

Are you interested in COBIT or Computer Forensics Training?

In order to better serve our members, the ISACA Philadelphia Chapter is eager to know your interest level in attending any of the following training courses:

- **Course 1** - Foundation Course: Implementing COBIT™
- **Course 2** - Implementing COBIT™ for IT Management and Governance
- **Course 3** - Fundamental Forensics for Auditors and Info Security Professionals

If there are enough members interested in attending these training courses on October 1-5, 2007, then the chapter will confirm the training schedule with these **World-Class** presenters.

Can you please review these training courses and notify us via email if you are interested in attending? Simply notify us via email at phillyisaca@yahoo.com by **Friday, April 20th** and indicate in the email which course(s) you are interested in attending: Course 1, 2, or 3, or any combination.

If you have any questions about the training courses, send an email to Steve Oberhauser at soberhauser@kpmg.com.

Donald F Caniglia, CISA, CISM, FLMI

Mr. Caniglia has been providing Information Systems Audit, financial/operational audit, information security consulting services and IS Audit and security training primarily to the financial services industry for more than 30 years. He has been a Certified Systems Auditor since 1984 and recently awarded the Certified Information Security Manager designation from the Information Systems Audit and Control Association (ISACA). He has better than 18 years direct experience in Banking and S&L operational Audit, IS Audit, Systems Support and Information Security, with the last several years providing IS Audit, Security and Compliance services to Community Banks. Some examples of his expertise include:

- Developed IS control structure implementation and governance processes,
- Established audit consulting services focusing on technology - based audits for diverse multi-platform environments with emphasis on compliance to regulatory practices, information security control implementation, data center and network operations, change management, technological control integration into business processes,
- Designed and Implemented Information technology and security policies and procedures,
- Established business continuity plans and business impact analysis processes
- Established GLBA compliance audit program and risk assessment and vendor management practices.
- Coordinated implementation of formalized Performance Management and Incentive Compensation System,
- Identified and implemented certification standards and baseline metrics, audit and attestation methods for network connectivity,
- Developed nineteen professional audit and technology-based seminars and presented more than 200+ instructional sessions to clients for all major industries worldwide since 1985.

One-day Course

COB100: Foundation Course: Implementing COBIT™

CPEs: 14

Description:

The seminar considers the need for an IT governance and control framework and explains how this is addressed by COBIT. The elements of the COBIT framework are explained using practical examples and scenario-based learning to show a process to successfully manage IT resources. For most organizations, one of the largest and least managed resources is Information Technology. As a manager, it is critical to know the business impacts and resource requirements and utilization of all processes as well as returns based on those processes. This seminar provides a framework that facilitates the management of the IT processes.

Audience:

This seminar is intended for organizational and IT management including anyone in the decision making and oversight processes for managing IT resources. Additional beneficiaries could include internal and external audit professionals, C-Level managers and decision makers. Security Officers, Controllers and their management, InfoSec professionals, operations managers, and anyone interested in obtaining a better understanding of the requirements necessary for identifying, developing and maintaining a viable and successful enterprise-wide IT governance initiative.

Prerequisites:

There is no prerequisite for this seminar.

Objectives:

After completing this seminar, participants will understand:

- The principles of IT Governance, how IT Governance helps organizations deal with IT management issues, and who should be responsible for IT Governance
- How IT management issues are affecting organizations;
- The need for a control framework driven by the need for IT Governance;
- How COBIT meets the requirement for an IT Governance framework;
- How COBIT is used with other standards and best practices;
- The benefits of using COBIT;
- The COBIT Framework and all the components of CobiT (Control Objectives, Control Practices, Management Guidelines, Audit Guidelines); and
- How to apply COBIT in a practical situation.

Course Outline:

- Responding to IT Challenges
- Introducing COBIT
- What does COBIT Provide? – Part 1
- What does COBIT Provide? – Part 2
- Applying COBIT in Practice
- Products and Support from ITGI

Two-day Course

COB200: Implementing COBIT™ for IT Management and Governance

CPEs: 14

Description:

Success in any organization has many factors, the least of which is proper management of resources. For most organizations, one of the largest and least managed resources is Information Technology. As a manager, it is critical to know the business impacts and resource requirements and utilization of all processes as well as returns based on those processes. Proper resource allocation and management is one of the five defined areas of governance along with strategic alignment, value addition, risk mitigation and measurement. Session participants will learn what governance should entail and how it can be implemented using the COBIT framework.

Audience:

This seminar is intended for organizational and IT management including anyone in the decision making and oversight processes for managing IT resources. Additional beneficiaries could include internal and external audit professionals, C-Level managers and decision makers. Security Officers, Controllers and their management, InfoSec professionals, operations managers, and anyone interested in obtaining a better understanding of the requirements necessary for identifying, developing and maintaining a viable and successful enterprise-wide IT governance initiative.

Prerequisites:

There is no prerequisite for this seminar.

Objectives:

After completing this seminar, participants will be able to:

- Understand the appropriate approach to implementation of governance practices using the implementation roadmap.
- Scope and plan IT governance initiatives.
- Identify needs using KPI's and KGI's.
- Create performance measurement framework using COBIT's measures and balanced scorecard
- Consider practical implementation strategies
- Understand how COBIT supports the implementation of governance practices.
- Assess process capability and maturity.
- Plan improvements using control objectives and control practices.
- Sustain IT governance practices
- Understand of implementation support resources.

Course Outline:

- Introduction to IT Governance Implementation and COBIT
- Scoping the use of COBIT
- Analyzing process maturity and identifying gaps
- Improvement strategies, defining projects & change plan
- Production & Measure performance
- Governance organization and processes
- Identify Needs
- Envision the Solution
- Plan Solution
- Implement Solution
- Building Sustainability
- This seminar is based on materials from COBIT Version 4 which is owned and provided by ISACA and ITGI.



