Table of Contents

About This Manual 17
Overview 17
Format of This Manual 17
Evaluation of This Manual 18
About the CISA Review Questions, Answers and Explanations Manual 18
CISA Online Review Course 18

Chapter 1:
The Process of Auditing Information Systems 19

Section One: Overview 20
Definition 20
Objectives 20
Task and Knowledge Statements 20
Tasks 20
Knowledge Statements 20
Suggested Resources for Further Study 28
Self-assessment Questions 29
Answers to Self-assessment Questions 30

Section Two: Content 32
1.1 Quick Reference 32
1.2 Management of the IS Audit Function 32
1.2.1 Organization of the IS Audit Function 32
1.2.2 IS Audit Resource Management 33
1.2.3 Audit Planning 33
Annual Planning 33
Individual Audit Assignments 33
1.2.4 Effect of Laws and Regulations on IS Audit Planning 34
1.3 ISACA IS Audit and Assurance Standards and Guidelines 35
1.3.1 ISACA Code of Professional Ethics 35
1.3.2 ISACA IS Audit and Assurance Standards 35
General 36
Performance 36
Reporting 37
1.3.3 ISACA IS Audit and Assurance Guidelines 37
General 38
Performance 39
Reporting 40
1.3.4 ISACA IS Audit and Assurance Tools and Techniques 40
1.3.5 Relationship Among Standards, Guidelines, and Tools and Techniques 40
1.3.6 ITAF™ 40
1.4 IS Controls 41
1.4.1 Risk Analysis 41
1.4.2 Internal Controls 42
1.4.3 IS Control Objectives 43
1.4.4 COBIT 5 44
1.4.5 General Controls 45
1.4.6 IS Specific Controls 45
1.5 Performing An IS Audit 45
1.5.1 Audit Objectives 46
1.5.2 Types of Audits 46
1.5.3 Audit Methodology 47

1.5.4 Risk-based Auditing 48
1.5.5 Audit Risk and Materiality 48
1.5.6 Risk Assessment and Treatment 49
Assessing Risk 49
Treating Risk 49
1.5.7 IS Audit Risk Assessment Techniques 50
1.5.8 Audit Programs 50
1.5.9 Fraud Detection 50
1.5.10 Compliance Versus Substantive Testing 51
1.5.11 Evidence 51
1.5.12 Interviewing and Observing Personnel in Performance of Their Duties 53
1.5.13 Sampling 54
1.5.14 Using the Services of Other Auditors and Experts 55
1.5.15 Computer-assisted Audit Techniques 56
CAATS as a Continuous Online Audit Approach 57
1.5.16 Evaluation of the Control Enviornment 57
Judging the Materiality of Findings 57
1.6 Communicating Audit Results 57
1.6.1 Audit Report Structure and Contents 58
1.6.2 Audit Documentation 59
1.6.3 Closing Findings 59
1.7 Control Self-assessment 60
1.7.1 Objectives of CSA 61
1.7.2 Benefits of CSA 61
1.7.3 Disadvantages of CSA 61
1.7.4 Auditor Role in CSA 61
1.7.5 Technology Drivers for CSA 61
1.7.6 Traditional Versus CSA Approach 61
1.8 The Evolving IS Audit Process 62
1.8.1 Integrated Auditing 62
1.8.2 Continuous Auditing 62
1.9 Case Studies 64
1.9.1 Case Study A 64
1.9.2 Case Study B 65
1.9.3 Case Study C 65
1.10 Answers to Case Study Questions 65
Answers to Case Study A Questions 65
Answers to Case Study B Questions 66
Answers to Case Study C Questions 66

Chapter 2:
Governance and Management of IT 67

Section One: Overview 68
Definition 68
Objectives 68
Task and Knowledge Statements 68
Tasks 68
Knowledge Statements 68
Suggested Resources for Further Study 80
Self-assessment Questions 81
Answers to Self-assessment Questions 82

