IT Governance Using COBIT® and Val IT™: TIBO Case Study, 2nd Edition

An extended case study in which students can apply their COBIT® knowledge.
IT Governance Institute®
The IT Governance Institute (ITGI™) (www.itgi.org) was established in 1998 to advance international thinking and standards in
directing and controlling an enterprise’s information technology. Effective IT governance helps ensure that IT supports business
goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities. ITGI offers original
research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclaimer
ITGI and the author of IT Governance Using COBIT® and Val IT™: TIBO Case Study, 2nd Edition have designed the publication
primarily as an educational resource for educators. ITGI, ISACA® and the authors make no claim that use of this product will assure
a successful outcome. The publication should not be considered inclusive of all proper procedures and tests or exclusive of all proper
procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure
or test, controls professionals should apply their own professional judgement to the specific control circumstances presented by
the particular systems or IT environment. Note that this publication is an update of COBIT® in Academia: TIBO Case Study.

Disclosure
© 2007 IT Governance Institute. All rights reserved. This publication is intended solely for academic use and shall not be used in any
other manner (including for any commercial purpose). Reproductions of selections of this publication are permitted solely for the use
described above and must include the following copyright notice and acknowledgement: ‘Copyright © 2007 IT Governance Institute.
All rights reserved. Reprinted by permission.’ IT Governance Using COBIT® and Val IT™: TIBO Case Study, 2nd Edition, may not
otherwise be used, copied or reproduced, in any form by any means (electronic, mechanical, photocopying, recording or otherwise),
without the prior written permission of ITGI. Any modification, distribution, performance, display, transmission or storage, in any
form by any means (electronic, mechanical, photocopying, recording or otherwise) of IT Governance Using COBIT® and Val IT™:
TIBO Case Study, 2nd Edition, is strictly prohibited. No other right or permission is granted with respect to this work.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org

ISBN 978-1-60420-025-6
IT Governance Using COBIT® and Val IT™: TIBO Case Study, 2nd Edition
Printed in the United States of America

IT Governance Institute
ACKNOWLEDGEMENTS

ITGI wishes to recognise:

Researcher
Ed O’Donnell, University of Kansas, USA

Contributors
Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA
Steven De Haes, University of Antwerp Management School, Belgium
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Robert Parker, CISA, CA, CMC, FCA, Canada
V. Sambamurthy, Ph.D., Michigan State University, USA
Scott Lee Summers, Ph.D., Brigham Young University, USA
John Thorp, The Thorp Network, Canada
Wim Van Grembergen, Ph.D., University of Antwerp (UA) and University of Antwerp Management School (UAMS) and IT Alignment and Governance Research Institute (ITAG), Belgium
Ramesh Venkataraman, Ph.D., Indiana University, USA

ITGI Board of Trustees
Everett C. Johnson, CPA, Deloitte & Touche (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Lucio Augusto Molina Focazio, CISA, Colombia, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FH KiO, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Singapore
Anil Jogan, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart, IV, CISA, CISM, CIPP/G, IBM, USA
Romulo Lomparte, CISA, Banco de Credito BCP, Peru
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

ITGI Advisory Panel
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA
ACKNOWLEDGEMENTS (CONT.)

Academic Relations Committee
Scott Lee Summers, Ph.D., Brigham Young University, USA, Chair
Casey G. Cegielski, Ph.D., CISA, Auburn University, USA
Patrick Hanrion, CISM, CISSP, CNE, MCSE, Microsoft, USA
Donna Hutcheson, CISA, XR Group Inc., USA
Cejka Jiri Josef, CISA, Dipl. El.-Ing., KPMG Fides Peat, Switzerland
Michael Lambert, CISA, CISM, CARRA, Canada
Ed O’Donnell, University of Kansas, USA
Theodore Tryfonas, Ph.D., CISA, University of Glamorgan, Wales
Ramesh Venkataraman, Ph.D., Indiana University, USA

CobIT Steering Committee
Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Steven DeHaes, University of Antwerp Management School, Belgium
Rafael Eduardo Fabius, CISA, Republica AFAP, S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISM, CISA, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium
Robert E. Stroud, CA Inc., USA

ITGI Affiliates and Sponsors
ISACA chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d’Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
CA Inc.
Hewlett-Packard
IBM
ITpreneurs Nederlands BV
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions
# TABLE OF CONTENTS

1. Purpose of This Document .................................................................................................................. 2

2. Case Study Description ........................................................................................................................ 3
   - A Day in the Life of the Outsourcing Story of TIBO ........................................................................ 3
   - TIBO's Profile ................................................................................................................................. 4
   - The Company's IT Environment ...................................................................................................... 5
     - Projects ........................................................................................................................................ 5
     - Technology ................................................................................................................................. 5
     - Standards and Procedures ........................................................................................................... 5
     - Security ..................................................................................................................................... 6
   - The Organisational Entities ........................................................................................................... 6
     - Board of Directors ..................................................................................................................... 6
     - Executive Committee ............................................................................................................... 6
     - Business Strategy Group ......................................................................................................... 6
     - IT Co-ordination Committee ................................................................................................... 7
     - IT Management ......................................................................................................................... 7
     - IT Teams .................................................................................................................................... 7
     - Business Operational ............................................................................................................... 7

3. Additional Material ............................................................................................................................ 10
   - The Security Issue ....................................................................................................................... 10
     - Questions ................................................................................................................................. 10
   - The Outsourcing Issue ............................................................................................................... 10
     - Questions ................................................................................................................................. 10
   - The Strategic Alignment Issue ................................................................................................... 10
     - Extra Background Information ............................................................................................... 10
     - Questions ................................................................................................................................. 11

Appendix 1 — Financial Ombudsman Service ....................................................................................... 12

Appendix 2 — COBIT Control Objectives and Maturity Models .......................................................... 13

COBIT and Related Products .............................................................................................................. 33
1. PURPOSE OF THIS DOCUMENT

_TIBO Case Study, 2nd Edition_, is a product developed by ITGI, in collaboration with a group of international academics and practitioners, as part of _IT Governance Using COBIT® and Val IT™_. The goal of this document is to provide an extended case study (including case description, student questions and extensive teaching notes) in which students can apply their COBIT knowledge to a practical situation. It can be integrated into curricula for information systems management, information security management, auditing, information systems auditing and/or accounting information systems.

This case has been designed primarily to be used in graduate-level classes. The case can also be used in undergraduate classes, if the students are thoroughly exposed to concepts of internal control in an IT-intensive environment, general control frameworks and COBIT, in particular.

The case has been designed to map to _IT Governance Using COBIT® and Val IT™: Student Book—2nd Edition_, a book that explains all the COBIT elements and that was also developed by ITGI. The materials in this case study draw directly on COBIT IT processes.

It is suggested that the case be handled in one or possibly two class sessions (see figure 1) after COBIT has been introduced (session 0). It is recommended that the first part of the case be held in one class session of approximately 1.5 hours. The students should be given the reading (case study description and _Board Briefing on IT Governance, 2nd Edition_) with the questions handed out in class on one or more of the described issues: security, outsourcing, strategic alignment (as provided in the Additional Material section). Questions can be handled during a second session in an interactive fashion or as assignments to small groups. Additional reading materials and suggested solutions to each part of the case are provided in the teaching notes.

