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, optimizes 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™: Caselets, 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 any proper procedures and tests or exclusive of any 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: Caselets.

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™: Caselets, 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™: Caselets, 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 978-1-60420-027-0
IT Governance Using COBIT® and Val IT™: Caselets, 2nd Edition
Printed in the United States of America
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 Guldenstaps, 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, University of Antwerp Management School, 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 KiIoD, 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 Saul, 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 Jogani, 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 Saul, CSP, Great-West Life Assurance and IGM Financial, Canada

ITGI Advisory Panel
Ronald Saul, 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 De Haes, 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. Steupening, CISA, PricewaterhouseCoopers LLC, Belgium
Robert E. Stroud, CA Inc., USA

ITGI Affiliates and Sponsors
ISACA chapters
American Institute of 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
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. Caselet: Jayhawk Medical Supply Inc. ............................................................................................................... 3
   Learning Objective ........................................................................................................................................ 3
   Case Information ......................................................................................................................................... 3
   Case Question ............................................................................................................................................ 3
   Control Objectives and Procedures for Evaluating Effectiveness ................................................................. 4

3. Caselet: Delta Lighting Design ......................................................................................................................... 9
   Learning Objective ....................................................................................................................................... 9
   Case Information ....................................................................................................................................... 9
   Case Questions ......................................................................................................................................... 9
   Control Objectives and Procedures for Evaluating Effectiveness ................................................................. 10

4. Caselet: International Communications Company ......................................................................................... 24
   Learning Objective ..................................................................................................................................... 24
   Case Information ..................................................................................................................................... 24
   Case Questions ....................................................................................................................................... 25
   Control Objectives and Procedures for Evaluating Effectiveness ................................................................. 25

5. Caselet: Union National Bank ......................................................................................................................... 37
   Learning Objective ..................................................................................................................................... 37
   Case Information ..................................................................................................................................... 37
   Case Questions ....................................................................................................................................... 37
   Control Objectives and Procedures for Evaluating Effectiveness ................................................................. 38

6. Caselet: Lux Insurance Brokers ......................................................................................................................... 45
   Learning Objective ..................................................................................................................................... 45
   Case Information ..................................................................................................................................... 45
   Case Questions ....................................................................................................................................... 46
   Control Objectives and Procedures for Evaluating Effectiveness ................................................................. 47

7. Caselet: Phoenix Electric Provider ..................................................................................................................... 54
   Learning Objective ..................................................................................................................................... 54
   Case Information ..................................................................................................................................... 54
   Case Questions ....................................................................................................................................... 55
   Control Objectives and Procedures for Evaluating Effectiveness ................................................................. 56

**ComT and Related Products** ............................................................................................................................. 66

Underlined titles are contained in this sample.
1. PURPOSE OF THIS DOCUMENT

Caselets, 2nd Edition, is a product of ITGI (www.itgi.org), and part of the IT Governance Using COBIT® and Val IT™ series. This document was developed in collaboration with a group of international academics and practitioners. These caselets provide three mini case studies on COBIT use in lifelike situations and are designed for use as small exercises (90-minute class period) in undergraduate and graduate classes on information systems (IS) management, information security management, auditing, IS auditing and/or accounting information systems. The objectives of these cases are to:

- Provide a foundation for students to identify risks and control areas in a rich information technology environment
- Provide a means for students to relate risks and controls to particular COBIT control objectives
- Help students learn how to use the COBIT assurance guidelines to identify appropriate procedures when developing methodologies for providing assurance over controls

Caselets, 2nd Edition, includes a case description for each caselet, which provides background on the case organisation and its IT processes and infrastructure, as well as potential questions for the students. Caselets, 2nd Edition—Teaching Notes supplies extra background information for the instructor, and suggestions on answers.

There are three other components that make up IT Governance Using COBIT® and Val IT™. The Student Book, 2nd Edition, explains and illustrates all the COBIT components, the Presentation, 2nd Edition, provides a PowerPoint deck of 35 slides explaining all the COBIT elements, and the TIBO Case Study, 2nd Edition, applies COBIT knowledge in a practical situation.

