IT Governance Using COBIT® and Val IT™: City Medical Partners Case Study, 3rd Edition

A Case Study on the Practical Use of COBIT
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™: City Medical Partners Case Study, 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™: City Medical Partners Case Study, 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 Zhidanov, 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, FIA, 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, CISA, AFCHSE, CHE, FACS, FCPA, FIA, 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 Stachtenken, CISA, CGEIT, CA, Stachtenken & 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.
SOAProjects Inc.
Symantec Corp.
TruArx Inc.
# TABLE OF CONTENTS

City Medical Partners Case Study ................................................................. 6
  Learning Objectives .................................................................................. 6
  Introduction .............................................................................................. 6
  Background .............................................................................................. 6
  Issue ......................................................................................................... 6

Appendix A. City Medical Partners—Organisation Chart ........................................ 8

Appendix B. Interview With Jim Foley, CIO, City Medical Partners ......................... 9

Appendix C. Interview With David Stow, CEO, City Medical Partners ................... 10

Appendix D. Interview With Bill Sayre, IT Director, City Medical Centre ................ 12

Appendix E. Interview With Barbara Winton, IT Director, City Medical Cancer Centre 14

Appendix F. Interview With Andy Lottle, IT Director, City Medical Kids Centre ........ 15

Appendix G. Interview With Dr. Antonio Pillotti, IT Director, City Medical School ...... 17

Appendix H. Interview With Dr. Mikhail Brodlovsky, IT Director, City Medical Research 18

Appendix I. Interview With Lisa Alott, IT Services Director/IT Controller, City Medical Partners 19

Appendix J. Interview With Frank Lee, Information Security Director, City Medical Partners 20

Appendix K. Interview With Sarah Singleton, Strategic Planning Director, City Medical Partners 21

Appendix L. COBIT Assurance Guidelines Related to the City Medical Partners Case Study 22

ISACA Professional Guidance Publications .................................................................. 28
LEARNING OBJECTIVES

The learning objectives of this case include the following:
• Identify and understand the COBIT principles relating to the governance of IT, risk assessment and IT value.
• Understand how organisational dynamics affect the achievement of best-practice governance, risk and value objectives.
• Identify root-cause issues, analyse alternatives and recommend viable solutions.

INTRODUCTION

City Medical Partners serves the community with two major teaching hospitals, a cancer treatment centre, a highly rated medical school and one of the foremost medical research institutions.

The organisation has experienced exponential growth in all of its areas. The chief executive officer (CEO) recently replaced the former chief information officer (CIO) with a new CIO to manage this growth.

Key business needs include:
• Recent health insurance legislation requiring the use of automated medical records
• Increased patient volumes
• New health programmes
• Lower government reimbursements leading to the need to look for more donations from foundations/benefactors

BACKGROUND

Company
City Medical Partners is a non-profit health organisation and parent to five operating units:
• City Medical Centre—A teaching hospital with an advanced life support and trauma centre
• City Medical Cancer Centre—A dedicated cancer treatment and research unit
• City Medical Kids Centre—A dedicated children’s teaching hospital
• City Medical School—A medical school to support the clinical teaching process
• City Medical Research—A dedicated facility for advanced medical research

Industry
The medical provider and education industry has been undergoing major change. Recent US health insurance legislation requires the use of automated medical records throughout hospitals. Increased patient volumes are expected by medical institutions as the uninsured become insured through new programmes. At the same time, there is hope that there will be some relief from the uninsured utilising emergency rooms for primary patient care.

The hospitals and medical school operate at a loss each year due to government medical programme reimbursements below cost of service, requiring the institutions to supplement their operational income with donations from foundations/benefactors.

Research is financed through government research grants, private industry contributions and donations from private foundations/benefactors.

Key Players
The key player is Jim Foley, CIO. Refer to appendix A for the organisation chart.

ISSUE

Jim Foley is the newly appointed CIO. Because there are numerous organisations with varying business focuses, Jim needs to understand the organisation and governance functions. In his prior position, he had adopted COBIT and had developed a strong working relationship with the previous organisation’s IT audit function. He believes that the most effective way to approach the management of this diverse organisation is to utilise COBIT and its best practices.
**Decision to Be Made**

In an interview with Jim, he has requested that you:

- Perform a risk assessment.
- Recommend how to implement a function that allows for the effective governance of IT.
- Recommend how he can reorganise the IT function.

To fully understand Jim’s needs, the transcript of his interview follows as appendix B.

Each of the principals identified in appendix A was interviewed. Their transcripts are provided in the subsequent appendices. The interviewer is a fellow auditor.

Your assignment is to respond to the three requests from Jim. Your instructor will define the presentation requirements.
APPENDIX A. CITY MEDICAL PARTNERS—ORGANISATION CHART

Figure 1—City Medical Partners Organisation Chart

David Stow  
CEO  
City Medical Partners

Jim Foley  
CIO  
City Medical Partners

Bill Sayre  
IT Director  
City Medical Centre

Barbara Winton  
IT Director  
City Medical Cancer Centre

Andy Lottle  
IT Director  
City Medical Kids Centre

Dr. Antonio Pillotti  
IT Director  
City Medical School

Dr. Mikhail Brodlovsky  
IT Director  
City Medical Research

Lisa Alott  
IT Services Director/IT Controller  
City Medical Partners

Frank Lee  
Information Security Director  
City Medical Partners

Sarah Singleton  
Strategic Planning Director  
City Medical Partners

Pages 9 through 27 have been deleted from this sample.
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 CMMF for Development V1.2 With COBIT® 4.0, 2007
• COBIT® Mapping: Mapping of FFIEC With COBIT® 4.1, 2007
• COBIT® Mapping: Mapping of ITIL V3 With COBIT® 4.1, 2008
• COBIT® Mapping: Mapping of ITIL With COBIT® 4.0, 2007
• COBIT® Mapping: Mapping of NIST SP800-53 With COBIT® 4.1, 2007
• COBIT® Mapping: Mapping of PMBOK® With COBIT® 4.0, 2006
• COBIT® Mapping: Mapping of SEI’s CMM® for Software With COBIT® 4.0, 2006
• COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0, 2007
• COBIT® Quickstart™, 2nd Edition, 2007
• COBIT® User Guide for Service Managers, 2009
• Implementing and Continually Improving IT Governance, 2009
• IT Assurance Guide: Using COBIT®, 2007
• 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