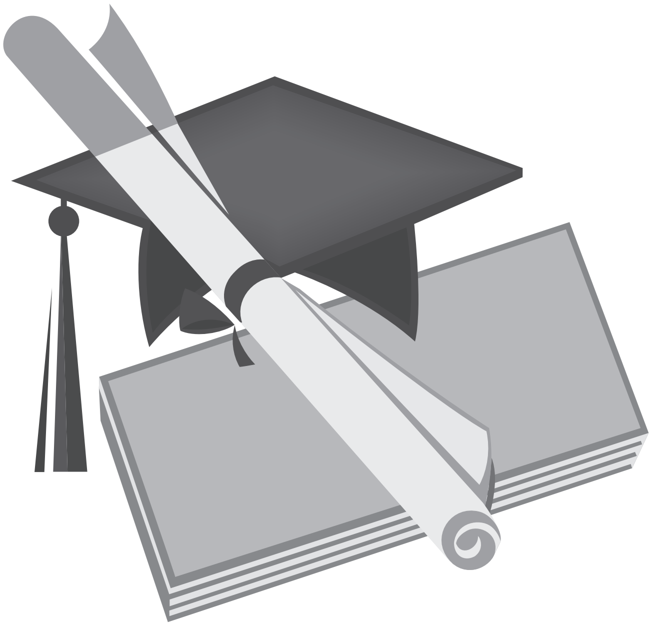
COBIT® CASE STUDY: TIBO



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

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

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

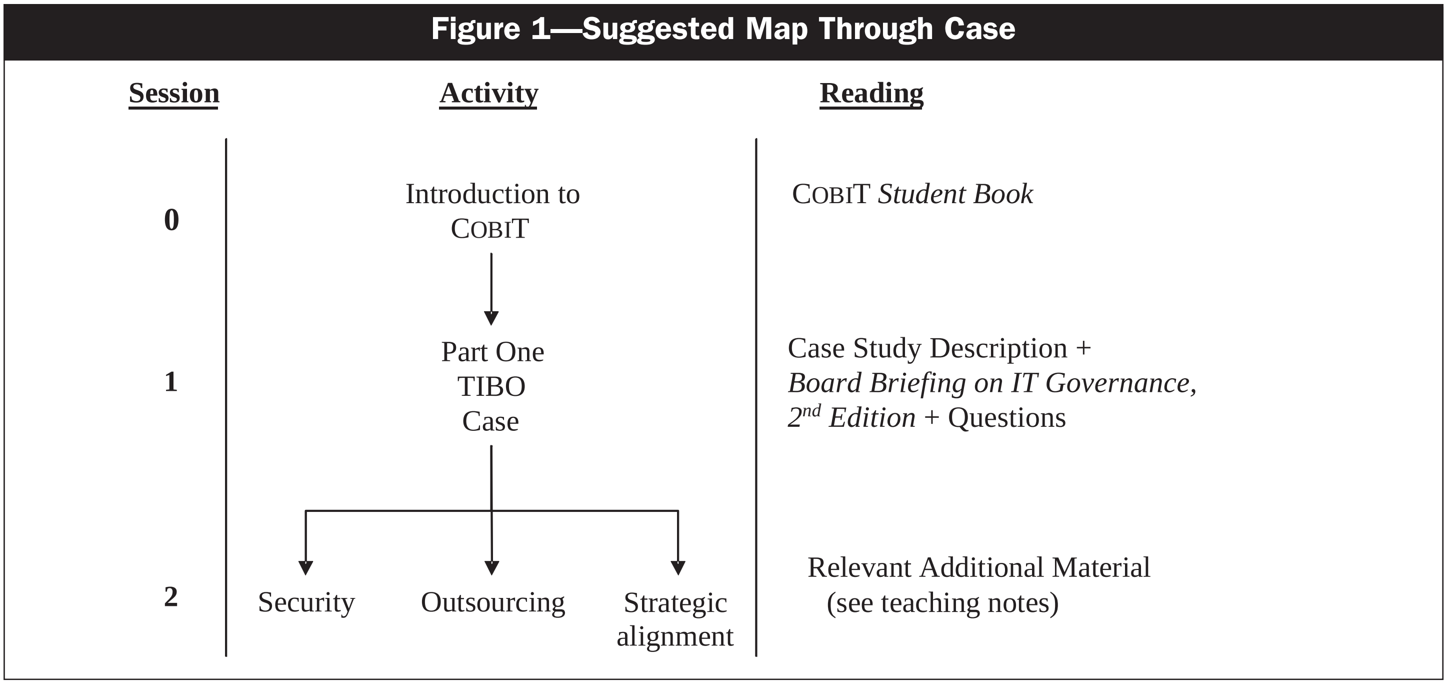
COBIT *Case Study: TIBO* is a product developed by the IT Governance Institute, in collaboration with a group of international academics and practitioners, as part of *COBIT in Academia*. The goal of this document is to provide an extended case study (including case description, student questions and 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