Section Two: Content 84
2.1 Quick Reference 84
2.2 Corporate Governance 85
2.3 Governance of Enterprise IT 85
2.3.1 Good Practices for Governance of Enterpise IT 86
Governance of Enterprise IT and Management Frameworks 86
Audit Role in Governance of Enterprise IT 87
2.3.2 IT Governing Committees 88
2.3.3 IT Balanced Scorecard 88
2.3.4 Information Security Governance 89
Effective Information Security Governance 90
Roles and Responsibilities of Senior Management and Boards of Directors 91
Matrix of Outcomes and Responsibilities 91
2.3.5 Enterprise Architecture 92
2.4 Information Systems Strategy 93
2.4.1 Strategic Planning 93
2.4.2 IT Steering Committee 94
2.5 Maturity and Process Improvement Models 94
2.6 IT Investment and Allocation Practices 95
2.6.1 Value of IT 95
2.6.2 Implementing IT Portfolio Management 95
2.6.3 IT Portfolio Management Versus Balanced Scorecard 95
2.7 Policies and Procedures 95
2.7.1 Policies 96
Information Security Policy 96
2.7.2 Procedures 98
2.8 Risk Management 98
2.8.1 Developing a Risk Management Program 98
2.8.2 Risk Management Process 98
Step 1: Asset Identification 98
Step 2: Evaluation of Threats and Vulnerabilities to Assets 99
Step 3: Evaluation of the Impact 99
Step 4: Calculation of Risk 99
Step 5: Evaluation of and Response to Risk 99
2.8.3 Risk Analysis Methods 100
Qualitative Analysis Methods 100
Semiquantitative Analysis Methods 100
Quantitative Analysis Methods 100
2.9 Information Technology Management Practices 100
2.9.1 Human Resource Management 100
Hiring 100
Employee Handbook 101
Promotion Policies 101
Training 101
Scheduling and Time Reporting 101
Employee Performance Evaluations 101
Required Vacations 101
Termination Policies 101
2.9.2 Sourcing Practices 102
Outsourcing Practices and Strategies 102
Industry Standards/Benchmarking 104
Globalization Practices and Strategies 104
Cloud Computing 104
Outsourcing and Third-party Audit Reports 104
Governance in Outsourcing 106

Capacity and Growth Planning 107
Third-party Service Delivery Management 107
Service Improvement and User Satisfaction 108
2.9.3 Organizational Change Management 108
2.9.4 Financial Management Practices 109
IS Budgets 109
Software Development 109
2.9.5 Quality Management 109
2.9.6 Information Security Management 110
2.9.7 Performance Optimization 110
Critical Success Factors 110
Methodologies and Tools 110
Tools and Techniques 111
2.10 IT Organizational Structure and Responsibilities 111
2.10.1 IT Roles and Responsibilities 111
Vendor and Outsourcer Management 112
Infrastructure Operations and Maintenance 113
Media Management 113
Data Entry 113
Supervisory Control and Data Acquisition 113
Systems Administration 113
Security Administration 113
Quality Assurance 114
Database Administration 114
Systems Analyst 114
Security Architect 114
System Security Engineer 114
Applications Development and Maintenance 115
Infrastructure Development and Maintenance 115
Network Management 115
2.10.2 Segregation of Duties Within IT 115
2.10.3 Segregation of Duties Controls 116
Transaction Authorization 116
Custody of Assets 116
Access to Data 116
Compensating Controls for Lack of Segregation of Duties 117
2.11 Auditing IT Governance Structure and Implementation 117
2.11.1 Reviewing Documentation 117
2.11.2 Reviewing Contractual Commitments 118
2.12 Business Continuity Planning 118
2.12.1 IT Business Continuity Planning 119
2.12.2 Disasters and Other Disruptive Events 120
Pandemic Planning 120
Dealing With Damage to Image, Reputation or Brand 120
Unanticipated/Unforeseeable Events 121
2.12.3 Business Continuity Planning Process 121
2.12.4 Business Continuity Policy 121
2.12.5 Business Continuity Planning Incident Management 122
2.12.6 Business Impact Analysis 123
Classification of Operations and Criticality Analysis 125
2.12.7 Development of Business Continuity Plans 125
2.12.8 Other Issues in Plan Development 126
2.12.9 Components of a Business Continuity Plan 126
Key Decision-making Personnel 127
Backup of Required Supplies 127
Insurance 127

