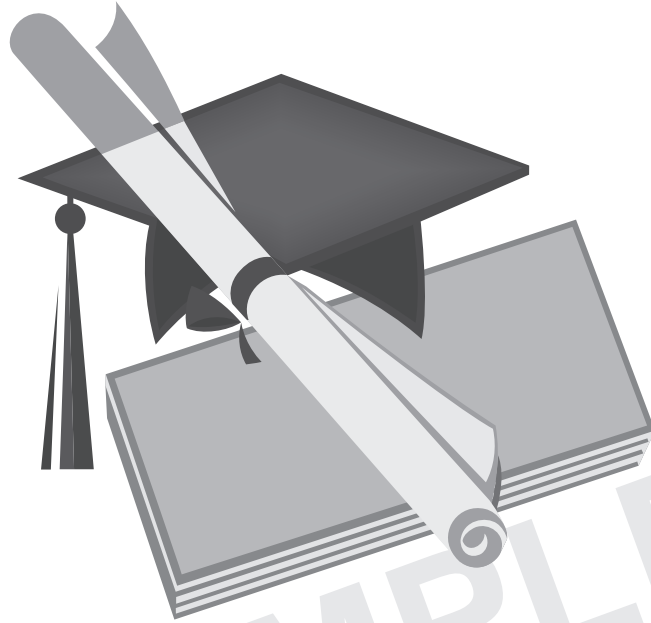


COBIT® CASE STUDY: TIBO



An extended case study in which students can apply their CoBIT knowledge to a real-life situation

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. The IT Governance Institute offers symposia, original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Information Systems Audit and Control Association®

With more than 35,000 members in more than 100 countries, the Information Systems Audit and Control Association (ISACA®) (www.isaca.org) is a recognised worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *Information Systems Control Journal*®, develops international information systems auditing and control standards, and administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 35,000 professionals since inception, and the Certified Information Security Manager® (CISM®) designation, a groundbreaking credential earned by 5,000 professionals in its first two years.

Disclaimer

The IT Governance Institute, Information Systems Audit and Control Association [the “Owner(s)”] and the authors have designed and created *COBIT in Academia* and its related publications, titled COBIT® *Case Study: TIBO*, COBIT® *Student Book*, COBIT® *Caselets* and COBIT® *Presentation Package*, (the “Work”), primarily as an educational resource for educators. The Owners make no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the educator should apply his/her own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Disclosure

Copyright © 2004 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 © 2004 IT Governance Institute. All rights reserved. Reprinted by permission.” *COBIT in Academia* 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 the IT Governance Institute. Any modification, distribution, performance, display, transmission, or storage, in any form by any means (electronic, mechanical, photocopying, recording or otherwise) of *COBIT in Academia* 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: research@isaca.org
Web sites: www.itgi.org and www.isaca.org

ISBN 1-893209-96-2

COBIT in Academia

Printed in the United States of America

ACKNOWLEDGEMENTS

IT GOVERNANCE INSTITUTE WISHES TO RECOGNISE:

The Board of Trustees

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, International President
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General's Office, Singapore, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Ricardo Bria, CISA, SAFE Consulting Group, Spain, Vice President
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Vice President
Howard Nicholson, CISA, CRN Solutions, Australia, Vice President
Bent Poulsen, CISA, CISM, VP Securities Services, Denmark, Vice President
Frank Yam, CISA, CIA, CCP, CFE, Focus Strategic Group Inc., Hong Kong, Vice President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Paul A. Williams, FCA, MBCS, Paul Williams Consulting, UK, Past International President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi, USA, Trustee
Ronald Saull, CSP, Great-West Life and IGM Financial, Canada, Trustee
Erik Guldentops, CISA, CISM, Belgium, Advisor, IT Governance Institute

The Development Team

Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium (Chair)
Roger Debreceny, Ph.D., University of Hawaii, USA
Steven De Haes, University of Antwerp Management School, Belgium (Project Manager)
Roger Lux, Farmers Insurance Group, USA
John Mitchell, CISA, CIA, CFE, LHS Business Control, UK
Ed O'Donnell, Ph.D., Arizona State University, USA
Scott Summers, Ph.D., Brigham Young University, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium

The Review Team

Peter Best, CA, FCPA, MACS, Q.U.T. Accountancy, Australia
Richard B. Dull, Ph.D., CISA, CPA, Clemson University, USA
Frederick Gallegos, CISA, CGFM, CDE, California State Polytechnic University at Pomona, USA

