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
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, CMCP, 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 KIoD, 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 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 Schirmbrandon, 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
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. **Case Study Description**
   - A Day in the Life of the Outsourcing Story of TIBO
   - TIBO’s Profile
   - The Company’s IT Environment
     - Projects
     - Technology
     - Standards and Procedures
     - Security
   - The Organisational Entities
     - Board of Directors
     - Executive Committee
     - Business Strategy Group
     - IT Co-ordination Committee
     - IT Management
     - IT Teams
     - Business Operational

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

**Appendix 1** — Financial Ombudsman Service

**Appendix 2** — COBIT Control Objectives and Maturity Models

**COBIT and Related Products**

Underlined titles are contained in this sample.
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 ITTM*. 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 ITTM: 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 ITTM* 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

---

<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</td>
<td>Relevant Additional Material (see teaching notes)</td>
</tr>
<tr>
<td></td>
<td>Outsourcing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Strategic Alignment</td>
<td></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.

\footnote{A consumer protection organisation—see appendix.}
\footnote{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 administrator 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**

And pages 5 through 9 deleted from this sample.
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

And pages 11 through 32 deleted from the sample.
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
• 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

COBIT and Related Products

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.