Pages 3 through 36 deleted from this sample.
5. CASELET: UNION NATIONAL BANK

LEARNING OBJECTIVE

Determine the COBIT control objectives to be used in implementing a customer relationship management (CRM) package.

CASE INFORMATION

Union National Bank (UNB) has history on its side. With well-established roots, the 149-year-old community bank has a reputation for old-fashioned customer service. However, it has recently found itself competing not only with other well-established local banks but also with giant conglomerates. The bank attempted to compete on price by lowering fees, discounting loan rates and inflating deposit rates, while still offering its hands-on customer service, but management discovered that was a money-losing move and decided to try another strategy.

During the current fiscal year, the seven-branch UNB embarked on a major change in its processes, products and pricing to stay profitable and still retain its customer-centric reputation by acquiring a CRM package. The CRM solution allows UNB to look more closely at not only its big-picture financials but also its profitability by customer. Management segmented the bank’s 37,000 accounts by profitability and drilled down into individual household information to get a view of spending and account activity. Management then fed all bank transactions into a single data warehouse, where they could be analysed later to pinpoint the most important products to its clients. The software alerts member service representatives (assigned to individual accounts) to life changes that may indicate an interest in another financial product. For example, recently married customers may be interested in mortgage services and customers who are nearing 65 years of age may be interested in retirement products. The CRM solution also helps the bank remain on customers’ good sides by asking how and when to contact them. This increases the likelihood of a positive response to a sales pitch. The bank has achieved more than US $1 million in efficiency gains, stemmed customer erosion and realised substantial revenue growth.

Management is using the CRM system tools to evaluate the profit of its bank customers by analysing all associated costs and revenue associated with each customer’s behaviour. Did customers visit tellers often or opt for less-expensive ATM and Internet transactions? How many cheques were written each month? Was there other revenue associated with customer accounts from optional services or extra fees? By segmenting its customer base into high-value and low-value buckets, the bank was able to segment its customer base into high-value and low-value buckets, as well as high-profit and low-profit sectors, and increase the profitability of the high-profit segment. The CRM solution also helps the bank remain on customers’ good sides by asking how and when to contact them. This increases the likelihood of a positive response to a sales pitch. The bank has achieved more than US $1 million in efficiency gains, stemmed customer erosion and realised substantial revenue growth.

The CRM solution enables management to figure out what new products it can safely introduce without competing with its existing offerings. For example, UNB recently used the system to help roll out its new savings account program. It hoped the year-end, high-minimum, short-term, high-interest offering would attract lucrative new customers with more than US $5,000 to invest. Management was able to use the CRM system to figure out how many accounts contained more than the minimum balance, the difference in rates of interest, and the potential financial loss if some or all of them switched to the new higher-rate account. Management could then balance that potential loss against potential new revenue.

CASE QUESTIONS

You are the external auditor for UNB.

1. Employ the PO1 Define a strategic IT plan COBIT process to:
   a. Identify which of the PO1 control objectives are most appropriate for you to consider in designing your audit plan. Be prepared to justify your selection of the relevant control objectives.
   b. For three of the control objectives that you chose in (1a), employ the COBIT process assurance steps for PO1 to develop a draft set of audit procedures to provide assurance on the achievement of these control objectives.

2. Employ the PO10 Manage projects COBIT process to:
   a. Identify which of the PO10 control objectives are most appropriate for you to consider in designing your audit plan. Be prepared to justify your selection of the relevant control objectives.
   b. For three of the control objectives that you chose in (2a), employ the COBIT process assurance steps for PO10 to develop a draft set of audit procedures to provide assurance on the achievement of these control objectives.

