

Certified Chief Information Security Officer

Table of Contents

Table of Contents

Domain 1: Governance (Policy, Legal & Compliance)

- Introduction..... 3**
- 1. Definitions 3**
 - 1.1. Governance.....3
 - 1.2. Compliance3
 - 1.3. Privacy.....4
 - 1.4. Risk Management.....4
- 2. Information Security Management Program 4**
 - 2.1. Security Policy.....5
 - 2.1.1. Necessity of a Security Policy6
 - 2.1.2. Security Policy Challenges6
 - 2.1.3. Policy Content.....7
 - 2.1.4. Types of Policies.....8
 - 2.1.5. Policy Implementation.....9
 - 2.2. Security Roles & Responsibilities.....10
 - 2.2.1. Reporting Structure11
 - 2.3. Security Standards, Guidelines & Frameworks.....12
 - 2.3.1. ISO 27000.....13
 - 2.3.2. ISO 27001.....13
 - 2.3.3. ISO 27002.....14
 - 2.3.4. ISO 27003.....15
 - 2.3.5. ISO 27004.....16
 - 2.3.6. ISO 15408 Evaluation Common Criteria Evaluation for Security.....17
 - 2.3.7. ISO/IEC 13335 (IT Security Management).....17
 - 2.3.8. NIST Special Publications.....18
 - 2.3.9. ISO Standard 24762 for Technical Disaster Recovery18
 - 2.3.10. ISO Standard for BCM.....19
 - 2.3.11. COBIT19
 - 2.3.12. ITIL20
 - 2.3.13. Other Examples of Standards, Guidelines, and Frameworks21
 - 2.4. Risk Management.....22

- 2.4.1. The Need for Risk Management.....22
- 2.4.2. Where Do Risks Come From.....23
- 2.4.3. Risk Identification23
- 2.4.4. Risk Analysis / Assessment24
 - 2.4.4.1. Quantitative Risk Analysis24
 - 2.4.4.2. Qualitative Risk Analysis.....25
- 2.4.5. Risk Agility.....26
- 2.4.6. Risk Treatment.....27
- 2.4.7. Risk Monitoring & Review.....27
- 2.4.8. Risk Management Guidelines and Practices28
- 2.5. Technical Security Architecture29
- 2.6. Asset Classification & Management.....31
 - 2.6.1. Asset Inventory.....33
 - 2.6.2. Information Classification.....33
 - 2.6.3. Asset Responsibility/Ownership34
 - 2.6.4. Asset Value34
 - 2.6.5. Asset Protection.....34
- 2.7. Security Management & Operations34
 - 2.7.1. Security Administration36
 - 2.7.2. Event Management36
 - 2.7.3. Security Event Management36
 - 2.7.4. Vulnerability & Threat Management37
 - 2.7.4.1. Threat Level Assignment.....37
 - 2.7.4.2. Threat & Vulnerability Remediation Activities38
 - 2.7.5. Security Incident Management39
 - 2.7.5.1. Objectives of Incident Management Framework40
 - 2.7.5.2. Definition.....40
 - 2.7.5.3. Security Incident Management Framework.....41
 - 2.7.5.4. Processes41
 - 2.7.5.4.1. Monitoring42
 - 2.7.5.4.1.1. Data Collection42
 - 2.7.5.4.1.2. Data Normalization.....42
 - 2.7.5.4.1.3. Data Correlation43