Session	Activity	Reading
0	Introduction to COBIT	COBIT *Student Book*
1	Part One TIBO Case	Case Study Description + *Board Briefing on IT Governance, 2nd Edition* + Questions
2	Security Outsourcing Strategic alignment	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.

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 Survey[2] 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 CISO[3] 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 contract[4] 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 administer who was actually overwhelmed with developing security procedures, getting acquainted with security tools, administrater 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…."

THE TRUSTED IMPERIAL BANKING ORGANISATION'S PROFILE

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

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

THE COMPANY'S IT ENVIRONMENT

PROJECTS

TIBO projects include:

- **We-BOP** (web-enabled banking operations)—Currently (partially live and outsourced), this includes customer access to savings and chequing applications; yet to be implemented are loan and credit card access, all with a single customer interface.
- **CRM** (customer relationship management)—This will pull all customer information together to enable cross-selling of products, to support both account managers and other customer support staff.
- **CoBAR** (core business applications rebuilding)—This includes primarily the savings, chequing and loan applications.

- **IT_Net**—Expanded IT network and standardised applications platforms
- **ForPay**—Foreign payment services
- **Work_it—**Workflow application and remote connectivity for account managers

TECHNOLOGY

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

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

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

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

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

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

STANDARDS AND PROCEDURES

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

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

System developments have been undertaken mostly in-house, based on the mainframe, with a system development life cycle (SDLC) methodology that was acquired some years ago and has been adjusted to suit the bank. In recent years these methods have been found to be outdated and too slow to undertake. However, they at least have ensured reasonable documentation of systems. There is little experience in acquiring packaged solutions. Only a few of the in-house team have any experience with client-server systems, and none have any web development experience.

Operations are well organised with good discipline and tight procedures. Generally, all work is treated as high priority. There are shifts covering operations 24 hours a day, with a small overnight team that handles mostly batch processing. Internal service level agreements (SLAs) are defined in technical terms and are really service level statements setting, for example, availability targets and capacity requirements for the network. There is a small internal help desk, which is mostly used for occasional user queries and password resets.

SECURITY

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

THE ORGANISATIONAL ENTITIES

BOARD OF DIRECTORS

The TIBO board of directors has the following attributes:

- The chairman of the board is not involved with the company on a daily basis.
- It is composed of both internal and external members, with the majority of audit committee members external.
- The members are technically literate, but they are risk-conscious and interested in what “others” do.

EXECUTIVE COMMITTEE

The TIBO c-suite and has the following attributes:

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

BUSINESS STRATEGY GROUP

The TIBO strategy group has the following attributes:

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

The current strategic initiatives are:

- Closing low-performing branches (almost complete)
- Creating a web-based banking system to unload the demand for services at branch offices (We-BOP) (in progress)
- Developing CRM capabilities to create opportunities to cross-sell banking services (project initiated)

IT COORDINATION COMMITTEE

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

IT MANAGEMENT

The IT director and his management team are:

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

IT TEAMS

The TIBO IT teams are:

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

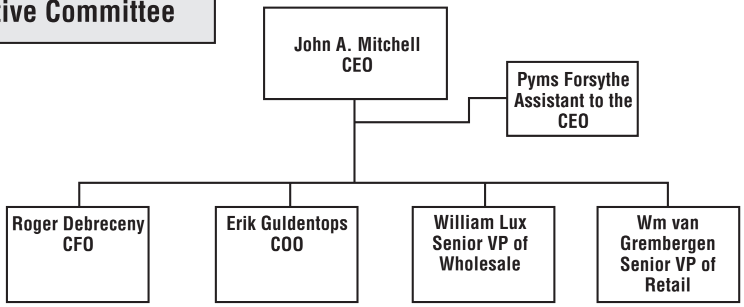
BUSINESS OPERATIONAL

TIBO executives are:

