IT Governance Using COBIT® and Val IT™: Caselets, 3rd Edition

Minicase Studies on the Practical Use of COBIT

ISACA®
Trust in, and value from, information systems
ISACA®
With more than 86,000 constituents in more than 160 countries, ISACA (www.isaca.org) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the ISACA® Journal, and develops international IS auditing and control standards. It also administers the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA offers the Business Model for Information Security™ (BMIS™) and the IT Assurance Framework™ (ITAF™). It also developed and maintains the COBIT®, Val IT™ and Risk IT frameworks, which help IT professionals and enterprise leaders fulfil their IT governance responsibilities and deliver value to the business.

Disclaimer
ISACA has designed and created IT Governance Using COBIT® and Val IT™: Caselets, 3rd Edition (the ‘Work’) primarily as an educational resource for those seeking to understand COBIT and Val IT. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all 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, enterprise leaders and governance of IT, management and assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment. The example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious. No association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

Reservation of Rights
© 2010 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and non-commercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: info@isaca.org
Web site: www.isaca.org

IT Governance Using COBIT® and Val IT™: Caselets, 3rd Edition

CRISC is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.
ACKNOWLEDGEMENTS

ISACA wishes to recognise:

Researcher
Norm Kelson, CISA, CGEIT, CPA, The Kelson Group, USA

Expert Reviewers
Carmen R. Cintron-Ferrer, Universidad Sagrado Corazon, Puerto Rico
Olayinka David-West, CISA, CGEIT, Lagos Business School, Nigeria
Andrea Ko, Ph.D., Corvinus University of Budapest, Hungary
Munir Majdalawieh, Ph.D., American University of Sharjah, UAE
Chris O. Odionu, Ph.D., CGEIT, Alabama A&M University, USA
Juan Pardo, Ph.D., University CEU Cardenal Herrera, Spain
Joerg Puchan, Ph.D., University of Applied Sciences Munich, Germany
Mario Spremic, Ph.D., CGEIT, University of Zagreb, Croatia
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Diane L. Wright, University of Delaware, USA
Dmitry Zhdanov, Ph.D., CISSP, University of Connecticut, USA

ISACA Board of Directors
Emil D’Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, INTRALOT S.A., Greece, Vice President
Ria Lucas, CISA, CGEIT, Telstra Corp. Ltd., Australia, Vice President
Hitoshi Ota, CISA, CISM, CGEIT, CIA, Mizuho Corporate Bank Ltd., Japan, Vice President
Jose Angel Pena Ibarra, CGEIT, Alintec S.A., Mexico, Vice President
Robert E. Stroud, CGEIT, CA Technologies, USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Rolf M. von Roessing, CISA, CISM, CGEIT, KPMG Germany, Germany, Vice President
Lynn C. Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Director
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Director
Howard Nicholson, CISA, CGEIT, CRISC, City of Salisbury, Australia, Director
Jeff Spivey, CPP, PSP, Security Risk Management, USA, ITGI Trustee

Knowledge Board
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Chair
Michael Berardi Jr., CISA, CGEIT, Nestle USA, USA
John Ho Chi, CISA, CISM, CBCP, CFE, Ernst & Young LLP, Singapore
Jose Angel Pena Ibarra, CGEIT, Alintec S.A., Mexico
Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, RSM Bird Cameron, Australia
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada
Patrick Stachtchenko, CISA, CGEIT, CA, Stachtchenko & Associates SAS, France
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA

Academic Program Subcommittee
Henny J. Claessens, CISA, CISM, CGEIT, Maastricht University, The Netherlands, Chair
Claudio Cilli, Ph.D., CISA, CISM, CGEIT, University of Rome, Italy
Graham Gal, Ph.D., University of Massachusetts, USA
Yonosuke Harada, CISA, CISM, CGEIT, CAIS, Institute of Information Security, Japan
Sharon Finney, CISM, Adventist Health System, USA
Richard M. Moore III, CISM, CISSP, MSIA, KPMG LLP, USA
Vincent Orrico, Ph.D., CISA, CGEIT, CBCP, CISSP, PMP, Optimal Vantage Strategies LLC, USA
Krishna Seebum, CFE, CISSP, PMP, University of Technology, Mauritius, Mauritius
Lolita E. Vargas-DeLeon, CISA, CIA, CPA, Puerto Rico
Acknowledgements (cont.)