- 2.7.5.4.1.4. Data Identification.....43
- 2.7.5.4.2. Triage44
 - 2.7.5.4.2.1. Impact, Urgency, Priority - Impact level.....44
 - 2.7.5.4.2.2. Impact, Urgency, Priority - Urgency level.....45
 - 2.7.5.4.2.3. Impact, Urgency, Priority - Priority Level.....45
- 2.7.5.4.3. Detailed Analysis46
- 2.7.5.4.4. Incident Handling46
- 2.7.5.4.5. Compliance Management46
- 2.7.5.4.6. Reporting.....46
- 2.7.5.5. Return to Normal Operations.....46
- 2.7.5.6. Incident Response in Practice47
- 2.7.5.7. Steps / Tasks / Actions / Decisions48
- 2.8. Business Resilience.....49
 - 2.8.1. Business Continuity Management.....49
 - 2.8.2. Disaster Recovery.....53
 - 2.8.2.1. Performance Indicators for Disaster Recovery.....53
 - 2.8.2.2. Management Awareness54
 - 2.8.2.2.1. Identify Possible Disaster Scenarios.....54
 - 2.8.2.2.2. Build Management Awareness55
 - 2.8.2.2.3. Obtain Management Sign-Off and Funding55
 - 2.8.2.3. Disaster Recover Planning Process.....55
 - 2.8.2.3.1. Risk Assessment.....55
 - 2.8.2.3.2. Critical Application Analysis.....56
 - 2.8.2.3.3. Determine Recovery Window Requirements58
 - 2.8.2.3.4. Define Recovery Process58
 - 2.8.2.3.5. Develop Draft DR Plan59
 - 2.8.2.3.6. Establish Communications Plan, Teams, and Roles.....60
 - 2.8.2.3.7. Disaster Recovery Site Planning61
 - 2.8.2.3.8. Data & Application Access.....62
 - 2.8.2.3.9. Document the DR Plan in Detail62
 - 2.8.2.3.10. Exercise the DR Plan.....63
 - 2.8.2.3.11. Refine & Re-test DR Plan64

2.9. Training & Awareness64

 2.9.1. Behavior.....65

 2.9.2. Accountability65

 2.9.3. Comparative Framework.....66

 2.9.4. Awareness66

 2.9.5. Training.....67

 2.9.5.1. General Users67

 2.9.5.2. Specialized or Advanced Training.....68

 2.9.6. Education.....68

 2.9.7. Deployment.....68

 2.9.7.1. Identify Program Scope, Goals, and Objectives69

 2.9.7.2. Identify Training Staff.....70

 2.9.7.3. Identify Target Audiences70

 2.9.7.4. Buy In71

 2.9.7.5. Topics71

 2.9.7.6. Methods.....71

 2.9.7.7. Materials71

 2.9.7.8. Timing.....72

 2.9.7.9. Frequency.....72

 2.9.7.10. Communications72

 2.9.7.11. Updates.....72

 2.9.7.12. Evaluation Criteria72

 2.9.7.13. Funding73

 2.9.8. Top Reasons for Failure.....73

2.10. Security Metrics & Reporting75

 2.10.1. Objectives77

 2.10.2. What is a Security Metric?77

 2.10.3. Characteristics of Good Metrics.....78

 2.10.4. Types of Metrics78

 2.10.5. Using Security Metrics80

2.11. Information Security Governance81

2.12. Information Security Compliance85

3. Information Security Laws, Regulations & Guidelines	88
3.1. Broadly Applicable Laws and Regulations	89
3.1.1. Sarbanes-Oxley Act (aka Sarbox, SOX)	89
3.1.2. Payment Card Industry Data Security Standard (PCI DSS).....	90
3.1.3. The Gramm-Leach-Bliley Act (GLB) Act of 1999.....	91
3.2. Industry-Specific Regulations and Guidelines	91
3.2.1. Federal Information Security Management Act (FISMA).....	92
3.2.2. North American Electric Reliability Corp. (NERC) Standards.....	92
3.2.3. Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records	93
3.2.4. Health Insurance Portability and Accountability Act (HIPAA).....	93
3.2.5. The Health Information Technology for Economic and Clinical Health Act (HITECH)	95
3.3. Key State Regulations.....	95
3.3.1. Massachusetts 201 CMR 17 (aka Mass Data Protection Law)	95
3.3.2. Nevada Personal Information Data Privacy Encryption Law NRS 603A.....	96
3.4. International Laws	97
3.4.1. Personal Information Protection and Electronic Documents Act (PIPED Act, or PIPEDA)—Canada.....	97
3.4.2. Law on the Protection of Personal Data Held by Private Parties—Mexico	97
3.4.3. European Union Data Protection Directive	98
3.4.4. Safe Harbor Act.....	99
4. Privacy Laws	99
4.1. United States Privacy Laws.....	100
4.1.1. Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule.....	100
4.1.2. Children's Online Privacy Protection Act.....	101
4.2. Data Breach Disclosure Laws	103
4.3. Security Breach Notification Law Components.....	104
4.4. International Privacy Laws	105
4.4.1. Collection Limitation Principle	105
4.4.2. Data Quality Principle	105
4.4.3. Purpose Specification Principle.....	105
4.4.4. Use Limitation Principle.....	105
4.4.5. Security Safeguards Principle.....	105

