CCITAGS
Canadian Conference on IT Audit, Governance and Security

April 2-4, 2019
The Globe and Mail Center
Toronto

The Institute of Internal Auditors Toronto Chapter
The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada
CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Fundamentals of Information Technology Audit

April 3-4, 2019, Toronto

Time: Two full days of class time in total, which includes two case studies.

Workshop Leader: Craig R. McGuffin, CPA, CA, CITP, CISA, CISM, CGEIT, CRISC
Principal of C.R. McGuffin Consulting Services

WORKSHOP AGENDA:

Part 1 — The IT Audit Process
An overview covering setting up the IT audit function within an organization, as well as conducting individual audits. Also covers the objectives of various types of IT audits, as well as audit risks.

Part 2 — Control Overview / Impact on Audit Strategy
Discuss control objectives and categorizations (e.g. general vs. business process, preventive vs. detective). Introduces the control benchmark we'll be using during subsequent sections. Discuss the impact of controls on audit strategy and testing.

Part 3 — Controls Over IT Management
Examine the types of controls expected over the management of IT. Examples include long-range and short-range planning, steering committee, issuing governance, risk management.

Part 4 — Controls Over SDLC
Review the traditional systems development life cycle, and examine the controls expected at each point. Special focus on controls over the transition of systems from development to testing to production. Also covers steps suitable for package acquisition. Includes a case study to identify missing controls.

Part 5 — Controls Over IT Operations
Examine the types of controls expected over IT operations. Examples include hardware capacity planning and monitoring, operating schedules, and preventative maintenance. Also covers controls over outsourcing.

Part 6 — Controls Over IT Security
Examine the types of controls expected over logical and physical security of IT systems. Will include a generic model for security controls, then apply to examples at the operating system, database, and firewall levels. Includes a case study to identify missing controls.

Part 7 — Controls Over BCP / DRP

Review the process for developing Business Continuity Plans and Disaster Recovery Plans, including key concepts (user-driven BIAs, Recovery Point Objective, Recovery Time Objective), and examine the control expectations at each level. Also addresses the overall topic of Incident Response.

Part 8 — Controls Over Business Processes

Explains business process (application) controls, and their relationship to the general controls covered previously. Discuss typical information system processing components (transaction files, master files) and the controls appropriate for each. Consideration of two methods of evaluating business controls: traditional (checklist based) and systematic. Also includes a discussion of documentation requirements and techniques.

Part 9 — Testing IT Controls

Discuss options and techniques for testing IT controls found during the audit.

Part 10 — Communicating Audit Findings

Discuss issues surrounding communicating audit findings, techniques for presentation, and whether recommendations are appropriate in all cases.