ISACA and IT Governance Institute Affiliates and Sponsors
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d’Information
Institute of Management Accountants Inc.
ISACA chapters
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
University of Antwerp Management School
Analytix Holdings Pty. Ltd.
BWise B.V.
Hewlett-Packard
IBM
Project Rx Inc.
SOAPProjects Inc.
Symantec Corp.
TruArx Inc.
# Table of Contents

Purpose of This Document .................................................................................................................................... 6

1. Caselet: DentDel Inc. ...................................................................................................................................... 7  
   Learning Objective ........................................................................................................................................ 7  
   Background ................................................................................................................................................ 7  
   Issue ........................................................................................................................................................ 7  
   Questions ............................................................................................................................................... 8

2. Caselet: Your Neighborhood Grocers ............................................................................................................ 9  
   Learning Objective ........................................................................................................................................ 9  
   Background .............................................................................................................................................. 9  
   Issue ........................................................................................................................................................ 9  
   Questions ............................................................................................................................................. 10

3. Caselet: All World Airways ......................................................................................................................... 11  
   Learning Objective ..................................................................................................................................... 11  
   Background ........................................................................................................................................... 11  
   Issue ...................................................................................................................................................... 11  
   Questions ............................................................................................................................................... 12  
   Exhibit .................................................................................................................................................. 12

4. Caselet: ClaimProof Insurance ..................................................................................................................... 14  
   Learning Objective .................................................................................................................................... 14  
   Background .............................................................................................................................................. 14  
   Issue ...................................................................................................................................................... 14  
   Questions ............................................................................................................................................... 15

5. Caselet: Software Programs Inc. .................................................................................................................. 16  
   Learning Objective ..................................................................................................................................... 16  
   Background .............................................................................................................................................. 16  
   Issue ...................................................................................................................................................... 16  
   Questions ............................................................................................................................................... 17

ISACA Professional Guidance Publications ......................................................................................................... 18
Purpose of This Document

Caselets, 3rd Edition is a product of ISACA (www.isaca.org) and is part of the IT Governance Using COBIT® and Val IT™ series. This publication supplements and complements the existing Caselets, 2nd Edition and should be used with the Student Book, 2nd Edition.

This publication was developed in collaboration with a group of international academic professionals and practitioners. These caselets provide five additional minicase studies on governance and assurance using COBIT in real-life situations and are designed to be used by graduate and undergraduate classes either in class as a 90-minute student group exercise or as weekly student assignments.

The caselets are based on themes from the Student Book, 2nd Edition. The objectives 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
• Help students learn how to apply COBIT to the governance of IT

Each caselet includes a learning objective, background on the organisation including IT processes and infrastructure, and specific problem areas that students are required to solve using the information in the Student Book, 2nd Edition or, as appropriate, the supplementary information outlined for each caselet.

Note that extra background information, guidance and teaching notes are outlined in a separate publication that is available for professors only.

The components that make up IT Governance Using COBIT and Val IT are the:

• Student Book, 2nd Edition
• Caselets, 2nd Edition and Teaching Notes
• TIBO Case Study, 2nd Edition and Teaching Notes (Spanish translation also available)
• Presentation, 2nd Edition (35-slide PowerPoint presentation on COBIT)
• Caselets, 3rd Edition and Teaching Notes
• City Medical Partners Case Study, 3rd Edition and Teaching Notes

Pages 7 and 13 have been deleted from this sample.
4. CASELET: CLAIMPROOF INSURANCE

LEARNING OBJECTIVE
This case focuses on the IT audit assurance process.