ITGI has developed three additional products that can accompany this case study in the _IT Governance Using COBIT® and Val IT™_ series for academics:
- _Student Book, 2nd Edition_ (mentioned previously)
- Presentation, 2nd Edition, a 35-slide PowerPoint deck on COBIT
- _Caselets, 2nd Edition_, which includes mini-cases for smaller COBIT exercises, to be used at the graduate and undergraduate levels

---

**Figure 1—Suggested Case Study Schedule**

<table>
<thead>
<tr>
<th>Session</th>
<th>Activity</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Introduction to COBIT</td>
<td><em>IT Governance Using COBIT® and Val IT™ Student Book, 2nd Edition</em></td>
</tr>
<tr>
<td>1</td>
<td>Part One TIBO Case</td>
<td>Case Study Description + <em>Board Briefing on IT Governance, 2nd Edition</em> + Questions</td>
</tr>
<tr>
<td>2</td>
<td>Security, Outsourcing, Strategic Alignment</td>
<td>Relevant Additional Material (see teaching notes)</td>
</tr>
</tbody>
</table>

---

1 IT Governance Institute, _Board Briefing on IT Governance, 2nd Edition_, USA, 2003
2. CASE STUDY DESCRIPTION

A DAY IN THE LIFE OF THE OUTSOURCING STORY OF TIBO

It was clear that the chief executive officer (CEO) of the Trusted Imperial Banking Organisation (TIBO), John Mitchell, was not in the mood for polite conversation. The director of IT, Steven De Haes, was ushered into the CEO’s office on the 30th floor of the bank’s head office in London’s city financial district by the CEO’s personal assistant, Pyms Forsythe. De Haes had some inkling of the problem when Forsythe called him to the meeting a few minutes ago. Forsythe stated, ‘Mitchell has had the Financial Ombudsman Survey on the phone, and he has been on the phone to the senior vice president (SVP) of retail ever since. He is not happy, and your fancy web-enabled business operations project (We-BOP) is as good as dead. Anyway, he wants to see you right away’.

De Haes knew that the SVP of retail, Wim Van Grembergen, was not a friend of IT. The IT group had been working on the We-BOP project over the last year for the retail group, struggling to meet the competition for the retail customer in the UK. This competition came not only from the Internet offerings of some banks but also from Internet-only financial institutions. De Haes just wished that his boss, the chief operating officer (COO), Erik Guldentops, was with him, but he was travelling on an overseas business trip (again). Mitchell snapped, ‘What are you boffins in IT doing with We-BOP? I have had the banking ombudsman on the phone to tell me that he is working on a formal complaint about our e-banking service. He has had more than 40 complaints over the last two months alone. I have been talking to Wim Van Grembergen, and he tells me that he has had no involvement in We-BOP for the last six months, since you guys outsourced it. I want you to bring We-BOP in-house and I want you to do it now’.

De Haes was able to calm the CEO and provide some more information on the project’s history. This revealed that there is a lot of dissatisfaction with IT relative to the quality of work of the third party, but also between the business and IT because IT made the outsourcing decision on its own. De Haes claimed IT did this in good faith because the business had been ‘livid’ about its inability to compete in the e-banking market. The discussion also revealed that there have been several warning signals about service quality.

‘You know Steven, that is right’, Mitchell said. ‘In talking to Wim earlier, I learned that the help desk report produced by the third party went to Joshua Dean, one of your guys, the manager of user support. Joshua assumed that the outsourcing company had dealt effectively with these complaints. They were not entered into his user support system. Joshua noticed that the reports were getting longer each month and mentioned it to Ed O’Donnell. Ed wasn’t surprised since he had noticed that the bill for the outsourced help desk had been increasing over the last few months. On top of it, Katherine over in development had heard that the Singaporean service provider was unable to resolve the erroneous transaction problems’.

It was clear to TIBO’s CEO that he was going to have to call in all the key players to get to the bottom of this issue. He asked Forsythe to set up a meeting for the next day. ‘Pyms, also shift that security meeting of the audit committee of the board of directors, will you please? I know we have all been getting seriously concerned about the fire-fighting approach to security after 11 September 2001 and the hacking and virus incidents, but we have got to solve the We-BOP problem first’.

‘Oh by the way, Steven, before you go, do you have an idea about whom we should call in as our guru on security for the audit committee meeting?’

‘You may recall, John, that we did put in a requisition for a senior CISO position, but the conclusion of the executive committee was that we could do without. I am still having a debate with internal audit, which is trying to pin that responsibility on me, because Erik and Roger could not agree on who it should be. We really have only Ida Doano, our security administrator, and Ida would really be out of her depth in a board meeting’.

On his way back to his office, De Haes kept thinking about how it all had started. IT had planned the We-BOP project but did not have the development capabilities or skills, given that most of the IT people are mainframe-oriented. During a golf game, De Haes heard from his friend at another financial company about a fabulous development company in Singapore that produces top-end, reusable, e-banking applications that could be used for outsourcing.

---

2 A consumer protection organisation—see appendix.
3 Chief information security officer
A contract was made based on the standard vendor’s agreements, negotiated by De Haes and Guldentops and signed by TIBO’s CEO. The bank’s legal department also reviewed the contract and some changes were made to its legal aspects. The service level agreement (SLA) of the outsourcing contract covered:

- The scope of the work
- Timeline definitions for development and rollout
- Performance, tracking and reporting
- Roles and responsibilities
- Payments and functionalities

The intention was for the third-party service provider to provide full e-banking services—including front-office functionality, interfaces to the back office and customer support functions—in two stages. At the first stage, customers would have access to their savings and chequing accounts. Functions to be integrated in the web application in the future were loans and credit cards. The back-office infrastructure had been developed internally and was operational.

When the application went into operation all went well for the small volume of users (5 percent of customer base). After six months, when the number of users grew, the following problems with the quality of service delivery began:

- Response time was unsatisfactory.
- Customers could access the system only during specific times of the day (availability of the system).
- Occasionally, transactions were not being processed or were processed erroneously.

As a result, the help desk received an increasing number of queries and complaints. The third-party supplier reported these complaints on a monthly basis and issued extra invoices because of the increase in support desk workload. Until now, these problems had not been escalated beyond the operational level, where they were solved by IT and business people by putting in overtime.

Before calling Guldentops, the COO, in Manila with an update on the We-BOP problem, De Haes was also reminded of poor Doano, a security administer who was overwhelmed with developing security procedures, getting acquainted with security tools, assigning administrator passwords for the business employees who wanted access to everything, and generating reports that did not provide the information needed and were read by few.

While the phone was ringing, De Haes also started mentally reshuffling his agenda for the next day. He really needed to have a word with Dean and his people about their lack of reaction to the firewall alarms and also with O’Donnell, who apparently knew the weakness existed. Then, there was the dreaded meeting about project priorities with Van Grembergen. De Haes needed to find a way to talk them out of their unreasonable expectations. Finally, Guldentops answered the phone.

‘Hi, Erik, I know it is near midnight in Manila, but we have a BIG problem ...’.

**TIBO’S PROFILE**

TIBO is a medium-sized financial institution with the following characteristics:

- Its core business competencies include retail banking—saving accounts, chequing accounts, loans, credit cards and personal banking—as well as performing clearing and settlement services for the other banks in the region. One of its strengths has been the personal attention provided to customers by account managers in the personal banking group.
- It is downsizing its physical branch network while aggressively pursuing e-banking business.
- It is starting to acquire outside IT services (outsource or joint venture).
- It has gone through several local mergers and, as a result, has a complex environment with shared IT services that are difficult to integrate.
- It is process-oriented with an emerging culture of stakeholder inclusion, but with no formal strategy and a tendency to shift priorities after long debates between stakeholders.
- It is competing in a market in which a number of changes have taken place, including an increased presence of building societies (savings and loans) and international banks. New products being introduced by competitors—including higher savings interest rates—are attractive to customers. In addition, electronic financial services with 24/7 access are becoming ubiquitous.
- It possesses a steady customer base and revenues, and increasing acquisitions to this point, but the effects of increased competition are being felt ever more strongly. There is concern over the loss of market share and compressed profit margins.
- It is aware of indicators that the regulators are getting concerned about systemic risk, as TIBO provides payment and settlement services to other banking institutions.

*See the summary of the SLA on p. 9.*
THE COMPANY’S IT ENVIRONMENT

Projects

TIBO projects include:

• **We-BOP**—Currently (partially live and outsourced), this includes customer access to savings and chequing applications; yet to be implemented are loan and credit card access, all with a single customer interface.

• **Customer relationship management (CRM)**—This will pull all customer information together to enable cross-selling of products, to support account managers and other customer support staff members.

• **Core business applications rebuilding (CoBAR)**—This primarily includes the savings, chequing and loan applications.