2.12.10 Plan Testing 128
Specifications 128
Test Execution 128
Documentation of Results 129
Results Analysis 129
Plan Maintenance 129
Business Continuity Management Good Practices 129
2.12.11 Summary of Business Continuity 130
2.13 Auditing Business Continuity 130
2.13.1 Reviewing the Business Continuity Plan 130
Review the Document 130
Review the Applications Covered by the Plan 130
Review the Business Continuity Teams 130
Plan Testing 131
2.13.2 Evaluation of Prior Test Results 131
2.13.3 Evaluation of Offsite Storage 131
2.13.4 Interviewing Key Personnel 131
2.13.5 Evaluation of Security at Offsite Facility 131
2.13.6 Reviewing Alternative Processing Contract 132
2.13.7 Reviewing Insurance Coverage 132
2.14 Case Studies 132
2.14.1 Case Study A 132
2.14.2 Case Study B 132
2.14.3 Case Study C 133
2.14.4 Case Study D 133
2.14.5 Case Study E 134
2.15 Answers to Case Study Questions 134
Answers to Case Study A Questions 134
Answers to Case Study B Questions 134
Answers to Case Study C Questions 135
Answers to Case Study D Questions 135
Answers to Case Study E Questions 135

Chapter 3:
Information Systems Acquisition, Development and Implementation 137

Section One: Overview 138
Definition 138
Objectives 138
Task and Knowledge Statements 138
Tasks 138
Knowledge Statements 138
Suggested Resources for Further Study 147
Self-assessment Questions 148
Answers to Self-assessment Questions 149

Section Two: Content 151
3.1 Quick Reference 151
3.2 Benefits Realization 151
3.2.1 Portfolio/Program Management 152
3.2.2 Business Case Development and Approval 153
3.2.3 Benefits Realization Techniques 154

3.3 Project Management Structure 155
3.3.1 General Aspects 155
3.3.2 Project Context and Environment 155
3.3.3 Project Organizational Forms 155
3.3.4 Project Communication and Culture 156
3.3.5 Project Objectives 156
3.3.6 Roles and Responsibilities of Groups and Individuals 158
3.4 Project Management Practices 159
3.4.1 Initiation of a Project 160
3.4.2 Project Planning 160
System Development Project Cost Estimation 160
Software Size Estimation 161
Function Point Analysis 161
FPA Feature Points 161
Cost Budgets 161
Software Cost Estimation 162
Scheduling and Establishing the Time Frame 162
Critical Path Methodology 162
Gantt Charts 162
Program Evaluation Review Technique 163
Timebox Management 164
3.4.3 Project Execution 164
3.4.4 Project Controlling 164
Management of Scope Changes 164
Management of Resource Usage 164
Management of Risk 164
3.4.5 Closing a Project 165
3.5 Business Application Development 165
3.5.1 Traditional SDLC Approach 166
3.5.2 Description Of Traditional SDLC Phases 168
Phase 1—Feasibility Study 168
Phase 2—Requirements Definition 168
Phase 3A—Software Selection and Acquisition 169
Phase 3B—Design 171
Phase 4A—Configuration 173
Phase 4B—Development 173
Phase 5—Final Testing and Implementation 176
Phase 6—Postimplementation Review 182
3.5.3 Integrated Resource Management Systems 182
3.5.4 Risk Associated With Software Development 182
3.6 Virtualization and Cloud Computing Environments 183
3.6.1 Virtualization 183
Key Risk Areas 184
Typical Controls 184
3.7 Business Application Systems 185
3.7.1 E-Commerce 185
E-Commerce Models 185
3.7.2 Electronic Data Interchange 188
General Requirements 188
Traditional EDI 188
Web-Based EDI 189
3.7.3 EDI Risk and Controls 189

