Tampa Bay Office Furniture Inc.:
A Case Study

SAMPLE
ISACA®
With 95,000 constituents in 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 and management of IT, and IT-related risk and compliance. Founded in 1969, the non-profit, independent ISACA hosts international conferences, publishes the ISACA® Journal, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through 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 continually updates COBIT®, which helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer
ISACA has designed and created Tampa Bay Office Furniture Inc.: A Case Study (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 IT governance, management and assurance professionals should apply their own professional judgement to the specific control 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
© 2011 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

Tampa Bay Office Furniture Inc.: A Case Study
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:

Author
Uday Murthy, Ph.D., ACA, ISACA Academic Advocate, University of South Florida, School of Accountancy, 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, CFA, 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, Forfa AG, Germany, Vice President
Lynn C. Lawton, CISA, FBSCS 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, ACHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Director
Howard Nicholson, CISA, CGEIT, CRISC, City of Salisbury, Australia, Director
Jeff Spivey, CRISC, 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, Netherlands, Chair
Claudio Cilli, CISA, CISM, CGEIT, CRISC, CIA, CISSP, CSSLP, 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, CISSP, Adventist Health System, USA
M. Richard Moore III, CISM, CISSP, GPEN, MSIA, Nthnet, USA
Vincent Orrico, Ph.D., CISA, CGEIT, CBCLA, CBP, CISSP, Optimal Vantage Strategies LLC, USA
Krishna Seeburn, CIA, CISSP, CFE, PMP, University of Technology, Mauritius
Lolita E. Vargas-DeLeon, CISA, CIA, CPA, Puerto Rico
ISACA and IT Governance Institute® (ITGI®) 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
Institute of Management Accountants Inc.
ISACA chapters
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School
ASI System Integration
Hewlett-Packard
IBM
SOAPrjects Inc.
Symantec Corp.
TruArx Inc.
Tampa Bay Office Furniture Inc.

Tampa Bay Office Furniture Inc. (TBOF) is a publicly held company that manufactures office furniture. The company has two sales offices and a manufacturing plant in the Tampa Bay area. The company has an IBM AS/400 based accounting system that was implemented three years ago. The system was developed in-house. Internally, the company has installed a Novell network that connects all employee desktop computers to the AS/400 system. You are part of the IT audit team in the audit firm performing the independent audit of TBOF. You have been assigned to review and evaluate the IT general controls over:

- Access to the system
- Program change procedures
- Computer operations

As part of the audit process, you have interviewed various personnel in TBOF’s computer department, beginning with Mr. David Smith who is the manager of the IT department at TBOF. You have also observed personnel performing their regularly assigned duties and reviewed systems documentation and logs. Based on your interviews, observations and review of documentation, you have compiled a set of ‘audit notes’.

**Required**

1. Construct an internal control questionnaire (ICQ) containing questions for each of the three areas (access, program changes, operations), drawing from COBIT. Indicate the COBIT detailed control objective (e.g., PO1.1) relating to each ICQ question. The questions should be framed such that a ‘yes’ answer indicates a control strength and a ‘no’ answer signifies a control weakness. Only include questions that apply to the TBOF scenario.

2. For each of your questions, answer ‘yes’ or ‘no’ based on the information available in your audit notes. A ‘yes’ answer indicates a control strength and a ‘no’ answer indicates a control weakness. Note that some of the information in the audit notes may be irrelevant to constructing the ICQ. Also, for each ICQ question, indicate the audit note number relating to the question and the audit test(s) that should be undertaken to verify the ‘yes’ answers, i.e., to confirm that the control is operating properly. You may use the sample ICQ in this publication on page 8 as a model.

**Audit Notes**

1. Observed that the AS/400 system is housed in a secure area on the third floor of TBOF’s corporate office. Access to the computer room is controlled by an electronic card-key system. All entries to and exits from the computer room are logged. There is a Halon gas system installed that is automatically triggered in the event of smoke or fire.

2. In the initial interview with Mr. Smith, he indicated that the IT department was organised in the following sub-areas: systems administration, security, programming, testing and operations. There are 11 employees within the IT department.