• **IT_Net**—Expanded IT network and standardised applications platforms

• **ForPay**—Foreign payment services

• **Work_it**—Workflow application and remote connectivity for account managers

Technology

The IT environment consists of three distinct platforms. The mainframe platform provides the CoBAR primary business and financial applications; these include savings, chequing, loans, trust, personal banking and credit card interface (an alliance with a major credit card firm). All are real-time applications with nightly batch updates. The organisation’s clearing-settlement application and accounting applications—general ledger, accounts payable, fixed assets and bank reconciliation—are also mainframe-based. The mainframe platform is also currently used for ForPay, as a service to other banks.

A new client-server environment consisting of five UNIX servers will form the basis for the new CRM application in its initial stages of development.

Connectivity to the corporate systems is provided by IT_Net, which is a virtual private network (VPN) supplied by the organisation’s telecommunications supplier. Overall, the networking infrastructure is getting older and strained. Only senior managers have laptops.

The PC network platform involves Windows servers utilised for file and print services, communication services, and gateway services. PC workstations are running Windows. This is the platform for the Work_it application. Remote connectivity is to be introduced based on features available in IT_Net.

Mainframe access is granted by a security administration system. UNIX security is provided by the host operating system; no proprietary security tools are used. Firewalls are installed and managed by the IT_Net supplier, as a managed service.

The headquarters is home to approximately 600 employees. Nationwide, the corporation employs approximately 9,000 people, and 450 of them are in IT. IT services are critical to all 600 headquarters employees.

Standards and Procedures

IT procedures are developed in-house, and vary in quality and conformance from area to area within the IT group. IT strategy development is relatively informal; it is based on management discussion and documented via management meeting notes, rather than determined by a prescribed process or any standard format. IT would like more guidance from the business and executive management, but strategic decisions are made on a project-by-project basis.

The IT organisation is fairly traditional, with a systems development team, an operations team, and a system and technology team. The management team consists of a manager for each of the three groups, plus the head of the department.

System developments have been undertaken mostly in-house, based on the mainframe, with a system development life cycle (SDLC) methodology that was acquired some years ago and has been adjusted to suit the bank. In recent years, these methods have been found to be outdated and too slow to undertake. However, they at least have ensured reasonable documentation of systems. There is little experience in acquiring packaged solutions. Only a few of the in-house team members have any experience with client-server systems, and none have any web development experience.
Operations are well organised with good discipline and tight procedures. Generally, all work is treated as high priority. There are shifts covering operations 24 hours a day, with a small overnight team that handles mostly batch processing. Internal SLAs are defined in technical terms and are really service level statements setting, for example, availability targets and capacity requirements for the network. There is a small internal help desk that is mostly used for occasional user queries and password resets.

**Security**

Security is based on a long-standing procedure, which is based on a traditional mainframe security administration system. The workstations are diskless. The simple, but not up-to-date, security policy states general responsibilities and the importance of privacy and security of banking data. IT has hardened servers, firewalls, strong encryption and a VPN. Token-based user authentication is supported by well-enforced security policies. There is a small security administration group that supports security maintenance and handles joiners, leavers and changes to access rights. There is no dedicated security manager, although a security administrator is responsible for the allocation and management of privileges. Because of business and technology pressures, people tend to be lax about security rules. Security is still addressed in a reactive mode, and the bank has sought *ad hoc* outside assistance, advice and third-party offerings. Prior to this point, the general opinion has been that there have been few issues to worry about.

**THE ORGANISATIONAL ENTITIES**

The following sections describe entities found in TIBO.

**Board of Directors**

The TIBO board of directors has the following attributes:
- The chairman of the board is not involved with the company on a daily basis.
- It is composed of both internal and external members, with the majority of audit committee members being external.
- The members are technically literate, but they are risk-conscious and interested in what ‘others’ do.

**Executive Committee**

The TIBO C-suite has the following attributes:
- It wields strong influence on the board, but needs the co-operation of external board directors.
- It is focused on achieving monetary results, and is somewhat risk-taking.
- It consists of a CEO, chief financial officer (CFO), COO and a business executive. The COO oversees IT as part of his duties.
- Control is not high on the priority list, but the executive committee will listen to audit and will push for recommendation implementation.
- It recently pushed for development of the web banking systems of the bank.

**Business Strategy Group**

The TIBO strategy group has the following attributes:
- It reports to the business executive and is not technologically inclined.
- Major priorities on its list are CRM and the CRM project.
- It has recently gone through a major downsizing exercise, reducing the branch offices by 50 percent.
- It has benchmarked IT cost in the enterprise’s business sector and found TIBO’s own IT to be more expensive than the competition’s.
- It wants positive net present value (NPV) on major IT infrastructure investments.

The current strategic initiatives are:
- Closing low-performing branches (almost complete)
- Creating a web-based banking system to unload the demand for services at branch offices (We-BOP) (in progress)
- Developing CRM capabilities to create opportunities to cross-sell banking services (project initiated)
**IT Co-ordination Committee**

The IT co-ordination committee involves a mix of IT and user managers (see figure 2, organisation chart). It meets monthly and is primarily concerned with the oversight of existing and future developments. It reports quarterly to the business strategy group. It has had little involvement with the We-BOP development because of the outsourced nature of its development and operation.

**IT Management**

The IT director and his management team are:
- Highly technical and want to make a mark in e-business, specifically through We-BOP, which they support strongly
- Concerned about the aging network, which may run out of capacity as a result of the move to e-banking
- Fully supportive of tight controls over IT
- In agreement that more co-operation is needed with the business strategy group, which generally supports IT management project priorities but does not always agree on what should be done first
- Firm believers that the current core systems can support the business for several more years, and are getting cranky when core systems rebuilding is suggested

**IT Teams**

The TIBO IT teams are:
- Highly qualified professionals with a strong quality focus; they have put strong project control and performance measurement in place. However, the latter is too detailed and used only at the local level.
- Constantly diverted by change management issues as a result of many changes to the applications and infrastructure
- Concerned about rapid change, especially the outsourcing and business-promoted projects that are not always commercially successful and take resources away from needed infrastructure investments, such as the new IT network to increase connectivity and standardise solutions
- Concerned with the increase in maintenance problems and decrease in available skills relative to the core systems, and becoming increasingly frustrated

**Business Operational**

TIBO executives are:
- Becoming IT-literate and are a bit jealous of IT getting its budgets while they have had to downsize
- Claiming they need increased remote connectivity and automated workflow solutions to be effective in a downsized branch network
- Complaining about throughput of, and support for, core systems and pushing for SLAs and the rebuilding of the soon-to-be-obsolete core systems
- Connecting more and more e-customers even if they do not bring in immediate income, whilst stressing the operational and support systems
Figure 2—Organisation Charts

Executive Committee

John A. Mitchell
CEO

Pyms Forsythe
Assistant to the
CEO

Roger Debreceny
CFO

Erik Guldentops
COO

William Lux
Senior VP of
Wholesale

Wim Van
Grembergen
Senior VP of
Retail

Erik Guldentops
COO

Steven De Haes
Directory of Information Technology

Kelly Youngman
Director of Project Management

Ed O'Donnell
Director of Operations

James Thomas
Systems and Technology

Linda Wogelius
Director of Development

Scott Summers
Chief Technical Officer

Tyra Leigh
Quality Assurance

Marie Hanna
Systems Operations

Joshua Dean
User Support

Erika Escalante
Internal Networks

Katherine Noel
Applications Development

Andrew Joseph
Technology Acquisitions

Seungi Hong Min
Project Manager

Mercedes Mora
IT Budgeting

Nathan Tuple
Data Administrator

Jacob Samuel
External Networks

Alan Lord
Systems Support

Weng Chi
Technology Standards and Architecture

Ida Doano
Security Administrator

Pradash Takanti
Hardware Support

IT Co-ordinating Committee

Ed O'Donnell
Director of Operations (Chair)

Linda Wogelius
Director of Development

June Poor
Assistant Vice President of Wholesale Banking

Kelly Youngman
Director of Project Management

Max Rich
Assistant Vice President of Retail Banking
## Purpose of This Document
This document constitutes an agreement between the outsourcer and the third party, defined in the next section, for the development of full e-banking services referred to as ‘We-BOP.’ It details the environment, expectations, deliverables and responsibilities associated with the implementation of this agreement.