3.7.4 Controls in The EDI Environment 189
Receipt of Inbound Transactions 190
Outbound Transactions 190
Auditing EDI 191
3.7.5 Email 191
Security Issues of Email 192
Standards for Email Security 192
3.7.6 Point-of-sale Systems 193
3.7.7 Electronic Banking 193
Risk Management Challenges in E-banking 193
Risk Management Controls for E-banking 193
3.7.8 Electronic Finance 194
3.7.9 Payment Systems 194
Electronic Money Model 194
Electronic Checks Model 194
Electronic Transfer Model 194
3.7.10 Integrated Manufacturing Systems 194
3.7.11 Electronic Funds Transfer 195
Controls in an EFT Environment 195
3.7.12 Automated Teller Machine 195
Audit of ATMs 196
3.7.13 Interactive Voice Response 196
3.7.14 Purchase Accounting System 196
3.7.15 Image Processing 196
3.7.16 Industrial Control Systems 197
Risk Factors 197
Typical Controls 198
3.7.17 Artificial Intelligence and Expert Systems 198
3.7.18 Business Intelligence 199
Business Intelligence Governance 201
3.7.19 Decision Support System 202
Efficiency vs. Effectiveness 202
Decision Focus 202
DSS Frameworks 202
Design and Development 202
Implementation and Use 202
Risk Factors 203
Implementation Strategies 203
Assessment and Evaluation 203
DSS Common Characteristics 203
DSS Trends 203
3.7.20 Customer Relationship Management 203
3.7.21 Supply Chain Management 204
3.8 Development Methods 204
3.8.1 Use of Structured Analysis, Design and Development Techniques 204
3.8.2 Agile Development 204
3.8.3 Prototyping-evolutionary Development 205
3.8.4 Rapid Application Development 206
3.8.5 Object-oriented System Development 206
3.8.6 Component-based Development 207
3.8.7 Web-based Application Development 208
3.8.8 Software Reengineering 208
3.8.9 Reverse Engineering 209

4.2.5 Incident and Problem Management 259
Process of Incident Handling 259
Problem Management 259
Detection, Documentation, Control, Resolution and Reporting of Abnormal Conditions 259
4.2.6 Support/Help Desk 260
4.2.7 Change Management Process 260
Patch Management 261
4.2.8 Release Management 261
4.2.9 Quality Assurance 262
4.3 IT Asset Management 262
4.4 Information Systems Hardware 262
4.4.1 Computer Hardware Components and Architectures 262
Processing Components 262
Input/Output Components 262
Types of Computers 263
Common Enterprise Back-end Devices 263
Universal Serial Bus 264
Memory Cards/Flash Drives 264
Radio Frequency Identification 265
4.4.2 Hardware Maintenance Program 266
4.4.3 Hardware Monitoring Procedures 266
4.4.4 Capacity Management 266
4.5 IS Architecture and Software 267
4.5.1 Operating Systems 268
Software Control Features or Parameters 268
Software Integrity Issues 268
Activity Logging and Reporting Options 269
4.5.2 Access Control Software 269
4.5.3 Data Communications Software 269
4.5.4 Data Management 270
Data Quality 270
Data Life Cycle 270
4.5.5 Database Management System 270
DBMS Architecture 272
Detailed DBMS Metadata Architecture 272
Data Dictionary/Directory System 272
Database Structure 272
Database Controls 274
4.5.6 Utility Programs 275
4.5.7 Software Licensing Issues 275
4.5.8 Source Code Management 276
4.5.9 End-user Computing 276
4.6 IS Network Infrastructure 276
4.6.1 Enterprise Network Architectures 277
4.6.2 Types of Networks 277
4.6.3 Network Services 278
4.6.4 Network Standards and Protocols 278
4.6.5 OSI Architecture 278
4.6.6 Application of the OSI Model In Network Architectures 280
Local Area Network 280
Wide Area Network 284
Wireless Networks 287
Public "Global" Internet Infrastructure 289

