Table of Contents

Domain 1: Governance 2

Knowledge Assumptions 3

1. Drivers that Influence Governance 4

1.1 Business Drivers 4

1.1.1 Form of Business Organization 4

1.1.2 Organizational Structure 5

1.1.3 Industry 7

1.1.4 Organizational Maturity 7

1.2 Information Security Drivers 8

1.2.1 Corporate Governance and Organizational Alignment 9

1.2.2 Compliance 9

1.2.3 Information Privacy 22

2. Corporate Governance Activities 24

2.1 Risk Oversight 25

2.2 Enterprise Architecture 26

2.2.1 The Zachman Framework 27

2.2.2 The Open Group Architecture Framework (TOGAF) 28

2.2.3 Sherwood Applied Business Security Architecture (SABSA) 30

2.2.4 Federal Enterprise Architecture Framework (FEAF) 32

2.2.5 Department of Defense Architecture Framework (DoDAF) 34

2.3 Asset Management 36

2.3.1 Asset Ownership 37

2.3.2 Classification 37

2.3.3 Asset Inventory 39

2.3.4 Asset Value 40

2.3.5 Asset Protection 41

2.3.6 Asset Management in Practice 41

2.4 Managing and Controlling Organizational Changes 42

2.4.1 Change Control 44

2.4.2 Change Management 44

2.5 Business Continuity Management 52

2.5.1 Business Impact Analysis 52

2.5.2 Business Continuity Planning 53

2.5.3 Disaster Recovery Planning 54

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2.5.4 Alternate Processing Sites 54
2.5.5 BCM Plan Testing 56
2.5.7 Crisis Management 58
3. Information Security Governance Activities 59
4.1 Information Security Program Management 60
4.1.1 Formal Documentation 60
4.1.2 Education, Training, and Awareness 65
4.1.3 Information Security Steering Committee 65
4.1.4 Metrics and Reporting 66
4.2 Security Engineering 68
4.3 Security Operations 69
4.4 Corporate Governance and Security Responsibilities 70
4. Governance and Ethical Decision Making 77
5.1 EC-Council Code of Ethics 77
Domain 1 Summary 80

Domain 2: Security Risk Management, Controls, and Audit Management 81

Knowledge Assumptions 83
1. Risk Management 84
1.1 Risk Assessment 86
1.2 Risk Analysis Approaches 87
1.3 Organizational Risk Perspectives 88
1.4 Risk Management Constraints 90
2. Risk Treatment 91
2.1 Risk Treatment Options 91
2.2 Attributes of Controls 93
2.3 Selecting and Implementing Controls 95
2.4 Control Catalogs 96
3. Risk Management Frameworks 98
3.1 ISO 27005 98
3.2 NIST Risk Management Framework 104
3.2.1 NIST Risk Management and Assessment 106
3.3 Additional Risk Management Tools 108
3.3.1 ISO 31000 108
3.3.2 Threat Agent Risk Assessment (TARA) 109

All Rights Reserved. Reproduction is Strictly Prohibited.

3.3.3 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro110
3.3.4 Factor Analysis of Information Risk (FAIR) 111
3.3.5 COBIT Risk Management 111
3.3.6 ITIL Risk Management 112
4. Audit Management 112
4.1 Evaluation Standards and Controls 113
4.2 Analysis and Interpretation of Audit Results 116
4.3 Outcomes for Ineffective or Missing Controls 116
5. Risk Communication and Organizational Reporting 116
Domain 2 Summary 118

Domain 3: Security Program Management and Operations 119
Knowledge Assumptions 121
1. Information Security Portfolio Management 122
1.1 Information Security Portfolio Planning 123
1.2 Information Security Portfolio Alignment 125
2. Information Security Program Management 127
2.1 Information Security Program Development Model 127
3. Information Security Project Management 132
3.1 Project Initiation 133
3.2 Intermediate Project Phases 135
3.3 Project Closure 140
4. Security Operations 141
4.1 Security Operations Center (SOC) 142
4.1.1 Security Operations Personnel 142
4.1.2 Security Operations Processes: Policies and Procedures 143
4.1.3 Security Operations Technology 145
4.1.4 Security Operations Communication 146
4.2 Security Operations Program Activities 147
4.2.1 Event Management and Incident Response 148
4.2.2 Digital Forensic Investigation 153
4.2.3 Threat Hunting 156
Domain 3 Summary 158

All Rights Reserved. Reproduction is Strictly Prohibited.

Domain 4: Information Security Core Competencies 159
Knowledge Assumptions 161
1. Access Control 162
1.1. Access Control Plan 162
1.2. Types of Access Control 162
1.3. Authentication 164
1.4. Authorization 166
1.5. Access Administration 167
2. Physical Security 169
2.1. Physical Risk Analysis 169
2.2. Physical Security Audits 169
2.3. Physical Security Strategy 170
2.4. Facility Design 171
3. Network and Communications Security 173
3.1. Network Security Planning 173
3.2. Network Management Concerns 173
3.3. Network Topologies 174
3.4. Network Standards and Protocols 176
3.5. Network Security Controls 177
3.6. Wireless Communications Security 180
3.7. Voice-over-IP (VoIP) Security 181
4. Threat and Vulnerability Management 182
4.1. Threat Management 182
4.2. Vulnerability Management 183
5. System and Application Security 187
5.1. System Development 187
5.2. Separation of production, development, and test environments 189
5.3. Application Testing 189
5.4. System Security Management 190
5.5. Configuration management 190
5.6. System Hardening 191
5.7. Data Sanitization 192
5.8. Mobile System Security 193
6. Encryption Concepts and Technology 193
6.1. Encryption Algorithms 193
6.2. Public Key Infrastructure 194

Certified Chief Information Security Officer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6.3. Hashing....194
6.4. Digital Signatures....195
Domain 4 Summary....196

Domain 5: Strategic Planning, Financial Management, and Vendor Management 197

Knowledge Assumptions....199
1. Strategic Planning....200
1.1. Strategic Planning Phases....201
1.2. Strategic Planning Tools....203
2. Financial Management....205
2.1. Fundamental Accounting Concepts....206
2.2. Budgeting....207
2.3. Expense Management....207
2.4. Comparing Capital Investment Opportunities....209
2.5. Financial Accounting for Security Leaders....212
3. Vendor Risk Management....213
3.1. Procurement....213
3.1.1 Planning....213
3.1.2 Vendor assessment and selection....214
3.1.3 Contract negotiation....215
3.1.4 Managing Expectations and Performance....216
3.2. Vendor Management....217
3.2.1 Oversight....217
3.2.2 Risk Management....217
3.2.3 Disposition....217
Domain 5 Summary....220
References....221
Index....229

All Rights Reserved. Reproduction is Strictly Prohibited.