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

ORGANISATION CHARTS

Executive Committee



John A. Mitchell
CEO

Pyms Forsythe
Assistant to the CEO

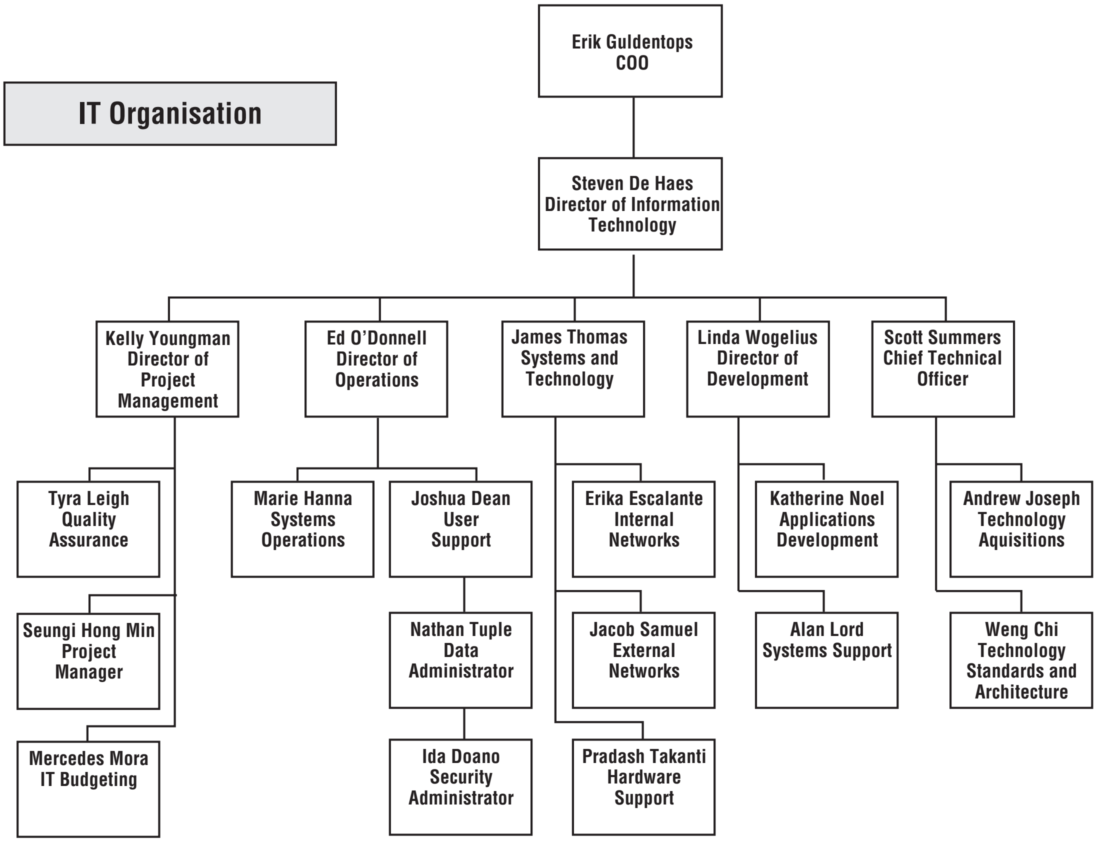
Roger Debreceny
CFO

Erik Guldentops
COO

William Lux
Senior VP of Wholesale

Wm van Grembergen
Senior VP of Retail

IT Organisation



Erik Guldentops
COO

Steven De Haes
Director of Information Technology

Kelly Youngman
Director of Project Management

- Tyra Leigh
Quality Assurance
- Seungi Hong Min
Project Manager
- Mercedes Mora
IT Budgeting

Ed O'Donnell
Director of Operations

- Marie Hanna
Systems Operations
- Joshua Dean
User Support
- Nathan Tuple
Data Administrator
- Ida Doano
Security Administrator