Network Administration and Control ... 292
Applications in a Networked Environment ... 293
On-demand Computing ... 295
4.7 Auditing Infrastructure and Operations ... 295
4.7.1 Enterprise Architecture and Auditing ... 295
4.7.2 Hardware Reviews ... 295
4.7.3 Operating System Reviews ... 295
4.7.4 Database Reviews ... 295
4.7.5 Network Infrastructure and Implementation Reviews ... 295
4.7.6 IS Operations Reviews ... 300
4.7.7 Scheduling Reviews ... 301
4.7.8 Problem Management Reporting Reviews ... 302
4.8 Disaster Recovery Planning ... 302
4.8.1 Recovery Point Objective and Recovery Time Objective ... 303
4.8.2 Recovery Strategies ... 304
4.8.3 Recovery Alternatives ... 304
Contractual Provisions ... 305
Procuring Alternative Hardware ... 305
Application Resiliency and Disaster Recovery Methods ... 306
Data Storage Resiliency and Disaster Recovery Methods ... 306
Telecommunication Networks Resiliency and Disaster Recovery Methods ... 306
4.8.4 Development of Disaster Recovery Plans ... 307
IT DRP Contents ... 307
IT DRP Scenarios ... 308
Recovery Procedures ... 308
4.8.5 Organization and Assignment of Responsibilities ... 308
4.8.6 Backup and Restoration ... 309
Offsite Library Controls ... 309
Security and Control of Offsite Facilities ... 310
Media and Documentation Backup ... 310
Types of Backup Devices and Media ... 310
Periodic Backup Procedures ... 311
Frequency of Rotation ... 311
Types of Media and Documentation Rotated ... 311
Backup Schemes ... 312
Method of Rotation ... 312
Record Keeping for Offsite Storage ... 313
4.8.7 Disaster Recovery Testing Methods ... 313
Types of Tests ... 313
Testing ... 314
Test Results ... 315
4.8.8 Invoking Disaster Recovery Plans ... 315
4.9 Case Studies ... 315
4.9.1 Case Study A ... 315
4.9.2 Case Study B ... 316
4.10 Answers to Case Study Questions ... 316
Answers to Case Study A Questions ... 316
Answers to Case Study B Questions ... 316

Chapter 5:
Protection of Information Assets 317

Section One: Overview 318
Definition 318
Objectives 318
Task and Knowledge Statements 318
Tasks 318
Knowledge Statements 318
Suggested Resources for Further Study 331
Self-assessment Questions 332
Answers to Self-assessment Questions 333

Section Two: Content 335
5.1 Quick Reference 335
5.2 Information Security Management 335
5.2.1 Key Elements of Information Security Management 336
Information Security Management System 336
5.2.2 Information Security Management Roles and Responsibilities 337
5.2.3 Classification of Information Assets 337
5.2.4 Fraud Risk Factors 338
5.2.5 Information Security Control Design 338
Managerial, Technical and Physical Controls 339
Control Standards and Frameworks 339
Control Monitoring and Effectiveness 339
5.2.6 System Access Permission 339
5.2.7 Mandatory and Discretionary Access Controls 340
5.2.8 Privacy Principles and the Role of IS Auditors 340
5.2.9 Critical Success Factors to Information Security Management 341
Security Awareness, Training and Education 341
5.2.10 Information Security and External Parties 342
Identification of Risk Related to External Parties 342
Addressing Security When Dealing With Customers 343
Addressing Security in Third-party Agreements 343
5.2.11 Human Resources Security and Third Parties 345
Screening 345
Terms and Conditions of Employment 345
During Employment 345
Termination or Change of Employment 345
Removal of Access Rights 346
5.2.12 Computer Crime Issues and Exposures 346
5.2.13 Security Incident Handling and Response 352
5.3 Logical Access 352
5.3.1 Logical Access Exposures 352
5.3.2 Familiarization With the Enterprise's IT Environment 353
5.3.3 Paths of Logical Access 353
General Points of Entry 353
5.3.4 Logical Access Control Software 353
5.3.5 Identification and Authentication 354
Logon IDS and Passwords 355
Token Devices, One-time Passwords 356
Biometrics 356
Single Sign-on 358