3. Employ the ME1 Monitor and evaluate IT performance COBIT process to:
   a. Identify which of the ME1 control objectives are most appropriate for you to consider in designing your audit plan. Be prepared to justify your selection of the relevant control objectives.
   b. For three of the control objectives that you chose in (3a), employ the COBIT process assurance steps for ME1 to develop a draft set of audit procedures to provide assurance on the achievement of these control objectives.
### Control Objectives and Procedures for Evaluating Effectiveness

**P01.4 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 the 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.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Establish a process to translate business strategy, business expectations, and current and future IT capabilities into an IT strategic plan.</td>
<td>• Enquire whether and confirm that a process was followed to document IT’s goals and objectives necessary to perform its tasks. They should be defined, documented and communicated, including the:</td>
</tr>
<tr>
<td>2 Ensure that IT has established a process to identify, document and adequately address organisational changes, technology evolution, regulatory requirements, business process re-engineering, staffing, in- and outsourcing opportunities, etc., in the planning process.</td>
<td>— Achievement of the benefits and management of the risks of the IT capabilities</td>
</tr>
<tr>
<td>3 Define roles and responsibilities of the stakeholders involved in the strategic planning process.</td>
<td>— Establishment of the current and future performance required to respond to business expectations</td>
</tr>
<tr>
<td>4 Develop IT capabilities to support the business requirements and contribute to expected benefits as included in the enterprise’s strategic plan.</td>
<td>— Provision of information on transparency and how IT delivers value to the business</td>
</tr>
<tr>
<td>5 Identify and document the implications on the business strategy in terms of risk and cost of the required IT capabilities. Resolve negative implications appropriately in co-ordination with the business.</td>
<td>• Enquire whether and confirm that there is a time frame for the development and execution of the strategic and tactical plans. This time frame should include the interrelationships and dependencies of the execution of the tactical plans. The time frame could vary based on scope, funding and prioritisation.</td>
</tr>
<tr>
<td>6 Define and document the IT goals and objectives necessary to cost-efficiently:</td>
<td>• Enquire whether and confirm that a process to capture outcome measures, represented by metrics (what) and targets (how much), of IT objectives exists and that the measures relate to business-identified benefits and the strategy’s direction.</td>
</tr>
<tr>
<td>• Achieve the benefits and manage the risks of the capabilities required of IT</td>
<td>• Confirm and review the policies and procedures supporting the structured planning approach to determine if they effectively support the process for creating an IT strategic plan.</td>
</tr>
<tr>
<td>• Establish the current and future performance required to respond to business expectations</td>
<td></td>
</tr>
<tr>
<td>• Provide transparency on capabilities delivered by IT and their contribution to strategic objectives</td>
<td></td>
</tr>
<tr>
<td>7 Translate the business-derived IT objectives into outcome measures represented by metrics (what) and targets (how much) that can be related to business benefits. Obtain appropriate stakeholder approval.</td>
<td></td>
</tr>
<tr>
<td>8 Formally approve and communicate the IT strategic plan and ensure that it is clearly understood by those who need to translate it into budgets, tactical plans, sourcing and acquisition strategies, processes, and organisational structures.</td>
<td></td>
</tr>
</tbody>
</table>
### P01.5 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.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Translate the approved IT strategic plan into tactical plans.</td>
<td>• Enquire whether and confirm that tactical IT plans exist and that they have been based on the IT strategic plan.</td>
</tr>
<tr>
<td>2. Ensure that the process of developing tactical plans allows for considerations to update strategic IT plans.</td>
<td>• Confirm that this is done in a structured manner in accordance with established processes and that there is no undue delay between updates of the strategic plan and the subsequent update of the tactical plans.</td>
</tr>
<tr>
<td>3. Ensure that the content of the tactical plans includes clearly stated project definitions for all programmes, project time frames and deliverables, required resources, and business benefits to be monitored.</td>
<td>• Validate that the contents of the IT tactical plan are adequate and that the plan contains proper project definitions, planning information, deliverables and quantified estimated benefits.</td>
</tr>
<tr>
<td>4. Explicitly state goal and performance indicators, goals risk assessment results, and related risk mitigation plans within the IT tactical plans.</td>
<td>• Review whether the tactical plan addresses IT-related risk.</td>
</tr>
<tr>
<td>5. Base the planning and elaboration of the IT-enabled investment programmes, IT projects, resources utilisation and monitoring techniques on the detailed tactical plan.</td>
<td></td>
</tr>
<tr>
<td>6. Determine that formal and comprehensive periodic review and change management processes exist to ensure that any changes made to the organisation’s mission and objectives are reflected in the IT tactical plans.</td>
<td></td>
</tr>
<tr>
<td>7. Use a methodology for a formal review of IT strategic and tactical plans to optimise current and future investments and strategies, in terms of the use of scarce resources, implementation alternatives, funding methods and timing.</td>
<td></td>
</tr>
</tbody>
</table>