## Parties in the Agreement
This agreement, dated as of February 200x, is between TIBO© with offices located in … (hereafter named as ‘the outsourcer’) and …., with offices located in … (hereafter named as the ‘third-party supplier’).

## Scope of Work
The scope of this agreement is for the third-party supplier to develop a full e-banking service, We-BOP. This service includes:

- The development of a web-based front office with following functionalities:
  - Access to savings account
  - Access to chequing account
  - Credit card administration
  - Loan administration
- The development of the interfaces between the front office and the back office of the outsourcer
- The setup of customer support functions (help desk) for the developed We-BOP application

## Timeline Definitions for Development and Rollout
The We-BOP application and its interface will be developed in two phases:

- **Phase 1:** To be operational 30 April 200x
  - A web-based front office enabling:
    - Access to savings account
    - Access to chequing account
  - The interface between the front office and the back office of the outsourcer
- **Phase 2:** To be operational 31 March 200x+1
  - Extended functionalities of the web-based front office:
    - Credit cards
    - Loans

## Performance Tracking and Reporting
### We-BOP
The third party will report quarterly on the performance of the We-BOP system. This report will be sent to the IT director of the outsourcer.

### Help Desk
The third party will report monthly regarding the help desk requests and how they are solved. This report will be sent to the IT director of the outsourcer. A specific error file, which can be accessed directly by the outsourcer, will be developed by the third party to keep track of and manage the reported errors.

## Roles and Responsibilities
### Communication
Contacts and communication between the outsourcer and the third party are by electronic mail, telephone and regular meetings. The outsourcer and the third party must communicate their group structure (and changes) to each other, so each group can maintain correct distribution lists. The outsourcer and the third party must inform each other of planned unavailability (e.g., meetings, holidays, replacements, backup specialists).

### Responsibilities of the Outsourcer
The outsourcer must provide to the third party all information regarding the back-office specifications necessary to establish the interface between the front office and the back office. The third party must be informed on all major changes to the back office that could impact the interface. The outsourcer will respond promptly—within five working days—to any of the third party’s requests to provide information or decisions that are reasonably necessary for the third party to develop the system and to provide the services.

### Responsibilities of the Third Party
The third party warrants that the development of the We-BOP systems and the customer support function will be performed in a professional and workman-like manner consistent with industry standards reasonably applicable to such services.

The third party will not disclose any confidential information about the outsourcer that it may obtain during the development process.

### Payment and Penalties
For the development of the web-based application, the outsourcer will pay the third party as follows:

- 25 percent at the start of the project
- 50 percent after delivery of phase 1
- 25 percent after delivery of phase 2

For the help desk, the third party will charge a monthly fixed price of US $ xxxx.xx.

If the web-based application cannot be delivered within the agreed timeline, a penalty of US $ xxxx.xx per day of delay will be charged by the outsourcer to the third party.

All fees are to be paid by the outsourcer, in the currency of the invoice, to the account designated by the third party. All invoices are payable within 30 days from the date of the invoice. If the invoice is not settled within 30 days of receipt, the third party may add an interest and administrative charge of 1.5 percent of the respective invoice.

## Signatures

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO of the Outsourcer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEO of the Third Party</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. ADDITIONAL MATERIAL

THE SECURITY ISSUE

Questions

1. In an anonymous call to the CFO, someone claims to have access to customer information leaked from the enterprise systems, and substantiates it with a fax containing sensitive information (names, account managers, etc.).
   • Analyse the security risks.
   • Recommend some good practices to better mitigate the risks.

2. You are informed that the breach occurred at the third party and are given a copy of the current (short and inadequate) SLA. The data leaked because the third party used live customer data during acceptance tests of the second phase on an insecure web server installation.
   • Define what management should have put into the SLA relative to security.
   • What do you think actually happened to allow these data to get into the public domain?

THE OUTSOURCING ISSUE

Questions

1. You are confronted here with a detailed outsourcing process. Give an evaluation of this process. Describe the problems TIBO encountered or the risks it faces, and identify best practices that, if implemented, would have prevented or alleviated the problems or risks.

2. Identify the roles that audit, IT management and the CEO should play in outsourcing. Compare these best practices to the roles actually played in TIBO.

THE STRATEGIC ALIGNMENT ISSUE

Extra Background Information

Business strategy is determined by the business strategy group, which is composed of the CEO, vice presidents of retail and wholesale operations, and two outside members. One of the outside members is Charles Penrose, the former CEO of Accubank. Accubank was merged into TIBO 18 months ago. The other outside member is Nigel Sorrell. He is also a member of the board of directors.

The business strategy group meets on the first Tuesday of each month to review progress on prior strategic initiatives and discuss the strategic direction of the bank. Information for progress reviews is usually obtained by inviting the project manager of the particular initiative to give a short presentation. The group tries to be aware of developments that may disrupt industry practices. In particular, the group has been thinking about:

• Channel strategies
• Current trends
• Customer relations and retention

The business strategy group has excellent documentation procedures. It maintains a strategic initiatives document that details each of the initiatives and charts progress on each. This document is distributed to the board of directors and the executive committee.

The executive committee meets on the first Thursday of each month. A discussion of strategic issues is always included on the executive committee’s agenda. John Mitchell always makes sure that the bank’s strategic direction is given adequate attention.

The board of directors (see figure 4) meets quarterly. Strategic initiatives are always amongst the many items discussed by the board.

Strategic decisions are passed down in the organisation for implementation. For example, the We-BOP initiative was passed to the director of IT for implementation. The director of IT assigned a project manager and then started looking for potential solutions for the We-BOP initiative. He decided that the safest way to enter the e-banking arena was to outsource this functionality.
Questions

1. Analyse the governance implications of how TIBO handled outsourcing from the board of directors, executive and IT management levels. What would be the best practices to govern outsourcing contracts?

2. Why was the CEO not aware of the customer complaints before the report from the ombudsman? How can this be avoided in the future? What governance changes do you propose to solve this problem?

3. As the board begins the CRM initiative, how could better alignment be achieved between IT and business strategy than was evident in the We-BOP initiative?
APPENDIX 1—FINANCIAL OMBUDSMAN SERVICE

The Financial Ombudsman Service is a powerful UK regulatory service that can help with a financial complaint that cannot be sorted out with a:

- Bank
- Building society
- Financial advisor
- Friendly society or credit union
- Insurance company
- Investment firm
- Stockbroker
- Unit trust company

The Financial Ombudsman Service was set up by law to give consumers a free, independent service for resolving disputes with financial firms. It can help with most financial complaints about:

- Banking services
- Credit cards
- Endowment policies
- Financial and investment advice
- Insurance policies
- Investment and fund management
- Life insurance
- Mortgages
- Personal pension plans
- Savings plans and accounts
- Stocks and shares
- Unit trusts and income bonds

It can impose fines, but the real impact of such incidents is the embarrassment resulting from the reports being made public.
APPENDIX 2—COBIT CONTROL OBJECTIVES AND MATURITY MODELS

PO1 DEFINE A STRATEGIC IT PLAN

Process Description

IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders’ understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource requirements, and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.

PO1.1 IT Value Management
Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programmes that have solid business cases. Recognise that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds. IT processes should provide effective and efficient delivery of the IT components of programmes and early warning of any deviations from plan, including cost, schedule or functionality, that might impact the expected outcomes of the programmes. IT services should be executed against equitable and enforceable SLAs. Accountability for achieving the benefits and controlling the costs should be clearly assigned and monitored. Establish fair, transparent, repeatable and comparable evaluation of business cases, including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits.

PO1.2 Business-IT Alignment
Establish processes of bi-directional education and reciprocal involvement in strategic planning to achieve business and IT alignment and integration. Mediate between business and IT imperatives to establish mutually agreed-upon priorities.

PO1.3 Assessment of Current Capability and Performance
Assess the current capability and performance of solution and service delivery to establish a baseline against which future requirements can be compared. Define performance in terms of IT’s contribution to business objectives, functionality, stability, complexity, costs, strengths and weaknesses.

PO1.4 IT Strategic Plan
Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise’s strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans.