TABLE OF CONTENTS

Purpose of This Document	5
Case Study Description	7
One Day in the Life of the Outsourcing Story of TIBO®	7
The Trusted Imperial Banking Organisation’s Profile.....	9
The Company’s IT Environment	9
Projects.....	9
Technology	10
Standards and Procedures	10
Security	11
The Organisational Entities	11
Board of Directors.....	11
Executive Committee	11
Business Strategy Group.....	11
IT Coordination Committee.....	12
IT Management.....	12
IT Teams.....	12
Business Operational.....	12
Organisation Charts	13
Additional Material	14
The Security Issue	14
Questions	14
Service Level Agreement of the Outsourcing Contract.....	15
The Outsourcing Issue	16
Questions.....	16
The Strategic Alignment Issue.....	16
Extra Background Information	16
Questions.....	17
Teaching Notes	18
Additional Material to Support This Case.....	18
In General.....	18
For the Outsourcing Issue	18
For the Strategic Alignment Issue.....	18
Suggested Solutions.....	19
General Answers	19
Expected Answers on Security	19
Expected Answers on Outsourcing.....	20
Expected Answers on Strategic Alignment.....	21
Appendix	22

Bold titles are contained in this sample.

PURPOSE OF THIS DOCUMENT

COBIT *Case Study: TIBO* is a product developed by the IT Governance Institute, in collaboration with a group of international academics and practitioners, as part of *COBIT in Academia*. 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 real-life 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 post-graduate level classes. The case could also be used in undergraduate classes, if the students were 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 the COBIT *Student Book*, a book explaining and illustrating all the COBIT elements, which was also developed by the IT Governance Institute as part of *COBIT in Academia*. The materials in this case study draw directly on the IT process covered in chapter 2 (DS2) of the COBIT *Student Book* and from the additional handouts on other processes supplied in chapter 3 (PO1, PO9, PO10, AI2, DS5, DS6, M1 and M2).

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). We suggest 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*¹), 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 on page 18.

Figure 1—Suggested Map Through Case

<u>Session</u>	<u>Activity</u>	<u>Reading</u>
0	Introduction to COBIT	COBIT <i>Student Book</i>
1	Part One TIBO Case	Case Study Description + <i>Board Briefing on IT Governance, 2nd Edition</i> + Questions
2	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">Security</div> <div style="text-align: center;">Outsourcing</div> <div style="text-align: center;">Strategic alignment</div> </div>	Relevant Additional Material (see teaching notes)

¹ IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003

The IT Governance Institute has also developed three other products that can accompany this case study: *COBIT Student Book* (mentioned previously); the *COBIT Presentation Package*, providing a comprehensive 80-slide PowerPoint deck on COBIT; and *COBIT Caselets*, which includes minicases for smaller COBIT exercises, to be used at the graduate and undergraduate levels.

SAMPLE

CASE STUDY DESCRIPTION

ONE 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 had called him to the meeting a few minutes ago. Forsythe stated, "Mitchell has had the Financial Ombudsman Survey² 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 down 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. 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 had noticed that the reports were getting longer each month and had 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," Mitchell said.

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 9/11 and the hacking and virus incidents, but we have got to solve the We-BOP problem first."

² A consumer protection organisation—see appendix

“Oh by the way, Steven, before you go. Do you have an idea about who 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 CISO³ position but the conclusion of the executive committee was that we could do without. I am still having a debate with internal audit because they are 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.

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 of the outsourcing contract⁴ covered:

- The scope of the work
- Time line 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 checquing accounts. New 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. There was a small volume of users (5 percent of customer base). After six months, when the number of users grew, problems began with the quality of the service delivery, such as:

- 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.

³ Chief information security officer

⁴ See the summary of the service level agreement on p. 15.

Before calling Guldentops, the COO, in Manila to provide him an update on the We-BOP problem, De Haes was also reminded of poor Doano in security administrator who was actually overwhelmed with developing security procedures, getting acquainted with security tools, 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 reshuffling in his mind his agenda for the next day. He really had to have a word with Dean and his people about their lack of reaction to the firewall alarms and also to O'Donnell, who apparently knew the weakness existed. And, there was the dreaded meeting about project priorities with Van Grembergen and Lux. He is going to have to find a way to talk them out of their unreasonable expectations. Finally, Guldentops picked up.

“Hi, Erik, I know it is near midnight in Manila but we have got a BIG problem....”

Pages 9 through 13 deleted from this sample.

SAMPLE

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 some sensitive information (names, account managers, etc.).
 - a. Analyse the security risks.
 - b. 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) service level agreement (SLA). The data leaked because the third party used real, live customer data during acceptance tests of the second phase on an insecure web server installation.
 - a. Define what management should have put into the SLA relative to security.
 - b. What do you think actually happened to allow these data to get into the public domain?

Pages 15 through 22 deleted from this sample.

SAMPLE