Introduction
The external auditors from Unqualified Opinions Ltd. have determined that the claim process is a high-risk area requiring audit focus. Their interim work has identified programme change control as a potential audit problem that may preclude placing reliance on the controls within the claim process system.

BACKGROUND

Company
ClaimProof Insurance is an international property and casualty insurance company. Its motto is: One Claim Is Enough! It operates in the Americas, European Union countries and the commonwealth countries of Asia.

Industry
The property and casualty insurance industry is competitive. Companies review their claims history frequently and, upon renewal date, determine whether it is in the company’s interests to retain the insured. Some companies will retain the insured, adjusting the premiums based on the claim history. ClaimProof is one of the low-premium leaders that is unwilling to retain customers if there is any claim history.

Key Player
The key player is Unqualified Opinions Ltd., an external accounting firm.

ISSUE
The claim process uses an automated adjudication system that evaluates the claim details, frequency of customer claim history, probabilities and other complex factors in approving claim payments, suspending the payments with referral to a specialist or denial of claims. This process is material in the evaluation of the financial statements. Unqualified Opinions Ltd. has determined that the most efficient audit methodology is to use a previous detailed audit of the process as a benchmark and focus on only the changes to the system. Since the basis for identifying changes to the system is the programme change control process, the internal audit department has been asked to perform an audit of the controls affecting the programme change control system (PCCS).

The PCCS controls the production source and executable program code, operating system configuration parameters, and any batch control processes (.BAT, .CMD and .JCL). The test libraries that contain source and executable code are open to all programmers throughout the installation. Once a programmer has completed the testing of a program, the program source is submitted to the programme change administrator. The administrator recompiles the program and moves the source and executable code into a production library that is accessible only to the production control team.

In a cost-cutting initiative, the production control team is only available during regular business hours. After hours, if a program change is required, one-time-use passwords are available. The programmer who makes the change must create a change ticket, obtain the one-time password from a file cabinet, and indicate in the password log the change ticket number and the date and time of the change. The programmer can then make the appropriate changes, move the program into production, and note on the move ticket the time and date of the completion of the move. Each morning, the programme change administrator reviews the sign-out log and verifies that the appropriate paperwork has been completed.

During an initial interview, the administrator was asked whether further examination of off-hours changes was performed; the response was no. An incident reporting system records all processing disruptions, but there is no reconciliation between the system and the PCCS.
**Decision to Be Made**
The external auditors have expressed concern regarding the synchronisation of the production source and executable code and whether any unauthorised changes to production logic have occurred.

**QUESTIONS**

You have been hired to respond to these concerns and answer the following questions:
1. What are the five steps required for the IT assurance of a specific area?
2. Based on the results of question 1 and your understanding of the control environment, identify the high-risk areas requiring audit attention.
3. How would you assess the control design?
4. How would you test the control effectiveness?

Pages 16 and 17 have been deleted from this sample.
ISACA Professional Guidance Publications

Many ISACA publications contain detailed assessment questionnaires and work programs. Please visit www.isaca.org/bookstore or e-mail bookstore@isaca.org for more information.

Frameworks and Models

- The Business Model for Information Security, 2010
- COBIT® 4.1, 2007
- Enterprise Value: Governance of IT Investments, The Val IT™ Framework 2.0, 2008
- The Risk IT Framework, 2009

