# Table of Contents

## PART I. IS Audit Process.

### CHAPTER 1. Technology and Audit.
- Technology and Audit.
- Batch and On-Line Systems.

### CHAPTER 2. IS Audit Function Knowledge.
- Information Systems Auditing.
- What Is Management?
- Understanding the Organization's Business.
- Establishing the Needs.
- Identifying Key Activities.
- Establish Performance Objectives.
- Decide The Control Strategies.
- Implement and Monitor the Controls.
- Executive Management’s Responsibility and Corporate Governance.
  - Audit Role.
  - Conceptual Foundation.
  - Professionalism within the IS Auditing Function.
  - Relationship of Internal IS Audit to the External Auditor.
  - Relationship of IS Audit to Other Company Audit Activities.
  - Audit Charter.
  - Charter Content.
  - Outsourcing the IS Audit Activity.
  - Regulation, Control, and Standards.

### CHAPTER 3. IS Risk and Fundamental Auditing Concepts.
- Computer Risks and Exposures.
- Effect of Risk.
- Audit and Risk.
- Audit Evidence.
- Reliability of Audit Evidence.
- Audit Evidence Procedures.
- Responsibilities for Fraud Detection and Prevention.

### CHAPTER 4. Standards and Guidelines for IS Auditing.
- IIA Standards.
- Code of Ethics.
- Advisory.
- Aids.
  - Standards for the Professional Performance of Internal Auditing.
  - ISACA Standards.
  - ISACA Code of Ethics.
  - COSO: Internal Control Standards.
  - BS 7799 and ISO 17799: IT Security.
  - NIST.
  - BSI Baselines.

### CHAPTER 5. Internal Controls Concepts Knowledge.
- Internal Controls.
Cost/Benefit Considerations.
Internal Control Objectives.
Types Of Internal Controls.
Systems of Internal Control.
Elements of Internal Control.
Control Procedures.
Application Controls.
Control Objectives and Risks.
General Control Objectives.
Data and Transactions Objectives.
Program Control Objectives.
Corporate IT Governance.

Nature of Risk.
Auditing in General.
Elements of Risk Analysis.
Defining the Audit Universe.
Computer System Threats.
Risk Management.

Benefits of an Audit Plan.
Structure of the Plan.
Types of Audit.

CHAPTER 8. Audit Management.
Planning.
Audit Mission.
IS Audit Mission.
Organization of the Function.
Staffing.
IS Audit as a Support Function.
Planning.
Business Information Systems.
Integrated IS Auditor vs Integrated IS Audit.
Auditees as Part of the Audit Team.
Application Audit Tools.
Advanced Systems.
Specialist Auditor.
IS Audit Quality Assurance.

Audit Evidence.
Audit Evidence Procedures.
Criteria for Success.
Statistical Sampling.
Why Sample?
Judgmental (or Non-Statistical) Sampling.
Statistical Approach.
Sampling Risk.
Assessing Sampling Risk.
Planning a Sampling Application.
Calculating Sample Size.
Quantitative Methods.
Project Scheduling Techniques.
Simulations.
Computer Assisted Audit Solutions.
Generalized Audit Software.
Application and Industry-Related Audit Software.
Customized Audit Software.
Information Retrieval Software.
Utilities.
On-Line Inquiry.
Conventional Programming Languages.
Microcomputer-Based Software.
Test Transaction Techniques.

CHAPTER 10. Audit Reporting Follow-up.
Audit Reporting.
Interim Reporting.
Closing Conferences.
Written Reports.
Clear Writing Techniques.
Preparing To Write.
Basic Audit Report.
Executive Summary.
Detailed Findings.
Polishing the Report.
Distributing the Report.
Follow-Up Reporting.
Types of Follow-Up Action.

PART II. Information Systems/Information Technology Governance.

CHAPTER 11. Management.
IS Infrastructures.
Project-Based Functions.
Quality Control.
Operations and Production.
Technical Services.
Performance Measurement and Reporting.
Measurement Implementation.

CHAPTER 12. Strategic Planning.
Strategic Management Process.
Strategic Drivers.
New Audit Revolution.
Leveraging IS.
IS as an Enabler of Re-Engineering.
Dangers of Change.
System Models.
Information Resource Management.
Strategic Planning for IS.
Decision Support Systems.
Steering Committees.
Strategic Focus.
Auditing Strategic Planning.
Design the Audit Procedures.

Privacy.
Copyrights, Trademarks, and Patents.
Ethical Issues.
Corporate Codes of Conduct.
IT Governance.
Sarbanes-Oxley Act.
Housekeeping.

General Frameworks.
COSO: Internal Control Standards.
Other Standards.

