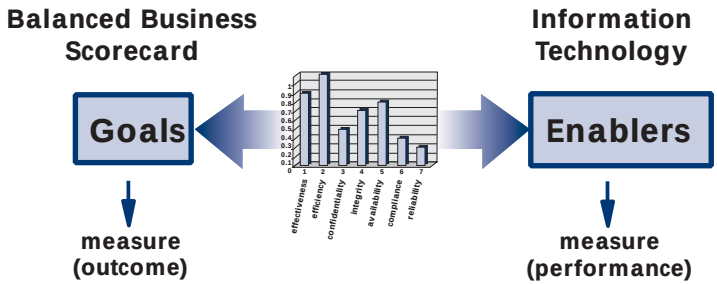
In summary, in order to provide the information that the organisation needs to achieve its objectives, IT governance must be exercised by the organisation to ensure that IT resources are managed by a set of naturally grouped IT processes. The following diagram illustrates this concept.



COBIT AND THE BALANCED BUSINESS SCORECARD

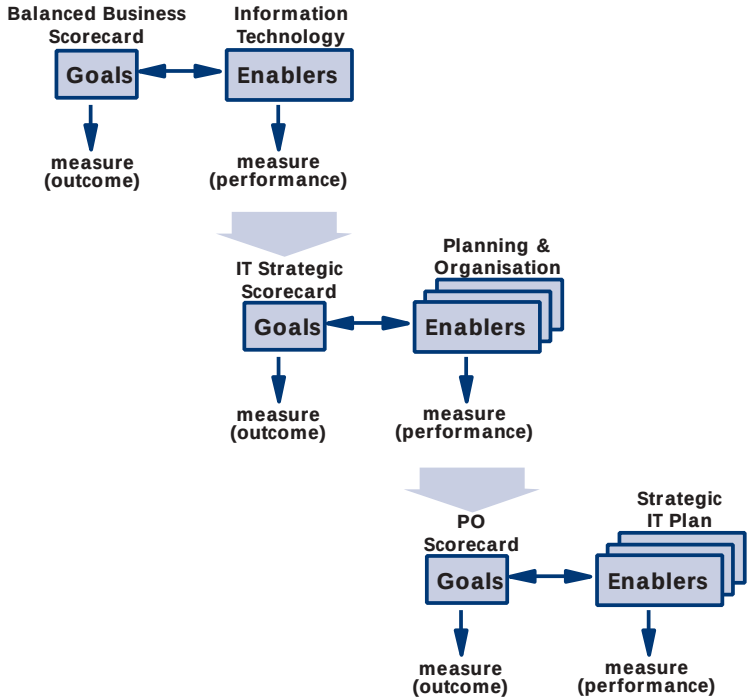
The COBIT *Framework* states that IT enables the business by delivering the information the business needs. IT's goal is therefore measured by looking at COBIT's Information Criteria contained in the COBIT *Framework*.

Information Criteria
• effectiveness
• efficiency
• confidentiality
• integrity
• availability
• compliance
• reliability