4.4.6. Openness Principle 105
 4.4.7. Individual Participation Principle..... 106
 4.4.8. Accountability Principle 106

Domain 2 – IS Management Controls and Auditing Management (Projects, Technology, and Operations)

Introduction..... 111

1. Design, Deploy, and Manage Security Controls in Alignment with Business Goals, Risk Tolerance, and Policies and Standards 116

1.1. Information Security Risk Management 118
 1.2. Context Establishment..... 119

2. Information Security Risk Assessment 122

2.1. Risk Identification 124
 2.2. Risk Analysis 130
 2.3. Risk Evaluation..... 133

3. Risk Treatment..... 134

3.1. Risk Modification..... 136
 3.2. Risk Retention 140
 3.3. Risk Avoidance..... 140
 3.4. Risk Sharing 140

4. Residual Risk..... 141

5. Risk Acceptance 142

6. Risk Management Feedback Loops..... 143

6.1. Risk Communication and Consultation..... 143
 6.2. Risk Monitoring and Review 144
 6.2.1. Risk Monitoring..... 144
 6.2.2. Risk Management Program Review..... 146

7. Business Goals..... 146

7.1. COBIT 4.1 PO1.2 Business IT-Alignment..... 147
 7.2. COBIT 5.0 AP002 Manage Strategy 148

8. Risk Tolerance 150

9. Policies and Standards 152

10. Understanding Security Controls Types and Objectives: Management Controls, Technical Controls, Policy and Procedural Controls, Organization Controls, and more..... 154

- 10.1. Introduction 154
 - 10.1.1. Procedural Controls (Administrative Controls) 155
 - 10.1.2. Logical Controls (Technical Controls) 155
 - 10.1.3. Physical Controls 156
- 10.2. What the control does..... 156
 - 10.2.1. Preventive (or Preventative) Controls 156
 - 10.2.2. Detective Controls..... 156
 - 10.2.3. Corrective Controls 156
 - 10.2.4. Combination of Detective and Corrective Controls 157
 - 10.2.5. Deterrent Controls 157
- 10.3. How the control is performed..... 157
 - 10.3.1. Manual Controls..... 157
 - 10.3.2. Automated Controls..... 157
- 10.4. Reliance upon controls 158
 - 10.4.1. Key Controls 158
 - 10.4.2. Compensating Controls 158
- 10.5. Choosing controls 159
 - 10.5.1. Control Catalog..... 159
 - 10.5.2. Control Objective 160
 - 10.5.3. Control Implementation Guidance 160
- 10.6. Common Types of Controls 160
 - 10.6.1. Organization Controls 161
 - 10.6.1.1. Control..... 161
 - 10.6.1.2. Implementation guidance 161
 - 10.6.2. Operational Controls..... 161
 - 10.6.2.1. Control..... 162
 - 10.6.2.2. Implementation guidance 162
 - 10.6.3. Personnel Controls 162
 - 10.6.3.1. Control..... 162
 - 10.6.3.2. Implementation guidance 162

10.6.4. Access Controls 163

 10.6.4.1. Control..... 163

 10.6.4.2. Implementation guidance 163

10.6.5. Asset Management Controls 164

 10.6.5.1. Control..... 164

 10.6.5.2. Implementation guidance 164

10.7. Last bit on controls 164

11. Implement Control Assurance Frameworks to: Define Key Performance Metrics (KPIs), Measure and Monitor Control Effectiveness, and Automate Controls 165