### P010.7 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.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Develop a project plan that provides information to enable management to control project progress. The plan should include details of project deliverables, required resources and responsibilities, clear work breakdown structures and work packages, estimates of resources required, milestones, key dependencies, and identification of a critical path. Identify interdependencies of resources (e.g., key personnel) and deliverables with other projects.</td>
<td>• Review plans, policies and procedures to verify that the integrated project plan provides information to permit management to control project progress and that the plan includes a statement of scope, details of project products and deliverables, required resources and responsibilities, clear work breakdown structures and work packages, estimates of resources required, milestones, key dependencies, and identification of a critical path.</td>
</tr>
<tr>
<td>2. Maintain the project plan and any dependent plans to ensure that they are up to date and reflect actual progress and material changes.</td>
<td>• Enquire whether and ensure that the integrated project plan and any dependent plans are updated with the agreement plan owner to reflect the actual progress and material changes from master project plan checkpoints.</td>
</tr>
<tr>
<td>3. Ensure that there is effective communication of project plans and progress reports amongst all projects and with the overall programme. Ensure that any changes made to individual plans are reflected in the other plans.</td>
<td>• Enquire whether and confirm that the project plan includes a communication plan that addresses changes and status reporting to key stakeholders.</td>
</tr>
</tbody>
</table>
### P010.8 Project Resources

**Definition:** 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.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identify resource needs for the project and clearly map out appropriate roles and responsibilities, with escalation and decision-making authorities agreed upon and understood.</td>
<td>• Enquire whether and confirm that resource needs are identified for the project and appropriate roles and responsibilities are clearly mapped out, with escalation and decision-making authorities agreed to and understood.</td>
</tr>
<tr>
<td>2. Identify required skills and time requirements for all individuals involved in the project phases in relation to defined roles. Staff the roles based on available skills information (e.g., IT skills matrix).</td>
<td>• Enquire whether and confirm that roles are identified and staffed with appropriate personnel.</td>
</tr>
<tr>
<td>3. Utilise experienced project management and team leader resources with skills appropriate to the size, complexity and risk of the project.</td>
<td>• Enquire whether and confirm that an experienced project management resource and team leader are utilised, with skills appropriate to the size, complexity and risk of the project being undertaken.</td>
</tr>
<tr>
<td>4. Consider and clearly define the roles and the responsibilities of other involved parties, including finance, legal, procurement, human resources, internal audit and compliance.</td>
<td>• Inspect plans, policies and procedures to verify that the roles and responsibilities of other interested parties are considered and clearly defined (e.g., interested parties include, but are not limited to, internal audit, compliance, finance, legal, procurement and human resources).</td>
</tr>
<tr>
<td>5. Clearly define and agree upon the responsibility for procurement and management of third-party products and services, and manage the relationships.</td>
<td>• Enquire whether and confirm that responsibility for procurement and management of third-party project and system support relationships is clearly defined.</td>
</tr>
</tbody>
</table>