Audit notes 3 through 25 and the sample ICQ have been removed from this sample.
ISACA Professional Guidance Publications

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

Frameworks and Model
- 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

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 CMMI® for Development V1.2 With COBIT® 4.1, 2011
- COBIT® Mapping: Mapping of FFEIC With COBIT® 4.1, 2010
- COBIT® Mapping: Mapping of ISO 20000 With COBIT® 4.1, 2011
- 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
- Implementing and Continually Improving IT Governance, 2009

Risk IT-related Publication
- The Risk IT Practitioner Guide, 2009

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

Academic Guidance
IT Governance Using COBIT® and Val IT™ material:
- Caselets, 2nd Edition and Teaching Notes, 2007
- TIBO Case Study, 2nd Edition and Teaching Notes, 2007 (Spanish translation also available)
- Presentation, 2nd Edition, 2007 (35-slide PowerPoint deck on COBIT)
- Caselets, 3rd Edition and Teaching Notes, 2010
- City Medical Center Case Study. 3rd Edition and Teaching Notes, 2010
- Tampa Bay Office Furniture Inc. and Teaching Notes, 2011
Academic Guidance cont.
Information Security Using the CISM® Review Manual and BMISTM material:
• Caselets, 2010
• More 4Less Foods Case Study, 2010
• Teaching Notes, 2010

Executive and Management Guidance
• An Executive View of IT Governance, 2008
• An Introduction to the Business Model for Information Security, 2009
• Board Briefing on IT Governance, 2nd Edition, 2003
• Creating a Culture of Security, 2011
• Information Security Governance—Top Actions for Security Managers, 2005
• ITGI Enables ISO/IEC 38500:2008 Adoption, 2009
• IT Governance and Process Maturity, 2008
• 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 Roundtables:
  – Defining IT Governance, 2008
  – IT Staffing Challenges, 2008
  – Unlocking Value, 2009
  – Value Delivery, 2008
• Global Status Report on GEIT 2011, 2011
• 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:
  – Apache™ Web Services Server Audit/Assurance Program, 2010
  – Change Management Audit/Assurance Program, 2009
  – Cloud Computing Management Audit/Assurance Program, 2010
  – Crisis Management Audit/Assurance Program, 2010
  – Generic Application Audit/Assurance Program, 2009
  – Identity Management Audit/Assurance Program, 2009
  – Information Security Management Audit/Assurance Program, 2010
  – IT Continuity Planning Audit/Assurance Program, 2009
  – Microsoft® Internet Information Services (IIS) 7 Web Services Server Audit/Assurance Program, 2011
  – Microsoft® SQL Server® Database Audit/Assurance Program, 2011
  – Mobile Computing Security Audit/Assurance Program, 2010
  – MySQL™ Server Audit/Assurance Program, 2010
  – Network Perimeter Security Audit/Assurance Program, 2009
  – Outsourced IT Environments Audit/Assurance Program, 2009
  – Security Incident Management Audit/Assurance Program, 2009
  – Social Media Audit/Assurance Program, 2011
  – UNIX/Linux Operating System Security Audit/Assurance Program, 2009
  – VMWare® Server Virtualization Audit/Assurance Program, 2011
Practitioner Guidance cont
- Windows Active Directory Audit/Assurance Program, 2010
- 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
- IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, 2011
- 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
- SharePoint® Deployment and Governance Using COBIT® 4.1: A Practical Approach, 2010
- Stepping Through the IS Audit, 2nd Edition, 2004
- Stepping Through the InfoSec Program, 2007
- Technical and Risk Management Reference Series:
- Top Business/Technology Issues Survey Results 2011, 2011
- Top Business/Technology Survey Results, 2008
- White Papers:
  - Data Analytics—A Practical Approach, 2011
  - Data Leak Prevention, 2010
  - Electronic Discovery, 2011
  - Leveraging XBRL for Value in Organizations, 2011
  - New Service Auditor Standard: A User Entity Perspective, 2010
  - Securing Mobile Devices, 2010
  - Social Media: Business Benefits and Security, Governance and Assurance Perspectives, 2010
  - Sustainability, 2011
  - Virtualization: Benefits and Challenges, 2010