## Contents

Preface xi
Acknowledgments xv

**PART ONE: CONDUCTING AN INFORMATION SYSTEMS AUDIT** 1

**Chapter 1: Overview of Systems Audit** 3
- Information Systems Audit 3
- Information Systems Auditor 4
- Legal Requirements of an Information Systems Audit 4
- Systems Environment and Information Systems Audit 7
- Information System Assets 8
- Classification of Controls 9
- The Impact of Computers on Information 12
- The Impact of Computers on Auditing 14
- Information Systems Audit Coverage 15

**Chapter 2: Hardware Security Issues** 17
- Hardware Security Objective 17
- Peripheral Devices and Storage Media 22
- Client-Server Architecture 23
- Authentication Devices 24
- Hardware Acquisition 24
- Hardware Maintenance 26
- Management of Obsolescence 27
- Disposal of Equipment 28
- Problem Management 29
- Change Management 30
- Network and Communication Issues 31

**Chapter 3: Software Security Issues** 41
- Overview of Types of Software 41
- Elements of Software Security 47
- Control Issues during Installation and Maintenance 53
- Licensing Issues 55
- Problem and Change Management 56
Chapter 4: Information Systems Audit Requirements 59
Risk Analysis 59
Threats, Vulnerability, Exposure, Likelihood, and Attack 61
Information Systems Control Objectives 61
Information Systems Audit Objectives 62
System Effectiveness and Efficiency 63
Information Systems Abuse 63
Asset Safeguarding Objective and Process 64
Evidence Collection and Evaluation 65
Logs and Audit Trails as Evidence 67

Chapter 5: Conducting an Information Systems Audit 71
Audit Program 71
Audit Plan 72
Audit Procedures and Approaches 75
System Understanding and Review 77
Compliance Reviews and Tests 77
Substantive Reviews and Tests 80
Audit Tools and Techniques 81
Sampling Techniques 84
Audit Questionnaire 85
Audit Documentation 86
Audit Report 87
Auditing Approaches 89
Sample Audit Work-Planning Memo 91
Sample Audit Work Process Flow 93

Chapter 6: Risk-Based Systems Audit 101
Conducting a Risk-Based Information Systems Audit 101
Risk Assessment 104
Risk Matrix 105
Risk and Audit Sample Determination 107
Audit Risk Assessment 109
Risk Management Strategy 112

Chapter 7: Business Continuity and Disaster Recovery Plan 115
Business Continuity and Disaster Recovery Process 115
Business Impact Analysis 116
Incident Response Plan 118
Disaster Recovery Plan 119
Types of Disaster Recovery Plans 120
Emergency Preparedness Audit Checklist 121
Business Continuity Strategies 122
Business Resumption Plan Audit Checklist 123
Recovery Procedures Testing Checklist 126
## Contents

Plan Maintenance Checklist 126  
Vital Records Retention Checklist 127  
Forms and Documents 128  

**Chapter 8: Auditing in the E-Commerce Environment** 147  
- Introduction 147  
- Objectives of an Information Systems Audit in the E-Commerce Environment 148  
- General Overview 149  
- Auditing E-Commerce Functions 150  
- E-Commerce Policies and Procedures Review 155  
- Impact of E-Commerce on Internal Control 155  

**Chapter 9: Security Testing** 159  
- Cybersecurity 159  
- Cybercrimes 160  
- What Is Vulnerable to Attack? 162  
- How Cyberattacks Occur 162  
- What Is Vulnerability Analysis? 165  
- Cyberforensics 168  
- Digital Evidence 170  

**Chapter 10: Case Study: Conducting an Information Systems Audit** 173  
- Important Security Issues in Banks 174  
- Implementing an Information Systems Audit at a Bank Branch 180  
- Special Considerations in a Core Banking System 185  

**PART TWO: INFORMATION SYSTEMS AUDITING CHECKLISTS** 197  

**Chapter 11: ISecGrade Auditing Framework** 199  
- Introduction 199  
- Licensing and Limitations 200  
- Methodology 200  
- Domains 200  
- Grading Structure 202  
- Selection of Checklist 203  
- Format of Audit Report 206  
- Using the Audit Report Format 207  

**Chapter 12: ISecGrade Checklists** 209  
- Checklist Structure 209  
- Information Systems Audit Checklists 210  

**Chapter 13: Session Quiz** 281  
- Chapter 1: Overview of Systems Audit 281  
- Chapter 2: Hardware Security Issues 284