### P010.14 Project Closure

**Definition:** 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.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Define and apply key steps for project closure, including post-implementation reviews that assess whether a project attained the desired results and benefits.</td>
<td>• Enquire whether and confirm that IT policies and procedures include key steps for project closure, including an effective post-implementation review.</td>
</tr>
<tr>
<td>2. Plan and execute post-implementation reviews to determine if projects delivered expected benefits and to improve the project management and system development process methodology.</td>
<td>• Inspect documentation of a sample of post-implementation reviews to determine if the reviews are effectively planned and executed.</td>
</tr>
<tr>
<td>3. Identify, assign, communicate and track any uncompleted activities required to achieve planned programme project results and benefits.</td>
<td>• Walk through the process used to identify, communicate and track any uncompleted activities required to achieve project programme benefits.</td>
</tr>
<tr>
<td>4. Collect from the project participants and reviewers the lessons learned and key activities that led to delivered benefits. Analyse the data and make recommendations for improving the project management method for future projects.</td>
<td>• Inspect post-implementation documentation to determine if uncompleted activities are identified, communicated and resolved.</td>
</tr>
<tr>
<td></td>
<td>• Walk through the process used to collect lessons learned to determine if the process is effective in improving future projects. Assess customer involvement in the review and analysis process.</td>
</tr>
</tbody>
</table>
**CASELET: UNION NATIONAL BANK**

**AI7.1 Training**—Train the staff members of the affected user departments and the operations group of the IT function in accordance with the defined training and implementation plan and associated materials, as part of every information systems development, implementation or modification project.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. For systems development, implementation or modification projects, a training plan is an integral part of the overall project master plan. Ensure that the plan clearly identifies learning objectives, resources, key milestones, dependencies and critical path tasks impacting the delivery of the training plan. The plan should consider alternative training strategies depending on the business needs, risk level (e.g., for mission-critical systems, a formal system of user accreditation and reaccreditation may be appropriate), and regulatory and compliance requirements (e.g., impact of varying privacy laws may require adaptation of the training at a national level).</td>
<td>• Enquire whether and confirm that a training plan is part of the overall project master plan for development projects.</td>
</tr>
<tr>
<td>2. Ensure that the training plan identifies and addresses all impacted groups, including business end users, IT operations, support and IT application development training, and service providers. The training plan should incorporate the delivery of the training in a timely manner. It should also identify staff members who must be trained and those for whom training is desirable.</td>
<td>• Inspect training documentation to determine compliance to the training plan (e.g., list of staff members invited to training, attendees list, evaluation forms for the achievement of learning objectives and other feedback).</td>
</tr>
<tr>
<td>3. Consider alternative training strategies that satisfy the training requirements, and select the most cost-effective approach that aligns with the organisation’s training framework. Alternative strategies include train the trainer, end-user accreditation and intranet-based training.</td>
<td>• Enquire whether and confirm that there is a process of monitoring training to obtain feedback that could lead to potential improvements in the system.</td>
</tr>
<tr>
<td>4. Confirm that there is a process to ensure that the training plan is executed satisfactorily. Complete the documentation detailing compliance with the training plan. Examples of information include lists of staff members invited to attend the training, attendees, evaluations of achievement of learning objectives and other feedback.</td>
<td>• Enquire whether and confirm that planned changes are monitored to ensure that training requirements are considered and suitable plans are created.</td>
</tr>
<tr>
<td>5. Monitor training to obtain feedback that could lead to potential improvements in either the training or the system.</td>
<td></td>
</tr>
<tr>
<td>6. Monitor all planned changes to ensure that training requirements have been considered and suitable plans created. Consider postponing the change if training has not been performed and if the lack of training would jeopardise the implementation of the change.</td>
<td></td>
</tr>
</tbody>
</table>
### A17.2 Test Plan

