

Introduction To IS Auditing

Instructor:

Bryan McAtee, ASA, CISA

Bryan McAtee & Associates - Brisbane, Australia

- * Course, Presenter and Delegate Introductions
- * Definition of Information Technology (IT) Auditing
- * IT Audit Standards & IT Best Practice
- * The IT Control Mix
- * Classification of IT Controls
- * Overview of IT Audit Process
- * IT Control Areas

IT Management

- * Planning for the IT Department/Activity
 - Long-Range Planning for the Organization
 - The Planning or Steering Committee for the IT Department
 - Long-Range Planning for the IT Department
 - Short-Range Planning for the Organization and for the IT Department
- * Policies, Standards and Procedures
 - Policies
 - Standards
 - Procedures
- * Organizational Responsibilities and Personnel Management
 - The Organizational Location of the IT Department
 - Description of Responsibilities Within the IT Department
 - The Segregation of Duties
 - The IT Department Position Descriptions
 - Personnel Selection
 - Personnel Security Clearance Procedures
 - Personnel Separation Procedures
 - Personnel Training
 - Employee Job Performance Evaluation
- * IT Department/Activity Quality Assurance
 - Responsibility for Quality Assurance (QA)
 - Organizational Aspects of the QA Function
 - The Qualifications of QA Personnel

- The QA Review Plan
- The QA Review of the Achievement of the IT Department's Objectives
- The QA Review of Adherence to the IT Department's Standards and Procedures
- The QA Review of Systems Controls
- The QA Review of Other Aspects of the IT Department's Functions
- Reports of Quality Assurance Reviews
- * External Requirements
 - Research the Applicable External requirements for an Organization
 - Evaluate Organization's Level of Compliance
- * Case Study on Management Controls

IT Systems Development

- * Systems Development Life Cycle Methodology and Responsibility (SDLC)
 - System Development Life Cycle Methodology
 - Roles and Responsibilities
 - Updating the System Development Life cycle
- * Project Initiation
 - Project Definition
 - User Department Participation in Project Initiation
 - Project Team Membership and Responsibilities
 - Definition of Information Requirements
 - Project Approval
- * Feasibility Study
 - Formulation of Alternative Courses of Action
 - Technological Feasibility Study
 - Economic Feasibility Study
 - Risk Analysis Report
 - Project Approval
 - Project Master Plan
 - Cost Monitoring
- * Design Phase
 - Design Methodology
 - Output Requirements Definition and Documentation
 - Input Requirements Definition and Documentation
 - File Requirements Definition and Documentation
 - Processing Requirements Definition and Documentation
 - Program Specifications
 - Source Data Collection Design
 - Controls and Security Design
 - Audit Trails Design
 - Design Approval
 - Program Documentation Standards
 - Validation, Verification and Test Plan
- * Development and Implementation

- Programming Objectives
- Detailed Program Documentation
- Application Software Packages
- Contract Application Programming
- Operations and Maintenance Manual
- User Manuals
- Training Plan
- Program Testing Standards
- System Testing Standards
- System Testing Documentation
- Evaluation of Test Results
- Conversion Plan
- Parallel Testing
- Final Acceptance Test
- * Operation and Maintenance
 - Operations Control Procedures
 - Cost Monitoring
 - System Modifications
 - Re-evaluation of User Requirements
- * Post Implementation Review
 - Post Implementation Review Plan
 - Results Evaluation
 - Evaluation of Meeting User Requirements
 - Evaluation of Cost-Benefit Analysis
 - Evaluation of Adherence to Development Standards
 - Reporting Post Implementation Review Findings
- * Case Study on SDLC

IT Operations & Networks

- * IT Resource Planning and Management
 - The Annual IT Operating Budget
 - Hardware Acquisition Plan
 - Capacity Management of Hardware
- * Computer Operations
 - Workload Scheduling
 - Personnel Scheduling
 - Preventive Maintenance for Hardware
 - Problem Management
 - Change Management
 - Job Cost Accounting
 - User Billing and Chargeback Procedures
 - Media Library Management Responsibilities
 - The Media Library Management System
 - Magnetic Media External Identification and Control
 - Processing Operations Procedures

- * Networks & Distributed Processing
 - Understanding Company Management Objectives
 - Network Implementation Plan
 - Control Standards for the Network
 - Hardware and Software Control Features
 - Database Distribution
 - Network Data Standards
 - Access to Network Data
 - Network Data Review Mechanism
 - Hardware and Software Backup Provisions
 - Network Operations
 - Software Communications
 - Access to Network Operating Systems Software
 - Access to Network Processing Facilities
 - Data Encryption
 - Network Security
 - Network Security Reviews
 - Documentation & Training of Network Operations Personnel
 - Network Post-Implementation Review
 - Network Performance Monitoring
 - Network Contingency Operations Plans
- * Network Redundancy Case Study
- * Operating System Software
 - Selection of System Software
 - Cost-Benefit of Systems Software
 - Installation of Changed System Software
 - System Software Maintenance
 - System Software Change Control
 - System Software Problem Management
 - System Software Security
- * Logical and Physical Security
 - Responsibility for Logical and Physical Security
 - Access to Computer Facility
 - Visitor Escort
 - Password Administration
 - Violation and Security Activity Reports
 - Logical Access Restrictions
 - Security of On-Line Access to Data
 - Limited Identification of the Data Processing Site
 - Fire Protection
 - Training in Security Procedures and Awareness
- * Disaster Recovery Planning
 - The Disaster Recovery Plan
 - Personnel Safety and Training in Emergency Procedures
 - Critical Data Processing Applications
 - Critical Computer Resources

- Telecommunication Services Restoration
- Back-Up: Site and Hardware
- Programming for Back-Up Operations
- Data File Recovery Procedures
- Disaster Recovery Supplies
- Testing the Disaster Recovery Plan
- Reconstruction of the IT Operations Site
- User Department Manual Processing Back-Up Procedures
- * Video on Disaster Recovery Planning

Application Software

- * Data Origination Controls
 - Data Preparation Procedures
 - Source Document Design
 - Source Document Control
 - Data Input Authorization Procedures
 - Source Document Retention
- * Data Input Controls
 - Data Conversion and Entry Procedures
 - On-Line Data Conversion and Entry Procedures
 - Data Validation and Editing
 - Data Input Error Handling
- * Data Processing Controls
 - Data Processing Integrity
 - Data Processing Integrity Provisions in Application Program

Software

- Data Processing Validation and Editing
- Data Processing Error Handling
- * Data Output Control
 - Output Review
 - Output Balancing and Reconciliation
 - Output Distribution
 - Output Error Handling
 - Output Handling and Retention
 - Security Provisions for Output Reports
- * Case Study on Application Controls

Note:

Throughout the course copies of Control Benchmarks for implementation by management, corresponding Audit Plans (160 in all) for use by the auditor, and flowcharts of audit programs are provided to delegates.