5.3.6 Authorization Issues 359
Access Control Lists 359
Logical Access Security Administration 359
Remote Access Security 359
Audit Logging in Monitoring System Access 360
Naming Conventions for Logical Access Controls 362
5.3.7 Storing, Retrieving, Transporting and Disposing of Confidential Information 362
Preserving Information During Shipment or Storage 363
Media-Specific Storage Precautions 363
5.4 Network Infrastructure Security 363
5.4.1 LAN Security 363
Virtualization 364
5.4.2 Client-server Security 365
5.4.3 Wireless Security Threats and Risk Mitigation 365
5.4.4 Internet Threats and Security 366
Network Security Threats 366
Passive Attacks 366
Active Attacks 366
Causal Factors for Internet Attacks 367
Internet Security Controls 367
Firewall Security Systems 367
Firewall General Features 368
Firewall Types 368
Examples of Firewall Implementations 369
Firewall Issues 370
Firewall Platforms 370
Intrusion Detection Systems 370
Intrusion Prevention Systems 371
Honeypots and Honeynets 371
5.4.5 Encryption 371
Key Elements of Encryption Systems 372
Symmetric Key Cryptographic Systems 372
Public (Asymmetric) Key Cryptographic Systems 374
Quantum Cryptography 374
Digital Signatures 374
Public Key Infrastructure 375
Applications of Cryptographic Systems 376
5.4.6 Malware 377
Virus and Worm Controls 377
Management Procedural Controls 377
Technical Controls 378
Anti-malware Software Implementation Strategies 378
5.4.7 Voice-over IP 379
VoIP Security Issues 379
5.4.8 Private Branch Exchange 380
PBX Risk 380
PBX Audit 381
PBX System Features 381
PBX System Attacks 381
Hardware Wiretapping 382
Hardware Conferencing 382
Remote Access 383
Maintenance 383
Special Manufacturer's Features 383

Manufacturer's Development and Test Features 383
Software Loading and Update Tampering 384
Crash-restart Attacks 384
Passwords 384
5.5 Auditing Information Security Management Framework 384
5.5.1 Auditing Information Security Management Framework 384
Reviewing Written Policies, Procedures and Standards 384
Logical Access Security Policies 384
Formal Security Awareness and Training 384
Data Ownership 385
Data Owners 385
Data Custodians 385
Security Administrator 385
New IT Users 385
Data Users 385
Documented Authorizations 385
Terminated Employee Access 385
Security Baselines 386
Access Standards 386
5.5.2 Auditing Logical Access 386
Familiarization With the IT Environment 388
Assessing and Documenting the Access Paths 388
Interviewing Systems Personnel 389
Reviewing Reports From Access Control Software 389
Reviewing Application Systems Operations Manual 389
5.5.3 Techniques for Testing Security 389
Terminal Cards and Keys 389
Terminal Identification 389
Logon IDs and Passwords 389
Controls Over Production Resources 390
Logging and Reporting of Computer Access Violations 390
Follow-up Access Violations 390
Bypassing Security and Compensating Controls 390
Review Access Controls and Password Administration 390
5.5.4 Investigation Techniques 391
Investigation of Computer Crime 391
Computer Forensics 391
Protection of Evidence and Chain of Custody 392
5.6 Auditing Network Infrastructure Security 392
5.6.1 Auditing Remote Access 393
Auditing Internet Points of Presence 393
Network Penetration Tests 393
Full Network Assessment Reviews 396
Development and Authorization of Network Changes 396
Unauthorized Changes 396
5.7 Environmental Exposures and Controls 397
5.7.1 Environmental Issues and Exposures 397
5.7.2 Controls for Environmental Exposures 397
Alarm Control Panels 397
Water Detectors 397
Handheld Fire Extinguishers 397
Manual Fire Alarms 397
Smoke Detectors 397
Fire Suppression Systems 398
Strategically Locating the Computer Room 398

