GROWTH LAB
& Executive Training

Risk Based IT Auditing Special Practical Summit

Introducing control techniques and best practices to ensure the confidentiality, integrity, and availability of your information assets

15th – 19th October, 2018, Premier Hotel, OR Tambo Int. Airport, Johannesburg, RSA

ABOUT THE WORKSHOP:

From the European Union Data Protection Directive to Basel II and Sarbanes-Oxley, recent regulations require organizations to ensure appropriate levels of protection for their critical information assets. To be sure, the common thread through these mandates is the requirement for security and effective controls at all levels of the enterprise. In this practical, five-day Special Summit you will immerse yourself in a risk-based approach to IT auditing that will ensure the confidentiality, integrity, and availability of your information assets throughout the enterprise. You will review COBIT, ISO-27002 and a number of other standards/ frameworks and learn how they can be applied to your IT audits to provide an appropriate risk focus. You will concentrate on determining risk in critical areas of the IT environment, including operating systems, database management systems, networks, logical security, change management, business continuity planning and application controls. You will learn a pro- active audit approach that will provide a value-added service to your organization. You will leave this intensive seminar with a thorough understanding of risk-based IT audit and control best practices that you can apply immediately to your next IT audit. **Leave with an action plan of best practices to apply immediately on the job.**

BENEFITS OF THIS TRAINING:

LEARN TO…:

- ***Plan***
  Your IT audit using risk-based approach, COBIT and COSO control framework
- ***Determine***
  Risk in critical areas of your IT environment, including operating systems, database management systems, business continuity and application controls
- ***Apply Risk Management Techniques***
  A pro-active audit approach to provide a value-added service to your organization
- ***Identify pros and cons of outsourced IT Operations***
  Outsourced IT operations
- ***Understand***
  Why IT governance is critical
- ***Perform Audits on***
  System development project

TRAINING METHODOLOGY:

The methodology is based on interactive learning, i.e. delegates will learn by doing. Furthermore delegates will use examples from their own environment, thus ensuring that all our delegates are anchored on their workplace. Most of the interactive learning will take the form of simulated exercises, interactive and illustrational video lessons, case studies where our delegates demonstrate the skills taught. At GrowthLab & Executive training with its partners, we strive to promote change and shift our delegates' mind-set through effective practical based training.

WHO SHOULD ATTEND?

Anyone responsible for ensuring the continuity of an organization's critical systems or processes, including **project and business managers, Internal Auditors,**

- **IT Audit Managers**
- **Information Systems Auditors,**
- **Information Security Managers and Analysts**
- **Information Management Systems Managers,**

LEARNING BASED OUTLINE

Managing Risks to the Organization

Characterizing risks

- Defining and identifying the sources of risk
- Choosing a risk assessment method
- Communicating risks across the organization

Developing appropriate responses

- Matching the response to the risk
- Taking preventive action
- Ensuring appropriate contingencies are in place

Planning the IT audit

- Risk-based auditing
- Integrated audit approaches
- Developing the audit strategy
- Using the COSO control framework for audit planning
- Planning and executing the audit

Risk assessment

- Risk-based auditing
- Identifying risk factors, vulnerabilities, and threats
- Business and technical risks
- Cost/risk evaluation
- Risk assessment factors
- IT risks in an automated environment

Complying with international regulations

- Risk coverage required by international data protection acts
- European Union Data Privacy
- Basel II
- Sarbanes-Oxley
- Payment Card Industry DSS

Using COBIT

- COBIT control objectives
- COBIT framework and domains
- Utilizing COBIT in planning the audit
- Applying COBIT audit guidelines

Applying the ISO-27002 security standard

- ISO 27002 structure overview
- Referencing the standard for auditing
- Security policies
- Information classification
- Physical security
- Access controls
- security monitoring

IT governance

- IT governance defined
- Why IT governance is critical
- Linking enterprise and IT strategies
- IT organization and management
- Policies and procedures
- IT steering committee
- Information security governance
- Separation of duties
- IIA and ISACA governance audit guidelines

System software

- Software integrity
- Operating system risks and controls
- Controlling privileged access
- Activity logging
- Vendor patch management
- Database management risks and controls
- Utility programmes
- Audit steps

Logical access controls

- Logical access control objectives
- Integrated roles of IT and business process owners
- Authentication objectives: password controls, tokens, and biometrics
- Authorization
- Audit trail
- Managing user accounts
- Security monitoring
- Single sign-on (SSO) authentication
- Remote access
- Sensitive data on PCs and
- workstations
- Social engineering risks
- Centralized vs. decentralized control
- Access control best practices
- Audit steps

Change management

- Change management objectives/risks
- Change requests
- Testing changes
- Implementation approval
- Programme migration
- Contingency plans
- System documentation
- Executable and source code integrity
- Emergency changes

- Library control software
- Vendor-supplied source code
- Audit steps

Physical and environmental controls

- Physical security objectives, risks, exposures, and controls
- Environmental exposures and risks
- Environmental controls: fire protection, water protection, and power conditioning audit steps

Network perimeter security

- Network security threat/risk analysis
- Network security strategy
- OSI model
- TCP/IP
- Firewalls
- DMZ
- Intrusion detection systems
- Remote access
- Wireless access
- Audit strategies encryption
- Types of encryption
- Symmetric and asymmetric encryption
- Public key infrastructure
- Network encryption layers
- Secure sockets layer
- Digital signatures

Application controls

- Relationship between general controls and application controls
- Business applications risks
- Transaction life cycle
- Completeness and accuracy of input
- Completeness and accuracy of processing
- Exception reporting
- Output controls
- Application change management
- End user computing
- Business/data warehouses
- Application system audit strategy

Disaster recovery and business continuity

- Disaster recovery planning
- Business continuity planning
- Business impact analysis
- Recovery time objectives
- Continuity plans and procedures
- Off-site data storage and information processing
- Contract requirements
- Auditing disaster recovery and business continuity plans

Auditing outsourced IT Operations

- Outsourcing risks
- Offshore outsourcing risks
- Ensuring strong contractual agreements
- How to obtain a right to audit
- Obtaining and assessing SAS-70 reports
- Relationship monitoring
- Audit focus areas

Auditing system Development projects

- Audit's role on development projects
- Business risks of development project
- Why auditors should be involved
- Getting involved how, when, who?
- Staffing the audit
- Communicating audit's roles & results
- Assessing project management
- System acquisitions
- Audit strategy

Executing IT audits

- Risk assessment
- Planning the audit
- Developing audit programs
- Testing controls
- Using CAATs and data analysis
- Work papers
- Audit report
- IT audit tool kit