James Thomas
Systems and Technology

- Erika Escalante
Internal Networks
- Jacob Samuel
External Networks
- Pradash Takanti
Hardware Support

Linda Wogelius
Director of Development

- Katherine Noel
Applications Development
- Alan Lord
Systems Support

Scott Summers
Chief Technical Officer

- Andrew Joseph
Technology Aquisitions
- Weng Chi
Technology Standards and Architecture

IT Coordinating Committee

Ed O'Donnell
Director of Operations
(Chair)

Linda Wogelius
Director of Development

June Poor
Assistant Vice President of Wholesale Banking

Kelly Youngman
Director of Project Management

Max Rich
Assistant Vice President of Retail Banking

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?

SERVICE LEVEL AGREEMENT OF THE OUTSOURCING CONTRACT

Web-enabled Banking Operations Project (We-BOP)

Revision	Date	Description	Pages affected
1.0	February 200x	First edition	All

Purpose of This Document
This document constitutes an agreement between the outsourcer and the third party, defined in the next section, for the development of full e-banking services referred to as “We-BOP.” It details the environment, expectations, deliverables and responsibilities associated with the implementation of this agreement.

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

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

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

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

- Phase 1: To be operational 30 April 200x
  - – A web-based front office enabling:
    - ▪ Access to savings account
    - ▪ Access to chequing account
  - – The interface between the front office and the back office of the outsourcer
  - – A fully operational help desk function for customer support
- Phase 2: To be operational 31 March 200x+1
  - – Extended functionalities of the web-based front office:
    - ▪ Credit cards
    - ▪ Loans

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

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

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

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

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

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

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

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

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

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

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

Signatures

CEO of the Outsourcer Date

CEO of the Third Party Date

THE OUTSOURCING ISSUE

QUESTIONS

1. You are confronted here with a detailed outsourcing process. Give an evaluation of this process. Describe the problems TIBO encountered or the risks they face, and identify best practices that, if implemented, would have prevented or alleviated the problems or risks.
2. Identify the roles that audit, IT management and the CEO should play in outsourcing. Compare these best practices to the roles actually played in TIBO.

THE STRATEGIC ALIGNMENT ISSUE

EXTRA BACKGROUND INFORMATION

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

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

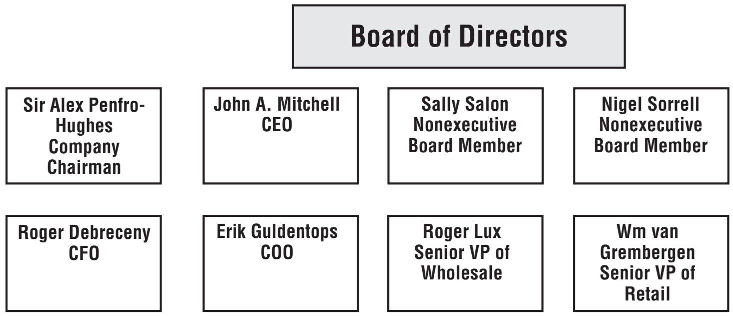
- Channel strategies
- Current trends
- Customer relations and retention

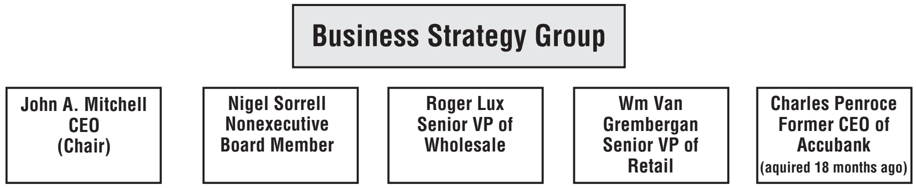
The business strategy group has excellent documentation procedures. It maintains a strategic initiatives document that details each of the initiatives and charts progress on each. This document is distributed to the board of directors and the executive committee.

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

The board of directors meets quarterly. Strategic initiatives are always among the many items discussed by the board.