12. COBIT (Control Objectives for Information and Related Technology)... 165

13. BAI06 Manage Changes..... 166

 13.1. Domain 166

 13.2. Process Description 166

 13.3. Process Purpose Statement 166

 13.4. Goals and Metrics..... 167

 13.5. RACI Chart 168

 13.6. Process Practices, Inputs/Outputs, and Activities 169

 13.6.1. BAI06.01 Evaluate, Prioritize, and Authorize change Requests..... 169

 13.6.2. BAI06.02 Manage Emergency Changes 170

 13.6.3. BAI06.03 Track and Report Change Status..... 170

 13.6.4. BAI06.04 Close and Document the Changes..... 171

14. COBIT 4.1 vs. COBIT 5..... 172

15. ISO 27001/27002..... 174

 15.1. Change Management..... 174

16. Automate Controls..... 176

17. Wrap-up 180

18. Understanding the Audit Management Process 180

 18.1. Let’s begin by defining what an audit is. 181

 18.2. Audit management standards and best practices (COBIT, etc.) 181

 18.2.1. So, where to start?..... 182

 18.2.1.1. ISO 27001/27002 182

 18.2.1.2. COBIT..... 184

18.3. Measure Effectiveness of the Audit Process against Business Goals and Risk Tolerance. 188

18.4. Analysis and Interpretation of Audit Reports 190

18.5. Formulation of Remediation Plans..... 191

18.6. Risk Assessment of Ineffective or Missing Controls 192

18.7. Monitor Effectiveness of Remediation Efforts 193

18.8. Reporting Process to Business Stakeholders 194

Conclusion..... 194

Domain 3: Management – Projects & Operations

Domain 3 Overview 199

1. The Role of the CISO..... 201

1.1. Assessing 201

 1.1.1. Corporate Cultures 201

 1.1.2. Ethics..... 203

 1.1.2.1. EC-Council – C|CISO Code of Ethics..... 204

 1.1.2.2. ISC2 Code of Ethics..... 205

 1.1.2.3. Computer Ethics Institute 208

 1.1.3. Accountability – Information Security Roles and Responsibilities 210

 1.1.3.1. Board of Directors (BoD) 210

 1.1.3.2. Chief Executive Officer (CEO)..... 211

 1.1.3.3. Chief Risk Officer (CRO)..... 211

 1.1.3.4. Chief Information Officer (CIO) 212

 1.1.3.5. Chief Information Security Officer (CISO)..... 213

 1.1.3.6. Information Security Department..... 214

 1.1.3.7. Chief Enterprise Architect (CEA)..... 214

 1.1.3.8. Chief Technology Operations Officer (CTOO) 215

 1.1.3.9. Database Administrator (DBA)..... 216

 1.1.3.10. System Administrators (SA)/Network Administrator (NA) 216

 1.1.4. Minding Your Own Business 217

 1.1.5. The Organizational Structure 218

 1.1.6. Building a Security Culture..... 220

 1.1.7. Self-Assessment 221

1.1.8. Assessing Organizational Risk.....	222
1.1.8.1. Threats.....	225
1.1.8.2. Vulnerabilities.....	225
1.1.8.3. Risk Frameworks.....	225
1.1.8.3.1. OCTAVE®.....	226
1.1.8.3.2. COBIT (Control Objectives for Information and Related Technologies).....	226
1.1.8.3.3. ISO 31000.....	227
1.1.8.3.4. NIST Special Publication 800-53.....	230
1.1.8.4. Preparing for the Risk Assessment.....	231
1.1.8.4.1. Identify the Purpose of the Risk Assessment.....	231
1.1.8.4.2. Identify the Scope of the Risk Assessment.....	232
1.1.8.4.3. Identify Assumptions and Constraints.....	232
1.1.8.4.4. Identify the Sources of Threat, Vulnerability, and Impact.....	235
1.1.8.5. Conducting the Risk Assessment.....	235
1.2. Planning.....	236
1.2.1. Program Mandates.....	237
1.2.2. Program Mission.....	237
1.2.3. Program Structure.....	237
1.2.4. Program Staffing and Functions.....	238
1.3. Designing.....	239
1.3.1. Infosec Documentation.....	240
1.3.1.1. Infosec Policies.....	240
1.3.1.2. Infosec Standards.....	241
1.3.1.3. Infosec Guidelines.....	241
1.3.1.4. Procedures.....	242
1.4. Executing.....	242
1.4.1. Infosec Governance.....	242
1.4.1.1. Characteristics of Effective Security Governance.....	243
1.4.2. Infosec Management.....	244
1.4.2.1. Incident Response.....	245
1.5. Metrics and Reporting.....	246
1.5.1. Why Measure Infosec?.....	246
1.5.2. Developing the Metrics Process.....	247