PO1.5 IT Tactical Plans
Create a portfolio of tactical IT plans that are derived from the IT strategic plan. The tactical plans should address IT-enabled programme investments, IT services and IT assets. The tactical plans should describe required IT initiatives, resource requirements, and how the use of resources and achievement of benefits will be monitored and managed. The tactical plans should be sufficiently detailed to allow the definition of project plans. Actively manage the set of tactical IT plans and initiatives through analysis of project and service portfolios.

PO1.6 IT Portfolio Management
Actively manage with the business the portfolio of IT-enabled investment programmes required to achieve specific strategic business objectives by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling programmes. This should include clarifying desired business outcomes, ensuring that programme objectives support achievement of the outcomes, understanding the full scope of effort required to achieve the outcomes, assigning clear accountability with supporting measures, defining projects within the programme, allocating resources and funding, delegating authority, and commissioning required projects at programme launch.
Maturity Model

Management of the process Define a strategic IT plan that satisfies the business requirement for IT of sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks is:

0 Non-existent when 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 when
the need for IT strategic planning is known by IT management. IT planning is performed on an as-needed basis in response to a specific business requirement. IT strategic planning is occasionally discussed at IT management meetings. The alignment of business requirements, applications and technology takes place reactively rather than by an organisationwide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 Repeatable but Intuitive when
IT strategic planning is shared with business management on an as-needed basis. Updating of the IT plans occurs in response to requests by management. 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 recognised in an intuitive way.

3 Defined when
a policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach that 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. 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 influence the acquisition of new products and technologies. IT strategic planning is discussed at business management meetings.

4 Managed and Measurable when
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. Management is able to monitor the IT strategic planning process, 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 organisationwide strategy are increasingly becoming more co-ordinated by addressing business processes and value-added capabilities and leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for determining the usage of internal and external resources required in system development and operations.

5 Optimised when
IT strategic planning is a documented, living process; is continuously considered in business goal setting; and results in discernible business value through investments in IT. Risk and value-added considerations are continuously updated in the IT strategic planning process. Realistic long-range IT plans are developed and constantly updated to reflect changing technology and business-related developments. Benchmarking against well-understood and reliable industry norms takes place and is integrated with the strategy formulation process. The strategic plan includes how new technology developments can drive the creation of new business capabilities and improve the competitive advantage of the organisation.
P09 ASSESS AND MANAGE IT RISKS

Process Description

A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.

P09.1 IT Risk Management Framework
Establish an IT risk management framework that is aligned to the organisation’s (enterprise’s) risk management framework.

P09.2 Establishment of Risk Context
Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include determining the internal and external context of each risk assessment, the goal of the assessment, and the criteria against which risks are evaluated.

P09.3 Event Identification
Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry.

P09.4 Risk Assessment
Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.

P09.5 Risk Response
Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.

P09.6 Maintenance and Monitoring of a Risk Action Plan
Prioritise and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution. Obtain approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s). Monitor execution of the plans, and report on any deviations to senior management.
**Maturity Model**

Management of the process *Assess and manage IT risks that satisfies the business requirement for IT of analysing and communicating IT risks and their potential impact on business processes and goals* is:

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

1  **Initial/Ad Hoc** when IT risks are considered in an *ad hoc* manner. Informal assessments of project risk take place as determined by each project. Risk assessments are sometimes identified in a project plan but are rarely assigned to specific managers. 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 seldom discussed at management meetings. Where risks have been considered, mitigation is inconsistent. There is an emerging understanding that IT risks are important and need to be considered.

2  **Repeatable but Intuitive** when a developing risk assessment approach exists and is implemented at the discretion of the project managers. The risk management is usually at a high level and is typically applied only to major projects or in response to problems. Risk mitigation processes are starting to be implemented where risks are identified.

3  **Defined** when an organisationwide risk management policy defines when and how to conduct risk assessments. Risk management follows a defined process that is documented, and risk management training is available to all staff members. Decisions to follow the risk management process and receive training are left to the individual’s discretion. The methodology for the assessment of risk is convincing and sound and ensures that key risks to the business are identified. A process to mitigate key risks is usually instituted once the risks are identified. Job descriptions consider risk management responsibilities.

4  **Managed and Measurable** when the assessment and management of risk are standard procedures. Exceptions to the risk management process are reported to IT management. IT risk management is a senior management-level responsibility. Risk is assessed and mitigated at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the business and IT environment that could significantly affect the IT-related risk scenarios. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. All identified risks have a nominated owner, and senior management and IT management determine the levels of risk that the organisation will tolerate. IT management develops standard measures for assessing risk and defining risk/return ratios. Management budgets for an operational risk management project to reassess risks on a regular basis. A risk management database is established, and part of the risk management processes is beginning to be automated. IT management considers risk mitigation strategies.

5  **Optimised** when risk management develops to the stage where a structured, organisationwide process is enforced and well managed. Good practices 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. Management detects and acts when major IT operational and investment decisions are made without consideration of the risk management plan. Management continually assesses risk mitigation strategies.
PO10 MANAGE PROJECTS

Process Description

A programme and project management framework for the management of all IT projects is established. The framework ensures the correct prioritisation and co-ordination of all projects. It includes a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, quality assurance (QA), a formal test plan, and testing and post-implementation review after installation to ensure project risk management and value delivery to the business. This approach reduces the risk of unexpected costs and project cancellations, improves communications to and involvement of business and end users, ensures the value and quality of project deliverables, and maximises their contribution to IT-enabled investment programmes.

PO10.1 Programme Management Framework
Maintain the programme of projects related to the portfolio of IT-enabled investment programmes by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling projects. Ensure that the projects support the programme’s objectives. Co-ordinate the activities and interdependencies of multiple projects, manage the contribution of all the projects within the programme to expected outcomes, and resolve resource requirements and conflicts.

PO10.2 Project Management Framework
Establish and maintain a project management framework that defines the scope and boundaries of managing projects, as well as the method to be adopted and applied to each project undertaken. The framework and supporting method should be integrated with the programme management processes.

PO10.3 Project Management Approach
Establish a project management approach commensurate with the size, complexity and regulatory requirements of each project. The project governance structure can include the roles, responsibilities and accountabilities of the programme sponsor, project sponsors, steering committee, project office and project manager, and the mechanisms through which they can meet those responsibilities (such as reporting and stage reviews). Make sure all IT projects have sponsors with sufficient authority to own the execution of the project within the overall strategic programme.

PO10.4 Stakeholder Commitment
Obtain commitment and participation from the affected stakeholders in the definition and execution of the project within the context of the overall IT-enabled investment programme.

PO10.5 Project Scope Statement
Define and document the nature and scope of the project to confirm and develop amongst stakeholders a common understanding of project scope and how it relates to other projects within the overall IT-enabled investment programme. The definition should be formally approved by the programme and project sponsors before project initiation.

PO10.6 Project Phase Initiation
Approve the initiation of each major project phase and communicate it to all stakeholders. Base the approval of the initial phase on programme governance decisions. Approval of subsequent phases should be based on review and acceptance of the deliverables of the previous phase, and approval of an updated business case at the next major review of the programme. In the event of overlapping project phases, an approval point should be established by programme and project sponsors to authorise project progression.

PO10.7 Integrated Project Plan
Establish a formal, approved integrated project plan (covering business and information systems resources) to guide project execution and control throughout the life of the project. The activities and interdependencies of multiple projects within a programme should be understood and documented. The project plan should be maintained throughout the life of the project. The project plan, and changes to it, should be approved in line with the programme and project governance framework.

PO10.8 Project Resources
Define the responsibilities, relationships, authorities and performance criteria of project team members, and specify the basis for acquiring and assigning competent staff members and/or contractors to the project. The procurement of products and services required for each project should be planned and managed to achieve project objectives using the organisation’s procurement practices.
PO10.9 Project Risk Management
Eliminate or minimise specific risks associated with individual projects through a systematic process of planning, identifying, analysing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change. Risks faced by the project management process and the project deliverable should be established and centrally recorded.

PO10.10 Project Quality Plan
Prepare a quality management plan that describes the project quality system and how it will be implemented. The plan should be formally reviewed and agreed to by all parties concerned and then incorporated into the integrated project plan.