Regular Inspection by Fire Department ... 399
Fireproof Walls, Floors and Ceilings of the Computer Room ... 399
Electrical Surge Protectors ... 399
Uninterruptible Power Supply/Generator ... 399
Emergency Power-off Switch ... 399
Power Leads From Two Substations ... 399
Fully Documented and Tested Business Continuity Plan ... 399
Wiring Placed in Electrical Panels and Conduit ... 399
Inhibited Activities Within the Information Processing Facility ... 399
Fire-resistant Office Materials ... 399
Documented and Tested Emergency Evacuation Plans ... 399
5.7.3 Auditing Environmental Controls ... 399
Water and Smoke Detectors ... 399
Handheld Fire Extinguishers ... 399
Fire Suppression Systems ... 400
Regular Inspection by Fire Department ... 400
Fireproof Walls, Floors and Ceilings of the Computer Room ... 400
Electrical Surge Protectors ... 400
Power Leads From Two Substations ... 400
Fully Documented and Tested Business Continuity Plan ... 400
Wiring Placed in Electrical Panels and Conduit ... 400
UPS/Generator ... 400
Documented and Tested Emergency Evacuation Plans ... 400
Humidity/Temperature Control ... 400
5.8 Physical Access Exposures and Controls ... 400
5.8.1 Physical Access Issues and Exposures ... 400
Physical Access Exposures ... 400
Possible Perpetrators ... 400
5.8.2 Physical Access Controls ... 401
5.8.3 Auditing Physical Access ... 402
5.9 Mobile Computing ... 402
5.10 Peer-to-peer Computing ... 404
5.11 Instant Messaging ... 405
5.12 Social Media ... 405
5.13 Cloud Computing ... 407
5.14 Data Leakage ... 410
5.14.1 Data Leak Prevention ... 410
Data at Rest ... 410
Data in Motion (Network) ... 410
Data in Use (Endpoint) ... 410
Policy Creation and Management ... 410
Directory Services Integration ... 410
Workflow Management ... 410
Backup and Restore ... 410
Reporting ... 410
5.14.2 DLP Risk, Limitations and Considerations ... 411
5.15 End-user Computing Security Risk and Controls ... 411
5.16 Case Studies ... 412
5.16.1 Case Study A ... 412
5.16.2 Case Study B ... 412
5.16.3 Case Study C ... 413
5.16.4 Case Study D ... 413

5.17 Answers to Case Study Questions 414
Answers to Case Study A Questions 414
Answers to Case Study B Questions 414
Answers to Case Study C Questions 415
Answers to Case Study D Questions 415

APPENDIX A: IS AUDIT AND ASSURANCE STANDARDS, GUIDELINES AND TOOLS AND TECHNIQUES 417
Relationship of Standards to Guidelines and Tools and Techniques 417
Use 417

APPENDIX B: CISA EXAM GENERAL INFORMATION 419
Requirements for Certification 419
Successful Completion of the CISA Exam 419
Experience in IS Auditing, Control and Security 419
Description of the Exam 419
Registration for the CISA Exam 419
CISA Program Accreditation Renewed Under ISO/IEC 17024:2012 419
Preparing for the CISA Exam 420
Types of Exam Questions 420
Administration of the Exam 420
Sitting for the Exam 420
Budgeting Your Time 421
Rules and Procedures 421
Grading the Exam 421

Glossary 423

Acronyms 447

Index 453