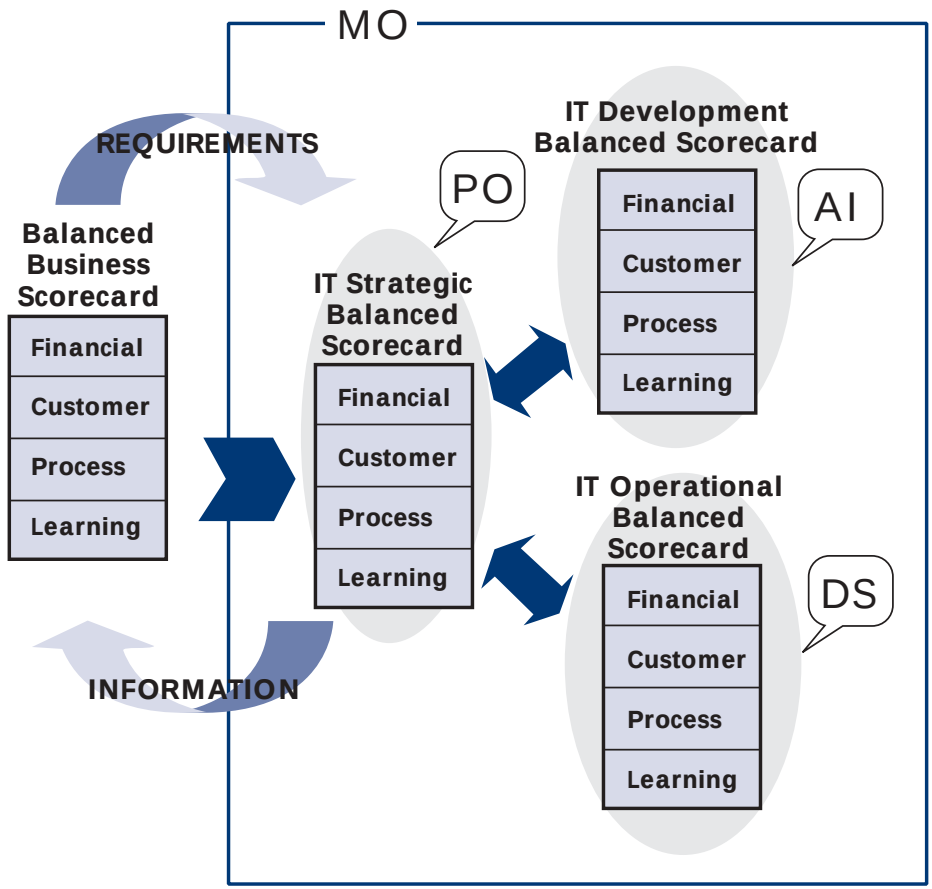
Each of these criteria will not be equally important. Their importance depends on the enterprise's business and the specific IT process one looks at. The relative importance of the criteria (expressed as a mini chart in the above graph) express the expectation of the business and are therefore the goal of IT, which thereby enables the business. These principles of measuring outcomes and performances are inherent to the Balanced Business Scorecard and have been used to develop the *Management Guidelines*.

The performance measures of the enablers become the goal for IT, which in turn will have a number of enablers. These could be the COBIT domains. Here again the measures can be cascaded, the performance measure of the domain becoming a goal for the process.



Another way to look at this is by starting from the balanced business scorecard and its 4 dimensions and then considering that IT enables the business, monitored by an IT strategic balanced business scorecard. Delivering the strategic IT goals is typically provided by two distinct responsibility domains in the enterprise, leading to a development scorecard and an operations scorecard.

Now we can easily map the 4 IT domains that the COBIT *Framework* has identified onto these scorecards. Planning and Organisation (PO) providing the measures of the IT strategic balanced business scorecard, Acquisition and Implementation (AI) providing the same for the development scorecard, while Delivery and Support (DS) supplies the operational scorecard. Overlaying these domains is the Monitoring (MO) domain which provides through management supervision and measurability, through audit and through assurance, the overall IT governance of the enterprise.



APPENDIX IV

Generic Process Management Guideline[1]

Control over an IT process and its activities with specific business goals

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 excellence and control appropriate for the business*

considers Critical Success Factors that leverage specific 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 performance is measured in financial terms, in relation to customer satisfaction, for process effectiveness and for future capability, and IT management is rewarded based on these measures
- The processes are aligned with the IT strategy and with the business goals; they are scalable and their resources are appropriately managed and leveraged
- Everyone involved in the process is goal focused and has the appropriate information on customers, on internal processes and on the consequences of their decisions
- A business culture is established, encouraging cross-divisional co-operation and teamwork, as well as continuous process improvement
- Control practices are applied to increase transparency, reduce complexity, promote learning, provide flexibility and allow scalability
- Goals and objectives are communicated across all disciplines and are understood
- It is known how to implement and monitor process objectives and who is accountable for process performance
- A continuous process quality improvement effort is applied
- There is clarity on who the customers of the process are
- The required quality of staff (training, transfer of information, morale, etc.) and availability of skills (recruit, retain, re-train) exist

Key Goal Indicators

- Increased level of service delivery
- Number of customers and cost per customer served
- Availability of systems and services
- Absence of integrity and confidentiality risks
- Cost efficiency of processes and operations
- Confirmation of reliability and effectiveness
- Adherence to development cost and schedule
- Cost efficiency of the process
- Staff productivity and morale
- Number of timely changes to processes and systems
- Improved productivity (e.g., delivery of value per employee)

Key Performance Indicators

- System downtime
- Throughput and response times
- Amount of errors and rework
- Number of staff trained in new technology and customer service skills
- Benchmark comparisons
- Number of non-compliance reportings
- Reduction in development and processing time

[1] Many of the elements of this guideline also apply to the IT Governance Management Guideline in Appendix V.