PO10.11 Project Change Control
Establish a change control system for each project, so all changes to the project baseline (e.g., cost, schedule, scope and quality) are appropriately reviewed, approved and incorporated into the integrated project plan in line with the programme and project governance framework.

PO10.12 Project Planning of Assurance Methods
Identify assurance tasks required to support the accreditation of new or modified systems during project planning, and include them in the integrated project plan. The tasks should provide assurance that internal controls and security features meet the defined requirements.

PO10.13 Project Performance Measurement, Reporting and Monitoring
Measure project performance against key project performance scope, schedule, quality, cost and risk criteria. Identify any deviations from the plan. Assess the impact of deviations on the project and overall programme, and report results to key stakeholders. Recommend, implement and monitor remedial action, when required, in line with the programme and project governance framework.

PO10.14 Project Closure
At the end of each project, require the project stakeholders to ascertain whether the project delivered the planned results and benefits. Identify and communicate any outstanding activities required to achieve the planned results of the project and the benefits of the programme, and identify and document lessons learned for use on future projects and programmes.
**Maturity Model**

Management of the process *Manage projects* that satisfies the business requirement for IT of ensuring the delivery of project results within agreed-upon time frames, budget and quality is:

0  **Non-existent** when 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** when
   the use of project management techniques and approaches within IT is a decision left to individual IT managers. There is a lack of management commitment to project ownership and project management. Critical decisions on project management 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 for the management of projects. Roles and responsibilities for the management of projects are not defined. Projects, schedules and milestones are poorly defined, if at all. Project staff time and expenses are not tracked and compared to budgets.

2  **Repeatable but Intuitive** when
   senior management gains and communicates an awareness of the need for IT project management. The organisation is in the process of developing and utilising some 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. Initial guidelines are developed for many aspects of project management. Application of project management guidelines is left to the discretion of the individual project manager.

3  **Defined** when
   the IT project management process and methodology are established and communicated. IT projects are defined with appropriate business and technical objectives. Senior IT and business management are beginning to be committed and involved in the management of IT projects. A project management office is established within IT, with initial roles and responsibilities defined. IT projects are monitored, with defined and updated milestones, schedules, budget and performance measurements. Project management training is available and is primarily a result of individual staff initiatives. QA procedures and post-system implementation activities are defined, but are not broadly applied by IT managers. Projects are beginning to be managed as portfolios.

4  **Managed and Measurable** when
   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 with project team members trained on enhancements. IT management implements a project organisation structure with documented roles, responsibilities and staff performance criteria. Criteria for evaluating success at each milestone are established. Value and risk are measured and managed prior to, during and after the completion of projects. Projects increasingly address organisation goals, rather than only IT-specific ones. There is strong and active project support from senior management sponsors as well as stakeholders. Relevant project management training is planned for staff members in the project management office and across the IT function.

5  **Optimised** when
   a proven, full life cycle project and programme methodology is implemented, enforced and integrated into the culture of the entire organisation. An ongoing initiative to identify and institutionalise best project management practices is implemented. An IT strategy for sourcing development and operational projects is defined and implemented. An integrated project management office is responsible for projects and programmes from inception to post-implementation. Organisationwide planning of programmes and projects ensures that user and IT resources are best utilised to support strategic initiatives.
AI2 ACQUIRE AND MAINTAIN APPLICATION SOFTWARE

Process Description

Applications are made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the development and configuration in line with standards. This allows organisations to properly support business operations with the correct automated applications.

A12.1 High-level Design
Translate business requirements into a high-level design specification for software acquisition, taking into account the organisation’s technological direction and information architecture. Have the design specifications approved by management to ensure that the high-level design responds to the requirements. Reassess when significant technical or logical discrepancies occur during development or maintenance.

A12.2 Detailed Design
Prepare detailed design and technical software application requirements. Define the criteria for acceptance of the requirements. Have the requirements approved to ensure that they correspond to the high-level design. Perform reassessment when significant technical or logical discrepancies occur during development or maintenance.

A12.3 Application Control and Auditability
Implement business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorised and auditable.

A12.4 Application Security and Availability
Address application security and availability requirements in response to identified risks and in line with the organisation’s data classification, information architecture, information security architecture and risk tolerance.

A12.5 Configuration and Implementation of Acquired Application Software
Configure and implement acquired application software to meet business objectives.

A12.6 Major Upgrades to Existing Systems
In the event of major changes to existing systems that result in significant change in current designs and/or functionality, follow a similar development process as that used for the development of new systems.

A12.7 Development of Application Software
Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards, QA requirements, and approval standards. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties.

A12.8 Software Quality Assurance
Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation’s quality policies and procedures.

A12.9 Applications Requirements Management
Track the status of individual requirements (including all rejected requirements) during the design, development and implementation, and approve changes to requirements through an established change management process.

A12.10 Application Software Maintenance
Develop a strategy and plan for the maintenance of software applications.
Maturity Model

Management of the process Acquire and maintain application software that satisfies the business requirement for IT of aligning available applications with business requirements, and doing so in a timely manner and at a reasonable cost is:

0  **Non-existent** when 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** when
There is an awareness that a process for acquiring and maintaining applications is required. Approaches to acquiring and maintaining application software vary from project to project. A variety of individual solutions to particular business requirements is likely to have been acquired independently, resulting in inefficiencies with maintenance and support.

2  **Repeatable but Intuitive** when
there are different, but similar, processes for acquiring and maintaining applications based on the expertise within the IT function. 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 is lost from the organisation. There is little consideration of application security and availability in the design or acquisition of application software.

3  **Defined** when
a clear, defined and generally understood process exists for the acquisition and maintenance of application software. This process is aligned with IT and business strategy. An attempt is made to apply the documented processes consistently across different applications and projects. The methodologies are generally inflexible and difficult to apply in all cases, so steps are likely to be bypassed. Maintenance activities are planned, scheduled and co-ordinated.

4  **Managed and Measurable** when
there is a formal and well-understood methodology that includes a design and specification process, criteria for acquisition, a process for testing and requirements for documentation. Documented and agreed-upon approval mechanisms exist to ensure that all steps are followed and exceptions are authorised. Practices and procedures evolve and are well suited to the organisation, used by all staff members and applicable to most application requirements.

5  **Optimised** when
application software acquisition and maintenance practices are aligned with the defined process. The approach is component-based, with predefined, standardised applications matched to business needs. The approach is enterprisewide. The acquisition and maintenance methodology is well advanced and enables rapid deployment, allowing for high responsiveness and flexibility in responding to changing business requirements. The application software acquisition and implementation methodology is subjected to continuous improvement and is supported by internal and external knowledge databases containing reference materials and good practices. The methodology creates documentation in a predefined structure that makes production and maintenance efficient.
DS2 MANAGE THIRD-PARTY SERVICES

Process Description

The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as by reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimizes the business risk associated with non-performing suppliers.

DS2.1 Identification of All Supplier Relationships
Identify all supplier services, and categorize them according to supplier type, significance and criticality. Maintain formal documentation of technical and organizational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.

DS2.2 Supplier Relationship Management
Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).

DS2.3 Supplier Risk Management
Identify and mitigate risks relating to suppliers’ ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.

DS2.4 Supplier Performance Monitoring
Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.
Maturity Model

Management of the process Manage third-party services that satisfies the business requirement for IT of providing satisfactory third-party services whilst being transparent about benefits, costs and risks is:

0 Non-existent when 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 when
management is aware of the need to have documented policies and procedures for third-party management, including signed contracts. There are no standard terms of agreement with service providers. Measurement of the services provided is informal and reactive. Practices are dependent on the experience (e.g., on demand) of the individual and the supplier.

2 Repeatable but Intuitive when
the process for overseeing third-party service providers, associated risks and the delivery of services is informal. A signed, pro forma contract is used with standard vendor terms and conditions (e.g., the description of services to be provided). Reports on the services provided are available, but do not support business objectives.

3 Defined when
well-documented procedures are in place to govern third-party services, with clear processes for vetting and negotiating with vendors. When an agreement for the provision of services is made, 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 legal, operational and control requirements. The responsibility for oversight of third-party services is assigned. Contractual terms are based on standardised templates. The business risk associated with the third-party services is assessed and reported.