CHAPTER 15. Governance Techniques.
Change Control.
Problem Management.
Auditing Change Control.
Operational Reviews.
Performance Measurement.
ISO 9000 Reviews.

PART III. Systems and Infrastructure Lifecycle Management.

Stakeholders.
Operations.
Systems Development.
Technical Support.
Other System Users.
Segregation of Duties.
Personnel Practices.
Object-Oriented Systems Analysis.
Enterprise Resource Planning.

CHAPTER 17. Information Management and Usage.
What Are Advanced Systems?
Service Delivery and Management.

Programming Computers.
Program Conversions.
System Failures.
Systems Development Exposures.
Systems Development Controls.
Systems Development Life Cycle Control: Control Objectives.
Micro-Based Systems.

Impact.
Continuous Monitoring.
Business Process Outsourcing.
E-Business.

CHAPTER 20. Software Development.
Developing a System.
Change Control.
Why Do Systems Fail?
Auditor's Role in Software Development.

CHAPTER 21. Audit and Control of Purchased Packages.
Information Systems Vendors.
Request For Information.
Requirements Definition.
Request For Proposal.
Installation.
Systems Maintenance.
Systems Maintenance Review.
Outsourcing.

CHAPTER 22. Audit Role in Feasibility Studies and Conversions.
Feasibility Success Factors.
Conversion Success Factors.

CHAPTER 23. Audit and Development of Application Controls.
What Are Systems?
Classifying Systems.
Controlling Systems.
Control Stages.
System Models.
Information Resource Management.
Control Objectives of Business Systems.
General Control Objectives.
CAATS and their Role in Business Systems Auditing.
Common Problems.
Audit Procedures.
CAAT Use in Non-Computerized Areas.
Designing an Appropriate Audit Program.

PART IV. Information Technology Service Delivery and Support.

Auditing the Technical Infrastructure.
Computer Operations Controls.
Operations Exposures.
Operations Controls.
Personnel Controls.
Supervisory Controls.
Operations Audits.

CHAPTER 25. Service Center Management.
Continuity Management and Disaster Recovery.
Managing Service Center Change.
PART V. Protection of Information Assets.

What Is Information Systems Security?
Control Techniques.
Workstation Security.
Physical Security.
Logical Security.
User Authentication.
Communications Security.
Encryption.
How Encryption Works.
Encryption Weaknesses.
Potential Encryption.
Data Integrity.
Double Public Key Encryption.
Steganography.
Information Security Policy.

CHAPTER 27. Logical Information Technology Security.
Computer Operating Systems.
Tailoring the Operating System.
Auditing the Operating System.
Security.
Criteria.
Auditing RACF.
Access Control Facility 2.
Top Secret.
User Authentication.
Bypass Mechanisms.

Communications and Network Security.
Network Protection.
Hardening the Operating Environment.
Client Server and Other Environments.
Firewalls and Other Protection Resources.
Intrusion Detection Systems.

CHAPTER 29. Physical and Environmental Security.
Control Mechanisms.
Implementing the Controls.

PART VI. Business Continuity and Disaster Recovery.

Risk Reassessment.
Disaster—Before and After.
Consequences of Disruption.
Where to Start.
Testing the Plan.
Auditing the Plan.
CHAPTER 31. Insurance.
Self-Insurance.

PART VII. Advanced IS Auditing.

CHAPTER 32. Auditing E-commerce Systems.
E-Commerce and Electronic Data Interchange: What Is It?
Opportunities and Threats.
Risk Factors.
Threat List.
Security Technology.
“Layer” Concept.
Authentication.
Encryption.
Trading Partner Agreements.
Risks and Controls within EDI and E-Commerce.
Nonrepudiation.
E-Commerce and Auditability.
Compliance Auditing.
E-Commerce Audit Approach.
Audit Tools and Techniques.
Auditing Security Control Structures.
Computer Assisted Audit Techniques.

CHAPTER 33. Auditing UNIX/Linux.
History.
Security and Control in a UNIX/Linux System.
Architecture.
UNIX Security.
Services.
Daemons.
Auditing UNIX.
Scrutiny of Logs.
Audit Tools in the Public Domain.
UNIX passwd File.
Auditing UNIX Passwords.

CHAPTER 34. Auditing Windows.
History.
NT and Its Derivatives.
Auditing Windows 23.
Password Protection.
File Sharing.
Security Checklist.

CHAPTER 35. Foiling the System Hackers.

CHAPTER 36. Investigating Information Technology Fraud.
Pre-Incident Preparation.
Detection of Incidents.
Initial Response.
Forensic Backups.
Investigation.
Network Monitoring.
Identity Theft.