Generic Process Maturity Model

Control over an IT process and its activities with specific business goals

0 Non-existent There is a complete lack of any recognisable process. The organisation has not even recognised that there is an issue to be addressed.

1 Initial / Ad Hoc There is evidence that the organisation has recognised that the 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 and inconsistent communication on issues and the approaches needed to address them.

2 Repeatable but Intuitive There is global awareness of the issues. Processes have developed to the stage where similar, though informal and intuitive procedures are followed by different individuals undertaking the same task, for which common tools are emerging. Hence, these processes are repeatable and some of them begin to be monitored. There is no formal training and the communication on standard procedures and responsibilities is left to the individual. There is high reliance on the knowledge of individuals and errors are, therefore, likely. However, there is consistent communication on the overall issues and the need to address them.

3 Defined Process The need to act is understood and accepted. Procedures have been standardised, documented and implemented. They are being communicated and informal training is established. The procedures are not sophisticated and are the formalisation of existing practices. Tools are standardised, using currently available techniques. IT specialists are involved in this formalisation, but internal non-IT specialists participate only occasionally. It is, however, left to the individual to receive training, to follow the standards and to apply them. Most processes are monitored against some metrics, but any deviation, while being acted upon mostly through individual initiative, is unlikely to be detected by management. Root cause analysis is only occasionally applied.

4 Managed and Measurable There is full understanding of the issues at all levels, supported by formal training. Responsibilities are clear and process ownership is established. It is possible to monitor and measure compliance with procedures and process metrics and to take action where processes appear not to be working effectively or efficiently. Action is taken in many, but not all cases. Performance metrics are still dominated by traditional financial and operations measurements, but new criteria are being gradually implemented. Processes are occasionally improved and enforce best internal practices. Root cause analysis is being standardised. Continuous improvement is beginning to be addressed. Control practices are becoming increasingly transparent, flexible and scalable. There is limited, primarily tactical use of technology, based on mature techniques and enforced standard tools. The IT strategy is becoming increasingly aligned with the enterprise strategy. There is involvement of all required internal domain experts.

5 Optimised There is advanced and forward-looking understanding of issues and solutions. Training and communication are supported by leading-edge concepts and techniques. Goals and objectives are communicated cross-functionally, using KGIs, CSFs and KPIs to monitor performance. Processes have been refined to a level of external best practice, based on results of continuous improvement and maturity modeling with other organisations. They have led to an organisation, people and processes that are quick to adapt. The IT strategy is fully aligned with the enterprise strategy and a business culture is established to involve the IT organisation in business process improvement and in creating new business opportunities. All problems and deviations are analysed for root causes and efficient action is expediently identified and initiated. IT is used in an extensive, integrated and optimised manner to strategically leverage technology in automating the workflow and providing tools that improve quality and effectiveness. External experts are leveraged and benchmarks are used for guidance. Control practices are enforced and continuously improved. IT performance measurements address financial criteria, customer satisfaction, operations effectiveness and development of future capabilities. The compensation of IT management includes incentives for meeting the enterprise goals.

This page intentionally left blank

APPENDIX V

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

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

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 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 standardized 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 organisation. 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.

GOVERNANCE INSTITUTE™

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

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

TELL US WHAT YOU THINK ABOUT COBIT

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

_____

_____

_____

_____

_____

_____

_____

_____

Name _____

Company _____

Address _____

City _____ State/Province _____

Country _____ ZIP/Postal Code _____

FAX Number _____

E-mail Address _____

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

☐ Please send me more information about:

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

Thank you!

All respondents will be acknowledged.