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


Board of Directors
Sir Alex Penfro-Hughes Company Chairman
John A. Mitchell CEO
Sally Salon Nonexecutive Board Member
Nigel Sorrell Nonexecutive Board Member
Roger Debreceny CFO
Erik Guldentops COO
Roger Lux Senior VP of Wholesale
Wm van Grembergen Senior VP of Retail


Business Strategy Group
John A. Mitchell CEO (Chair)
Nigel Sorrell Nonexecutive Board Member
Roger Lux Senior VP of Wholesale
Wm Van Grembergan Senior VP of Retail
Charles Penroce Former CEO of Accubank (aquired 18 months ago)

QUESTIONS

1. Analyse the governance implications of how TIBO handled outsourcing from the board of directors, executive and IT management levels. What would be the best practices to govern outsourcing contracts?
2. Why was the CEO not aware of the customer complaints before the report from the Ombudsman? How can this be avoided in the future? What governance changes do you propose to solve this problem?
3. As the board begins the CRM initiative, how could better alignment be achieved between IT and business strategy than was evident in the We-BOP initiative?

TEACHING NOTES

ADDITIONAL MATERIAL TO SUPPORT THIS CASE

IN GENERAL

- COBIT *Student Book* chapter 3 (process DS5 and PO9)
- International Organisation for Standardisation (ISO) 17799
- Introductory material on ITIL (IT Infrastructure Library, Office of Government Commerce, UK)

FOR THE OUTSOURCING ISSUE

- COBIT *Student Book* (process DS2)
- Outsourcing web sites
  - *www.outsourcing.com*
  - Cutter Consortium's Sourcing and Vendor Relationships E-mail Advisor—weekly e-mails:
    - Go to *cutter.com*.
    - Under "Data, Analysis, and Advice," click on "Sourcing and Vendor Relationships."
    - Sign up for trial subscription to weekly e-mail service.
    - There are also free reports available on the web site.
  - Computerworld Outsourcing—weekly e-mails (free):
    - Go to *www.cwrld.com/nl/sub.asp*. Select "Outsourcing", and register.
    - Also, for their Outsourcing Knowledge Center, go to *www.computerworld.com/managementtopics/outsourcing*.
  - Network World
    - Go to *www.nwfusion.com*, enter the search word "outsourcing."
  - Tech Republic
    - Go to *www.techrepublic.com*, enter the search word "outsourcing."
  - IDG—Content of eight magazines, including *InfoWorld, PC World, CIO Magazine*, etc.
    - Go to *www.idg.net*, enter the search word "outsourcing."
- Typical IT outsourcing publications supplied by the teacher
- Optionally, provide students typical articles on outsourcing and COBIT references.
- Consider how change management is being handled (how it was organised, after the number of operational changes due to the complaints and errors).
- Provide students with a short description of the SLA, as used originally by the company.
- Use the outsourcing audit programme provided by ISACA to point students in the right direction, *www.isaca.org*.

FOR THE STRATEGIC ALIGNMENT ISSUE

Students have been given the company's approach to strategy provided on page 16. Students also have the PO1 material from the COBIT *Student Book* and the *Board Briefing on IT Governance, 2nd Edition* (*www.itgi.org*) as reference material.

SUGGESTED SOLUTIONS

GENERAL ANSWERS

Some general issues that need to be emphasised in the answers provided by the students:

- The strategy is not clear to all parties, and there is a difference of opinion on priorities.
- There are major issues with change management as a result of the many changes.
- The enterprise is barely at maturity level 2 for information security.
- There is no co-ordination and a lack of communication.

Be aware that maturity level 2 is built into the case (reference to process DS5's maturity model). Its characteristics are:

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

EXPECTED ANSWERS ON SECURITY

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. The security risks are:
      - There appears to be a lack of management (board, audit committee) concern with security.
      - Security is underresourced.
      - There is no IT security plan.
      - Policies are based in the mainframe era and should be strengthened for new technologies, such as laptops and virtual disk drives.
      - Responsibilities and accountabilities for IT security are assigned to an IT security administrator with no management authority, reporting to the database supervisor.

   b. Recommend some good practices to better mitigate the risks. Some good risk-mitigation practices are:
      - Implementing ISO17799
      - Using COBIT process DS5

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. Management should require that the:
      - SLA stipulate that security should be to the level of ISO17799
      - Third party be certified and audited to that standard

   b. What do you think actually happened to allow these data to get into the public domain? The following could allow the data into the public domain:
      - Outsourcing staff could steal the data.
      - A server could have been decommissioned and sold without clearing the drive.