4 Managed and Measurable when
formal and standardised criteria are established for defining the terms of engagement, including scope of work, services/deliverables to be provided, assumptions, schedule, costs, billing arrangements and responsibilities. Responsibilities for contract and vendor management are assigned. Vendor qualifications, risks and capabilities are verified on a continual basis. Service requirements are defined and linked to business objectives. A process exists to review service performance against contractual terms, providing input to assess current and future third-party services. Transfer pricing models are used in the procurement process. All parties involved are aware of service, cost and milestone expectations. Agreed-upon key performance indicators (KPIs) and key goal indicators (KGI) for the oversight of service providers exist.

5 Optimised when
contracts signed with third parties are reviewed periodically at predefined intervals. The responsibility for managing suppliers and the quality of the services provided is assigned. Evidence of contract compliance to operational, legal and control provisions is monitored, and corrective action is enforced. The third party is subject to independent periodic review, and feedback on performance is provided and used to improve service delivery. Measurements vary in response to changing business conditions. Measures support early detection of potential problems with third-party services. Comprehensive, defined reporting of service level achievement is linked to the third-party compensation. Management adjusts the process of third-party service acquisition and monitoring based on the outcome of KPIs and KGI.
DS5 ENSURE SYSTEMS SECURITY

Process Description

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, plans, and procedures. Security management also includes performing security monitoring and periodic testing, and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.

DS5.1 Management of IT Security
Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.

DS5.2 IT Security Plan
Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.

DS5.3 Identity Management
Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs, and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

DS5.4 User Account Management
Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

DS5.5 Security Testing, Surveillance and Monitoring
Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise’s information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection, and subsequent timely reporting, of unusual and/or abnormal activities that may need to be addressed.

DS5.6 Security Incident Definition
Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process.

DS5.7 Protection of Security Technology
Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily.

DS5.8 Cryptographic Key Management
Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

DS5.9 Malicious Software Prevention, Detection and Correction
Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from viruses, worms, spyware, spam, etc.
DS5.10 Network Security
Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion
detection) to authorise access and control information flows from and to networks.

DS5.11 Exchange of Sensitive Data
Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of
submission, proof of receipt and non-repudiation of origin.
Maturity Model

Management of the process Ensure systems security that satisfies the business requirements for IT of maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents is:

0 Non-existent when 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 for IT security breaches. There is a complete lack of a recognisable system security administration process.

1 Initial/Ad Hoc when the organisation recognises the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive when responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analysed. Services from third parties may not address the specific security needs of the organisation. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT, and the business does not see IT security as within its domain.

3 Defined when security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. Ad hoc security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business, but is only informally scheduled and managed.

4 Managed and Measurable when responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and procedures are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorisation are standardised. Security certification is pursued for staff members who are responsible for the audit and management of security. Security testing is completed using standard and formalised processes, leading to improvements of security levels. IT security processes are co-ordinated with an overall organisation security function. IT security reporting is linked to business objectives. IT security training is conducted in both the business and IT, and is planned and managed in a manner that responds to business needs and defined security risk profiles. KGI and KPIs for security management have been defined but are not yet measured.

5 Optimised when 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 an approved security plan. Users and customers are increasingly accountable for defining security requirements, and security functions are integrated with applications at the design stage. Security incidents are promptly addressed with formalised incident response procedures supported by automated tools. Periodic security assessments are conducted to evaluate the effectiveness of the implementation of the security plan. Information on threats and vulnerabilities is systematically collected and analysed. Adequate controls to mitigate risks are promptly communicated and implemented. Security testing, root cause analysis of security incidents and proactive identification of risk are used for continuous process improvements. Security processes and technologies are integrated organisationwide. KGI and KPIs for security management are collected and communicated. Management uses KGI and KPIs to adjust the security plan in a continuous improvement process.
DS6 IDENTIFY AND ALLOCATE COSTS

Process Description

The need for a fair and equitable system of allocating IT costs to the business requires accurate measurement of IT costs and agreement with business users on fair allocation. This process includes building and operating a system to capture, allocate and report IT costs to the users of services. A fair system of allocation enables the business to make more informed decisions regarding the use of IT services.

DS6.1 Definition of Services
Identify all IT costs and map them to IT services to support a transparent cost model. IT services should be linked to business processes such that the business can identify associated service billing levels.

DS6.2 IT Accounting
Capture and allocate actual costs according to the enterprise cost model. Variances between forecasts and actual costs should be analysed and reported on, in compliance with the enterprise’s financial measurement systems.

DS6.3 Cost Modelling and Charging
Establish and use an IT costing model based on the service definitions that support the calculation of chargeback rates per service. The IT cost model should ensure that charging for services is identifiable, measurable and predictable by users to encourage proper use of resources.

DS6.4 Cost Model Maintenance
Regularly review and benchmark the appropriateness of the cost/recharge model to maintain its relevance and appropriateness to the evolving business and IT activities.
Maturity Model

Management of the process Identify and allocate costs that satisfies the business requirement for IT of ensuring transparency and understanding of IT costs and improving cost-efficiency through well-informed use of IT services is:

0 Non-existent when
there is a complete lack of any recognisable process for identifying and allocating costs with respect to information services provided. The organisation does not even recognise 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 when
there is a general understanding of the overall costs for information services, but there is no breakdown of costs per user, customer, department, groups of users, service functions, projects or deliverables. There is virtually no cost monitoring, with only aggregate cost reporting to management. IT costs are allocated as an operational overhead. Business is provided with no information on the cost or benefits of service provision.

2 Repeatable but Intuitive when
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. There is no formal training or communication on standard cost identification and allocation procedures. Responsibility for the collection or allocation of costs is not assigned.

3 Defined when
there is a defined and documented information services cost model. A process for relating IT costs to the services provided to users is defined. An appropriate level of awareness exists regarding the costs attributable to information services. The business is provided with rudimentary information on costs.

4 Managed and Measurable when
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 if cost deviations are detected. Information services cost reporting is linked to business objectives and SLAs and is monitored by business process owners. A finance function reviews the reasonableness of the cost allocation process. An automated cost accounting system exists, but is focused on the information services function rather than on business processes. KPIs and KGIs are agreed to for cost measurement but are inconsistently measured.

5 Optimised when
costs of services provided are identified, captured, summarised and reported to management, business process owners and users. Costs are identified as chargeable items and could support a chargeback system that appropriately bills users for services provided, based on utilisation. Cost details support SLAs. The monitoring and evaluation of costs of services are used to optimise the cost of IT resources. Cost figures obtained are used to verify benefit realisation and 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 is refined to a level of industry practice, based on the result of continuous improvement and benchmarking with other organisations. Cost optimisation is an ongoing process. Management reviews KPIs and KGIs as part of a continuous improvement process in redesigning cost measurement systems.
ME1 MONITOR AND EVALUATE IT PERFORMANCE

Process Description

Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, reporting performance in a timely and systematic manner, and acting promptly upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.

ME1.1 Monitoring Approach
Establish a general monitoring framework and approach to define the scope, methodology and process to be followed for measuring IT's solution and service delivery, and monitor IT's contribution to the business. Integrate the framework with the corporate performance management system.

ME1.2 Definition and Collection of Monitoring Data
Work with the business to define a balanced set of performance targets, and have them approved by the business and other relevant stakeholders. Define benchmarks with which to compare the targets, and identify available data to be collected to measure the targets. Establish processes to collect timely and accurate data to report on progress against targets.

ME1.3 Monitoring Method
Deploy a performance monitoring method (e.g., balanced scorecard) that records targets; captures measurements; provides a succinct, all-around view of IT performance; and fits within the enterprise monitoring system.

ME1.4 Performance Assessment
Periodically review performance against targets, analyse the cause of any deviations, and initiate remedial action to address the underlying causes. At appropriate times, perform root cause analysis across deviations.