Albert J. Marcella Jr., Ph.D., COAP, CQA, CCP, CDP, CFSA, CISA

Albert J. Marcella Jr., is president of Business Automation Consultants, LLC a global information technology and management-consulting firm providing information technology (IT) management consulting and IT audit and security reviews and training for an international clientele. Dr. Marcella is an internationally recognized public speaker, researcher, and seminar leader with 30 years of experience in IT audit, security and assessing internal controls, and an author of numerous articles and 28 books on various audit and security related subjects. Prior to the formation of his own firm in 1984, Dr. Marcella was employed by the Dun & Bradstreet Corporation where he established and formalized that organization's IT Audit function.

Dr. Marcella's additional professional experiences include providing internal systems consulting services to the Hartford Insurance Group, and the design and execution of operational, financial, and information technology audits for the Uniroyal Corporation, both in the United States and abroad. Dr. Marcella's most recent books include such titles as:

- **Disaster Recovery, Business Continuity, and Incident Management Planning: A Resource for Ensuring Ongoing Enterprise Operations**, which examines such critical issues as the key components of disaster recovery, business continuity and incident management plan, how to measure the effectiveness of an organization's business recovery, continuity and planning program, and what questions should be asked to determine an organization's overall preparedness to endure a disaster "event".
- **Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues**, providing organizations with everything they need to know to ensure that privacy considerations cohere with their global business strategy. In today's politically and financially volatile environment, corporations must keep up with current privacy legislation and mores, as well as have a strong company privacy policy that their employees and customers can trust.
- **Cyber Forensics: Collecting, Examining, and Preserving Electronic Evidence An Auditor's Field Manual**, focuses on issues, tools, and control techniques designed to assist audit, law enforcement, and infosecurity professionals in the successful investigation of illegal activities perpetrated through the use of information technology.
- WWW.StopThief.net, a text which comprehensively examines the growing threat and critical issue of identity theft, in the emergent presence of virtual markets.

Dr. Marcella holds a Ph.D. in Management with emphasis in Information Technology from Walden University, a Masters of Business Administration in Finance, from The University of New Haven, and a Bachelor of Science degree in Business Administration with a dual major in Management Information Systems and Management from Bryant University. Dr. Marcella's dissertation research examined the relationship between Ethics and Auditor Judgment.

Dr. Marcella is the Institute of Internal Auditors Leon R. Radde Educator of the Year, 2000, Award recipient. Dr. Marcella has taught IT audit seminar courses for the Institute of Internal Auditors, the Information Systems Audit and Control Association, and has been recognized by the IIA as a Distinguished Adjunct Faculty Member.

Two-day Course

Fundamental Forensics for Auditors and Info Security Professionals

CPE credits: 14.0

Description:

Traditional forensics professionals use fingerprints, DNA typing, and ballistics analysis to make their case. Infosec professionals have to develop new tools for collecting, examining and evaluating data in an effort to establish intent, culpability, motive, means, methods and loss resulting from e-crimes. This overview seminar will introduce the attendee to the broad field of cyber forensics and present the various tools and techniques designed to maintain control over organizational assets, digital or otherwise. This seminar covers computer forensics theory and methodology. It is not limited to the use of a specific software tool.

Audience:

This seminar is intended for internal and external audit professionals, General Counsels, Chief Security Officers, Controllers, InfoSec professionals, anyone interested in obtaining a better understanding of and general introduction to cyber forensics.

Prerequisites:

Attendees should possess a basic understanding of information technology concepts. Learning level – basic. No advanced preparation is required for this seminar.

Learning Outcomes:

After completing this seminar, participants will be able to:

- Identify, establish and maintain a physical "chain of custody."
- Pinpoint computer security risks and remedies.
- Determine incident responses and priorities in a cyber forensic investigation.
- Develop policies for the preservation of computer evidence.
- Implement solid computer forensics processing methods and procedures.
- Develop the documentation of computer forensics findings for executive management review.
- Coordinate Forensic Pre-Incident Preparation.
- Identify, establish and maintain a physical "chain of custody."
- Determine procedures necessary for gathering of all pertinent "Live" information.
- Identify volatile data, photos, physical media, and log files.
- Perform forensic acquisition of physical media.
- Identify various forensic toolkits and associated methodologies.
- Determine procedures necessary to conduct sound forensic analysis of the collected information.
- Identify essential components of a forensic analysis report.
- Communicate findings from a cyber forensic investigation to non-technical audiences.

Course Outline:

- Cyber Forensics Defined
- Junk Science Attack and the Investigator
- Rules of Evidence – Importance and Application to Forensic Investigations
- Establishing a Credible Chain of Custody
- Burn the Witness – Will You Be a Victim?
- Beginning an Investigation – Taking the Critical, Correct First Steps
- Investigation Methodology – The Good, the Bad, and the Dangerous
- Essential Steps in Preparing and Conducting an Investigation
- Creating a Safety Net
- Creating a Forensic Start-up Disk
- Preparing the Evidence Drive on the Processing Machine
- The Forensic Process - Taking Control of the Computer and Its Environment.
- Potential Exposures – Minimizing Your Risk and Exposure
- Uncovering Digital Evidence – Where Is It and How Do I Find It?
- Computer DNA – All You Need To Know
- Documentation Methodologies – Preserving Evidence and Creating Audit Trails
- I've Gathered Evidence Now What?
- Presenting the Evidence Report - Successfully
- Summary

Dr. Marcella's seminar is based on research and findings from his book, [Cyber Forensics](#), published by Auerbach Publications, ISBN 0-8493-0955-7, and research currently underway for his second text on cyber forensics due for release in November 2007.