Establish a test plan based on organisationwide standards that defines roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Develop and document the test plan, which aligns to the project quality plan and relevant organisational standards. Communicate and consult with appropriate business process owners and IT stakeholders.</td>
<td>• Enquire whether and confirm that a test plan is developed and documented in accordance with the project quality plan and relevant organisational standards and that it is communicated to appropriate business owners and IT stakeholders.</td>
</tr>
<tr>
<td>2 Ensure that the test plan reflects an assessment of risks from the project and that all functional and technical requirements are tested. Based on assessment of the risk of system failure and faults on implementation, the plan should include requirements for performance, stress, usability, pilot and security testing.</td>
<td>• Enquire whether and confirm that the test plan reflects an assessment of the project’s risks and that all functional and technical testing requirements are included.</td>
</tr>
<tr>
<td>3 Ensure that the test plan addresses the potential need for internal or external accreditation of outcomes of the test process (e.g., financial regulatory requirements).</td>
<td>• Enquire whether and confirm that the test plan identifies resources to execute the tests and evaluate test results.</td>
</tr>
<tr>
<td>4 Ensure that the test plan identifies the necessary resources to execute testing and evaluate the results. Examples of resources include construction of test environments and staff for the test group, including potential temporary replacement of test staff in the production or development environments. Ensure that stakeholders are consulted on the resource implications of the test plan.</td>
<td>• Confirm that stakeholders are consulted on resource implications of the test plan.</td>
</tr>
<tr>
<td>5 Ensure that the test plan identifies testing phases appropriate to the operational requirements and environment. Examples of such testing phases include unit test, system test, integration test, user acceptance test, performance test, stress test, data conversion test, security test, operational readiness, and backup and recovery tests.</td>
<td>• Enquire whether and confirm that the test plan considers test preparation, including site preparation, training requirements, installation or update of a defined test environment, planning/performance/documentation/retention of test cases; error and problem handling, correction and escalation; and formal approval.</td>
</tr>
<tr>
<td>6 Confirm that the test plan considers test preparation (including site preparation), training requirements, installation or an update of a defined test environment, planning/performance/documenting/retaining test cases, error and problem handling, correction and escalation, and formal approval.</td>
<td>• Enquire whether and confirm that the test plan establishes clear criteria for measuring the success of undertaking each testing phase and that consultations with the business process owners and IT stakeholders are considered in defining the success criteria.</td>
</tr>
<tr>
<td>7 Ensure that the test plan establishes clear criteria for measuring the success of undertaking each testing phase. Consult the business process owners and IT stakeholders in defining the success criteria. Determine that the plan establishes remediation procedures when the success criteria are not met (e.g., in case of significant failures in a testing phase, the plan provides guidance on whether to proceed to the next phase, stop testing or postpone implementation).</td>
<td>• Determine if the plan establishes remediation procedures when the success criteria are not met (e.g., in case of significant failures in a testing phase, the plan provides guidance on whether to proceed to the next phase, stop testing or postpone implementation).</td>
</tr>
<tr>
<td>8 Confirm that all test plans are approved by stakeholders, including business process owners and IT, as appropriate. Examples of such stakeholders are application development managers, project managers and business process end users.</td>
<td>• Enquire whether and confirm that test plans are approved by stakeholders, including business process owners and IT, as appropriate. Examples of other stakeholders are application development managers, project managers and business process end users.</td>
</tr>
</tbody>
</table>
### Caselet: Union National Bank