ME1.5 Board and Executive Reporting
Develop senior management reports on IT's contribution to the business, specifically in terms of the performance of the enterprise’s portfolio, IT-enabled investment programmes, and the solution and service deliverable performance of individual programmes. Include in status reports the extent to which planned objectives have been achieved, budgeted resources used, set performance targets met and identified risks mitigated. Anticipate senior management's review by suggesting remedial actions for major deviations. Provide the report to senior management, and solicit feedback from their review.

ME1.6 Remedial Actions
Identify and initiate remedial actions based on performance monitoring, assessment and reporting. This includes follow-up of all monitoring, reporting and assessments through review, negotiation and establishment of management responses; assignment of responsibility for remediation; and tracking of the results of actions committed.
Maturity Model

Management of the process Monitor and evaluate IT performance that satisfies the business requirement for IT of transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with governance requirements is:

0 Non-existent when
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 when
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. The accounting function monitors basic financial measures for IT.

2 Repeatable but Intuitive when
basic measurements to be monitored are identified. Collection and assessment methods and techniques exist, but the processes are not adopted across the entire organisation. Interpretation of monitoring results is based on the expertise of key individuals. Limited tools are chosen and implemented for gathering information, but the gathering is not based on a planned approach.

3 Defined when
management communicates and institutes standard monitoring processes. Educational and training programmes for monitoring are implemented. A formalised knowledge base of historical performance information is developed. Assessment is still performed at the individual IT process and project level and is not integrated amongst all processes. Measurements of the contribution of the information services function to the performance of the organisation are defined, using traditional financial and operational criteria. IT-specific performance measurements, non-financial measurements, strategic measurements, customer satisfaction measurements and service levels are defined. A framework is defined for measuring performance.

4 Managed and Measurable when
management defines the tolerances under which processes must operate. Reporting of monitoring results is standardised and normalised. There is integration of metrics across all IT projects and processes. The IT organisation's management reporting systems are formalised. Automated tools are integrated and leveraged organisationwide to collect and monitor operational information on applications, systems and processes. Management is able to evaluate performance based on agreed-upon criteria approved by stakeholders. Measurements of the IT function align with organisationwide goals.

5 Optimised when
a continuous quality improvement process is developed for updating organisationwide monitoring standards and policies and incorporating industry good practices. All monitoring processes are optimised and support organisationwide objectives. Business-driven metrics are routinely used to measure performance and are integrated into strategic assessment frameworks, such as the IT balanced scorecard. Process monitoring and ongoing redesign are consistent with organisationwide business process improvement plans. Benchmarking against industry and key competitors becomes formalised, with well-understood comparison criteria.
ME2 MONITOR AND EVALUATE INTERNAL CONTROL

Process Description

Establishing an effective internal control programme for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.

ME2.1 Monitoring of the Internal Control Framework
Continuously monitor, benchmark and improve the IT control environment and control framework to meet organisational objectives.

ME2.2 Supervisory Review
Monitor and evaluate the efficiency and effectiveness of internal IT managerial review controls.

ME2.3 Control Exceptions
Identify control exceptions, and analyse and identify their underlying root causes. Escalate control exceptions and report to stakeholders appropriately. Institute necessary corrective action.

ME2.4 Control Self-assessment
Evaluate the completeness and effectiveness of management’s control over IT processes, policies and contracts through a continuing programme of self-assessment.

ME2.5 Assurance of Internal Control
Obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews.

ME2.6 Internal Control at Third Parties
Assess the status of external service providers’ internal controls. Confirm that external service providers comply with legal and regulatory requirements and contractual obligations.

ME2.7 Remedial Actions
Identify, initiate, track and implement remedial actions arising from control assessments and reporting.
Maturity Model

Management of the process Monitor and evaluate internal control that satisfies the business requirement for IT of protecting the achievement of IT objectives and complying with IT-related laws and regulations is:

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

1  **Initial/Ad Hoc** when
management recognises the need for regular IT management and 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 the 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** when
the organisation uses informal control reports to initiate corrective action initiatives. Internal control assessment is dependent on the skill sets of key individuals. The organisation has an increased awareness of internal control monitoring. Information service management performs monitoring over the effectiveness of what it believes are critical internal controls on a regular basis. Methodologies and tools for monitoring internal controls are starting to be used, but not based on a plan. Risk factors specific to the IT environment are identified based on the skills of individuals.

3  **Defined** when
management supports and institutes internal control monitoring. Policies and procedures are developed for assessing and reporting on internal control monitoring activities. An education and training programme for internal control monitoring is defined. A process is defined for self-assessments and internal control assurance reviews, with roles for responsible business and IT 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. Process-specific risks and mitigation policies are defined.

4  **Managed and Measurable** when
management implements a framework for IT internal control monitoring. The organisation establishes tolerance levels for the internal control monitoring process. Tools are implemented to standardise assessments and automatically detect control exceptions. A formal IT internal control function is established, with specialised and certified professionals utilising a formal control framework endorsed by senior management. Skilled IT staff members are routinely participating in internal control assessments. A metrics knowledge base for historical information on internal control monitoring is established. Peer reviews for internal control monitoring are established.

5  **Optimised** when
management establishes an organisationwide continuous improvement programme that takes into account lessons learned and industry good practices for internal control monitoring. The organisation uses integrated and updated tools, where appropriate, that allow effective assessment of critical IT controls and rapid detection of IT control monitoring incidents. Knowledge sharing, specific to the information services function, is formally implemented. Benchmarking against industry standards and good practices is formalised.
COBIT AND RELATED PRODUCTS

The COBIT framework, in versions 4.0 and higher, includes all of the following:

- **Framework**—Explains how COBIT organises IT governance, management and control objectives and good practices by IT domains and processes, and links them to business requirements
- **Process descriptions**—Include 34 IT processes covering the IT responsibility areas from beginning to end
- **Control objectives**—Provide generic best practice management objectives for IT processes
- **Management guidelines**—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- **Maturity models**—Provide profiles of IT processes describing possible current and future states

In the years since its inception, COBIT’s core content has continued to evolve, and the number of COBIT-based derivative works has increased. Following are the publications currently derived from COBIT:

- **Board Briefing on IT Governance, 2nd Edition**—Designed to help executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
- **COBIT Online**—Allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys; frequently asked questions; benchmarking; and a discussion facility for sharing experiences and questions.
- **COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition**—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with the IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition.
- **IT Assurance Guide: Using COBIT®—Provides guidance on how COBIT can be used to support a variety of assurance activities and offers suggested testing steps for all the COBIT IT processes and control objectives. It replaces the information in the Audit Guidelines for auditing and self-assessment against the control objectives in COBIT 4.1.
- **IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition**—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives
- **IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition**—Provides a generic road map for implementing IT governance using COBIT and Val IT resources and offers a supporting tool kit
- **COBIT® Quickstart**—Provides a baseline of control for the smaller organisation and a possible first step for the larger enterprise
- **COBIT® Security Baseline**—Focuses on essential steps for implementing information security within the enterprise
- **COBIT® mappings**—Currently posted at www.isaca.org/downloads:
  - Aligning COBIT®, ITIL and ISO 17799 for Business Benefit
  - COBIT® Mapping: Overview of International IT Guidance, 2nd Edition
  - COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0
  - COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0
  - COBIT® Mapping: Mapping of ITIL With COBIT® 4.0
  - COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0
  - COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0
  - COBIT® Mapping: Mapping of SEI’s CMM for Software With COBIT® 4.0
  - COBIT® Mapping: Mapping of TOGAF 8.1 for Software With COBIT® 4.0

Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Current Val IT-related publications are:

- **Enterprise Value: Governance of IT Investments—The Val IT™ Framework**, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into:
  - Three processes—Value Governance, Portfolio Management and Investment Management
  - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as COBIT’s control objectives.
- **Enterprise Value: Governance of IT Investments—The Business Case**, which focuses on one key element of the investment management process
- **Enterprise Value: Governance of IT Investments—The ING Case Study**, which describes how a global financial services company manages a portfolio of IT investments in the context of the Val IT framework

For the most complete and up-to-date information on COBIT, Val IT and related products, case studies, training opportunities, newsletters, and other framework-specific information, visit www.itgi.org, www.isaca.org/cobit and www.isaca.org/valit.