- The data could have been “googled” (found while using the Google search engine) by someone searching for a neighbour’s name.
- Ex-employee accounts could have been improperly deactivated.

EXPECTED ANSWERS ON OUTSOURCING

1. You are confronted here with a detailed outsourcing process. Give an evaluation of this process. Describe the problems TIBO encountered or the risks they face, and identify best practices that, if implemented, would have prevented or alleviated the problems or risks. Point out the risks of the:
   - Inadequate governance of the selection process
   - CEO’s lack of awareness or positioning to make this technology decision
   - Lack of testing
   - Elements not defined, or weakly defined, in the SLA
   - Lack of security metrics
   - Absence of business orientation of other metrics
   - Inadequate customer complaint handling
   - Inadequate reporting (which reports, who is responsible)
   - Items not covered in the SLA of the outsourcing contract. Ideally, these should be identified by the students:
     - Performance metrics
     - Response time
     - Availability of the system. It appears that customers can access the system only during specific times of the day.
     - Security
     - Testing (because of lack of testing some things are not processed or are processed incorrectly)
     - Training (the third party developed an error file for managing errors, but the internal IT staff were not trained to manage this)
     - Extra charges for the help desk in case the workload increases
     - Requirements not fully thought out
     - Change management (how was this organised after the number of operational changes due to the complaints and errors?)
2. Identify the roles that audit, IT management and the CEO should play in outsourcing. Compare these best practices to the roles actually played in TIBO. The comparisons are:
   - Audit should have been involved in the development. There was new technology, high risk and a new outsourcing process for which there was no in-house expertise. There was a high customer-facing component with potentially large public exposure.
   - Business management should have been more involved in determining the solution. They left the solution entirely to IT and therefore were not aware of the possible business risks related to outsourcing.
   - IT management should have been more proactive in managing the outsourced contract and should not have left things solely to the third party.

EXPECTED ANSWERS ON STRATEGIC ALIGNMENT

1. Analyse the governance implications of how TIBO handled outsourcing from the board of directors, executive and IT management levels. What would be the best practices to govern outsourcing contracts? Major themes that should come out in the discussions:
   - Communication (e.g., help desk report: nothing was done due to incorrect assumptions about responsibilities)
   - IT steering and IT strategy committees
   - Organisation and positions within the organisation
   - Greater involvement of the business
   - Clarity about the value (primarily intangible) to be returned by IT investment
2. Why was the CEO not aware of the customer complaints before the report from the Ombudsman? How can this be avoided in the future? What governance changes do you propose to solve this problem? It was dealt with as a technological operational solution rather than on a business risk basis. Thus:
   - Outsourcing was not seen as a strategic opportunity by the board or executive management.
   - IT viewed it as a tactical solution to its own resource problems.
   - The lack of an IT strategy committee meant that outsourcing was not considered in a strategic business context and, as a result, the new business risks were not evaluated.
   - Selection of the third party should be a formal process in which all appropriate parties, such as IT and procurement, should be involved.
   - Someone with responsibility needs to manage the outsourced contract on a day-to-day basis.
   - The customer complaints were directed to a very low level (Joshua Dean) and he thought it was just an information report. His boss thought that all the complaints had already been dealt with by the third party because of the increased invoices for support that he had received. The erroneous transaction problem was not identified as being significant by the outsourced support desk due to poor training.
   - The SLA should have a section dealing with problem management with an escalation procedure for serious incidents. The customer complaints should go to the contract manager and not directly to IT user support.
3. As the board begins the CRM initiative, how could better alignment be achieved between IT and business strategy than was evident in the We-BOP initiative? There is a need for an IT strategy committee or an increased IT membership of the business strategy group to provide business/IT alignment.
   - An IT steering committee is needed instead of the co-ordination committee.
   - The *Board Briefing on IT Governance, 2nd Edition*, guidelines should be followed.

Appendix

The Financial Ombudsman Service is a powerful UK regulatory service.

The Financial Ombudsman Service, located in the UK, may be able to help with a financial complaint you cannot sort out with a:

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

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

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

It can impose fines, but the real impact of such incidents is the embarrassment resulting from the reports being made public.