#### 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.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
</table>
| 1. Define targets for the IT metrics in line with the coverage and characteristics of the metrics defined in the monitoring framework. Obtain IT and business management approval for the targets. | • Enquire whether and confirm that:  
  - Targets have been defined for the IT metrics in line with the coverage and characteristics of the metrics defined in the monitoring framework. Obtain IT and business management approval for the targets.  
  - Performance data needed by the monitoring approach are collected satisfactorily and in an automated fashion, wherever feasible. Verify that the measured performance is compared to the targets at agreed-to intervals.  
  - There is a process to control all changes to performance monitoring data sources  
  - Performance targets have been defined and focus on those that provide the largest insight-to-effort ratio  
  - The integrity of the data collected is assessed by carrying out reconciliation and control checks at agreed-upon intervals |
| 2. Collect performance data needed by the monitoring approach in an automated fashion wherever feasible. Compare the measured performance to the targets at agreed-to intervals. |  
  - Performance data needed by the monitoring approach are collected satisfactorily and in an automated fashion, wherever feasible. Verify that the measured performance is compared to the targets at agreed-to intervals. |
| 3. Ensure consistency, completeness and integrity of performance monitoring source data. Ensure control over all changes to performance monitoring data sources. |  
  - There are procedures for ensuring consistency, completeness and integrity of performance monitoring source data  
  - Performance targets have been defined and focus on those that provide the largest insight-to-effort ratio  
  - The integrity of the data collected is assessed by carrying out reconciliation and control checks at agreed-upon intervals |
| 4. Define performance targets and focus on those that provide the largest insight-to-effort ratio. |  
  - The integrity of the data collected is assessed by carrying out reconciliation and control checks at agreed-upon intervals |
| 5. Assess the integrity of the data collected by carrying out reconciliation and control checks at agreed-upon intervals. |  
  - The integrity of the data collected is assessed by carrying out reconciliation and control checks at agreed-upon intervals |

#### 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.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
</table>
| 1. Compare the performance values to internal targets and benchmarks and, where possible, to external benchmarks (industry and key competitors). | • Interview process owners to confirm that target performance levels for key processes are established and validated against the industry and competition.  
  • Inspect performance reports for timeliness of measurement and effectiveness of comparison to the targets.  
  • Verify that informal feedback is obtained and used for service delivery and/or reporting improvements.  
  • Analyse performance reports to verify that results are consistently assessed against targets at agreed-to intervals and that relevant stakeholders receive reporting data.  
  • Inspect evidence of performance assessment, and determine if the assessment and analysis are complete and effective.  
  • For an appropriate sample, verify that causes are identified and translated into remedial actions that are assigned to someone with the appropriate authority and resource and followed up appropriately.  
  • Enquire whether and confirm that root causes are periodically identified across deviations and appropriately acted upon. |
| 2. Consider implementing in parallel with the performance management system a less formal feedback mechanism to obtain alternative measures of perceived performance. Use the data to improve the performance measurement system and, where necessary, solution and service delivery. |  
  • Interview process owners to confirm that target performance levels for key processes are established and validated against the industry and competition.  
  • Inspect performance reports for timeliness of measurement and effectiveness of comparison to the targets.  
  • Verify that informal feedback is obtained and used for service delivery and/or reporting improvements.  
  • Analyse performance reports to verify that results are consistently assessed against targets at agreed-to intervals and that relevant stakeholders receive reporting data.  
  • Inspect evidence of performance assessment, and determine if the assessment and analysis are complete and effective.  
  • For an appropriate sample, verify that causes are identified and translated into remedial actions that are assigned to someone with the appropriate authority and resource and followed up appropriately.  
  • Enquire whether and confirm that root causes are periodically identified across deviations and appropriately acted upon. |
| 3. Assess performance against targets and analyse results. Compare measured performance to targets at agreed-to intervals. Ensure that performance targets and results are communicated to IT and senior and business management via the established performance monitoring framework. |  
  • Interview process owners to confirm that target performance levels for key processes are established and validated against the industry and competition.  
  • Inspect performance reports for timeliness of measurement and effectiveness of comparison to the targets.  
  • Verify that informal feedback is obtained and used for service delivery and/or reporting improvements.  
  • Analyse performance reports to verify that results are consistently assessed against targets at agreed-to intervals and that relevant stakeholders receive reporting data.  
  • Inspect evidence of performance assessment, and determine if the assessment and analysis are complete and effective.  
  • For an appropriate sample, verify that causes are identified and translated into remedial actions that are assigned to someone with the appropriate authority and resource and followed up appropriately.  
  • Enquire whether and confirm that root causes are periodically identified across deviations and appropriately acted upon. |
| 4. Analyse the cause of deviations against targets, initiate remedial actions, assign responsibilities for remediation, and follow up. At appropriate times, review all deviations and search for root causes, where necessary. Document the issues for further guidance if the problem recurs. Collect and retain the appropriate evidence and documentation to support the analysis. |  
  • Interview process owners to confirm that target performance levels for key processes are established and validated against the industry and competition.  
  • Inspect performance reports for timeliness of measurement and effectiveness of comparison to the targets.  
  • Verify that informal feedback is obtained and used for service delivery and/or reporting improvements.  
  • Analyse performance reports to verify that results are consistently assessed against targets at agreed-to intervals and that relevant stakeholders receive reporting data.  
  • Inspect evidence of performance assessment, and determine if the assessment and analysis are complete and effective.  
  • For an appropriate sample, verify that causes are identified and translated into remedial actions that are assigned to someone with the appropriate authority and resource and followed up appropriately.  
  • Enquire whether and confirm that root causes are periodically identified across deviations and appropriately acted upon. |
| 5. Where feasible, link achievement of performance targets to the organisational reward compensation system. |  
  • Interview process owners to confirm that target performance levels for key processes are established and validated against the industry and competition.  
  • Inspect performance reports for timeliness of measurement and effectiveness of comparison to the targets.  
  • Verify that informal feedback is obtained and used for service delivery and/or reporting improvements.  
  • Analyse performance reports to verify that results are consistently assessed against targets at agreed-to intervals and that relevant stakeholders receive reporting data.  
  • Inspect evidence of performance assessment, and determine if the assessment and analysis are complete and effective.  
  • For an appropriate sample, verify that causes are identified and translated into remedial actions that are assigned to someone with the appropriate authority and resource and followed up appropriately.  
  • Enquire whether and confirm that root causes are periodically identified across deviations and appropriately acted upon. |
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 have been used, set performance targets have been met and identified risks have been mitigated. Anticipate senior management’s review by suggesting remedial actions for major deviations. Provide the report to senior management, and solicit feedback from management’s review.