BMIS-related Publication

- An Introduction to the Business Model for Information Security, 2009

COBIT-related Publications

- Aligning COBIT® 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit, 2008
- Building the Business Case for COBIT® and Val IT™: Executive Briefing, 2009
- COBIT® and Application Controls, 2009
- COBIT® Mapping: Mapping of CMMP® for Development V1.2 With COBIT® 4.0, 2007
- COBIT® Mapping: Mapping of FFIEC With COBIT® 4.1, 2007
- COBIT® Mapping: Mapping of ITIL With COBIT® 4.0, 2007
- COBIT® Mapping: Mapping of PMBOK® With COBIT® 4.0, 2006
- COBIT® Mapping: Mapping of SEI’s CMMP® for Software With COBIT® 4.0, 2006
- COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0, 2007
- Implementing and Continually Improving IT Governance, 2009
- SharePoint® Deployment and Governance Using COBIT® 4.1: A Practical Approach, 2010

Risk IT-related Publication

- The Risk IT Practitioner Guide, 2009

Val IT-related Publications

- The Business Case: Using Val IT™ 2.0, 2010
- Enterprise Value: Getting Started With Value Management, 2008
- Value Management Guidance for Assurance Professionals: Using Val IT™ 2.0, 2010

Academic Guidance

- IT Governance Using COBIT and Val IT material:
  – Student Book, 2nd Edition
  – Caselets, 2nd Edition and Teaching Notes
  – TIBO Case Study, 2nd Edition and Teaching Notes (Spanish translation also available)
  – Presentation, 2nd Edition (35-slide PowerPoint presentation on COBIT)
  – Caselets, 3rd Edition and Teaching Notes
  – City Medical Partners Case Study, 3rd Edition and Teaching Notes
EXECUTIVE AND MANAGEMENT GUIDANCE

- An Executive View of IT Governance, 2008
- Information Security Governance—Top Actions for Security Managers, 2005
- IT Governance Domain Practices and Competencies:
  - Governance of Outsourcing, 2005
  - Information Risks: Whose Business Are They?, 2005
  - IT Alignment: Who Is in Charge?, 2005
  - Measuring and Demonstrating the Value of IT, 2005
  - Optimising Value Creation From IT Investments, 2005
- IT Governance and Process Maturity, 2008
- IT Governance Roundtables:
  - Defining IT Governance, 2008
  - IT Staffing Challenges, 2008
  - Unlocking Value, 2009
  - Value Delivery, 2008
- Managing Information Integrity: Security, Control and Audit Issues, 2004
- Understanding How Business Goals Drive IT Goals, 2008
- Unlocking Value: An Executive Primer on the Critical Role of IT Governance, 2008

PRACTITIONER GUIDANCE

- Audit/Assurance Programs:
  - Change Management Audit/Assurance Program, 2009
  - Generic Application Audit/Assurance Program, 2009
  - Identity Management Audit/Assurance Program, 2009
  - IT Continuity Planning Audit/Assurance Program, 2009
  - Network Perimeter Security Audit/Assurance Program, 2009
  - Outsourced IT Environments Audit/Assurance Program, 2009
  - Security Incident Management Audit/Assurance Program, 2009
  - Systems Development and Project Management Audit/Assurance Program, 2009
  - UNIX/LINUX Operating System Security Audit/Assurance Program, 2009
  - z/OS Security Audit/Assurance Program, 2009
- Cybercrime: Incident Response and Digital Forensics, 2005
- Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment, 2004
- Information Security Career Progression Survey Results, 2008
- Information Security Harmonisation—Classification of Global Guidance, 2005
- IT Control Objectives for Basel II, 2007
- OS/390—z/OS: Security, Control and Audit Features, 2003
- Peer-to-peer Networking Security and Control, 2003
- Security Awareness: Best Practices to Serve Your Enterprise, 2005
- Security Critical Issues, 2005
- Stepping Through the InfoSec Program, 2007
- Stepping Through the IS Audit, 2nd Edition, 2004
- Technical and Risk Management Reference Series:
- Top Business/Technology Survey Results, 2008
- White Papers:
  - New Service Auditor Standard: A User Entity Perspective, 2010
  - Securing Mobile Devices, 2010
  - Social Media: Business Benefits and Security, Governance and Assurance Perspectives, 2010