<table>
<thead>
<tr>
<th>Control Practices</th>
<th>Assurance Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Establish a board and executive reporting process, based on the performance</td>
<td>• Enquire whether and confirm that a board and executive reporting process</td>
</tr>
<tr>
<td>monitoring framework, for regular, accurate and timely reporting on IT’s</td>
<td>has been established.</td>
</tr>
<tr>
<td>contribution to the business by measuring achievement of IT goals, mitigation of</td>
<td>• Verify that the reporting covers IT’s contribution to the business by</td>
</tr>
<tr>
<td>IT risks and the usage of resources.</td>
<td>measuring achievement of IT goals, mitigation of IT risks and the usage of</td>
</tr>
<tr>
<td>2 Design senior management reports to highlight key issues (positive and</td>
<td>resources and that it is based on the performance monitoring framework</td>
</tr>
<tr>
<td>negative) generally relating to IT’s contribution to the business and</td>
<td>(e.g., balanced scorecards, trending analysis, executive dashboards).</td>
</tr>
<tr>
<td>specifically to IT solution and service delivery capability and performance.</td>
<td>• Confirm that board and executive reports are based on consolidated</td>
</tr>
<tr>
<td>3 Consolidate results of IT performance measurement. Translate them into</td>
<td>information of IT performance measurement.</td>
</tr>
<tr>
<td>business performance impacts (positive or negative) and incorporate the results</td>
<td>• Verify that there is a process in place to manage report versions and</td>
</tr>
<tr>
<td>into standard periodic reports to the board. Clearly link IT performance</td>
<td>iterations.</td>
</tr>
<tr>
<td>measurement to business outcomes and identify how IT supports business strategy.</td>
<td></td>
</tr>
</tbody>
</table>
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.
- **IT Control Objectives for Sarbanes-Oxley, The Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition**—Provides guidance on how to assess 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 With COBIT® 4.0
- **Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition**—Presents information security in business terms and contains tools and techniques to help uncover security-related problems

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.isaca.org/cobit](http://www.isaca.org/cobit) and [www.isaca.org/valit](http://www.isaca.org/valit).