1.5.3. Developing and Selecting for the Metrics Program	247
1.5.4. Implementing the Metrics Program.....	248
2. Information Security Projects	249
2.1. Alignment with Business Goals	250
2.2. Identification of Project Stakeholders.....	250
2.3. Alignment with Risk Tolerance.....	251
2.4. Infosec Project Execution Best Practices.....	253
2.4.1. Infosec Project Initiation Phase	254
2.4.1.1. Creation of a Product Description Statement	254
2.4.1.2. Development of Project Feasibility.....	254
2.4.1.3. Development of a Project Concept Document	255
2.4.1.4. Creation of a Project Charter	255
2.4.1.5. Potential Barriers to Project Initiation.....	255
2.4.1.6. Problems during the Initiation Phase.....	255
2.4.1.7. Project Initiation Responsibilities.....	256
2.4.2. Scope Definition.....	256
2.4.3. Schedules	257
2.4.4. Budgets.....	258
2.4.5. Resources.....	259
2.4.6. Constraints.....	262
2.4.6.1. Time Constraints.....	263
2.4.6.2. Cost Constraints.....	263
2.4.6.3. Project Scope Constraints.....	263
3. Security Operations Management	263
3.1. Staff Functions and Skills.....	264
3.1.1. Technical vs. Administrative Responsibilities	264
3.1.1.1. Technical Infosec Staff and Skills.....	264
3.1.1.2. Administrative Security Staff and Skills	266
3.2. Communication Planning	266
3.3. Vendor Management	267
3.4. Accountability.....	269
3.4.1. Essentials for Audit Log Policy.....	269
3.5. Integration of Security Requirements into Other Operational Processes	271

- 3.5.1. Change Control..... 271
 - 3.5.1.1. Definitions 271
 - 3.5.1.2. Change Categories 271
 - 3.5.1.3. Change Process 272
 - 3.5.1.3.1. Emergency Changes 272
 - 3.5.1.3.2. Standard Changes..... 272
 - 3.5.1.3.3. Administrative and Development Changes 273
 - 3.5.1.4. Change Schedule 274
- 3.5.2. Disaster Recovery..... 274
- 3.5.3. System Development Lifecycle 276
 - 3.5.3.1. Sample Checklist for Security Requirements 277
 - 3.5.3.1.1. User Authentication and System Access Controls..... 277
 - 3.5.3.1.2. Account Administration..... 278
 - 3.5.3.1.3. Resource Access 279
 - 3.5.3.1.4. Access Privileges 279
 - 3.5.3.1.5. Accountability and Logging..... 279
 - 3.5.3.1.6. Disaster Recovery 280
 - 3.5.3.1.7. Administrator and Default User Account Security..... 281
 - 3.5.3.1.8. File and Database Access Permissions 281
- Summary 282**
- Additional Resources..... 282**

Domain 4: Information Security Core Competencies

- 1. Access Control 285**
 - 1.1. Access Control Design..... 285
 - 1.2. Types of Access Control..... 286
 - 1.2.1. Discretionary Access Control..... 286
 - 1.2.2. Mandatory Access Control..... 287
 - 1.2.3. Role-based Access 287
 - 1.3. Authentication Principles..... 287
 - 1.4. Authorization Principles 289
 - 1.4.1. Least Privilege Principle 289

1.4.2. Need to Know 290

1.4.3. Separation of duties..... 290

1.4.4. Unsuccessful Logons 290

1.4.5. Notification of System Use..... 290

1.4.6. Last Login Notification/Concurrent Sessions 290

1.5. Access Administration..... 291

2. Physical Security 292

2.1. Physical Risk Analysis..... 293

2.2. Facility Design Considerations..... 293

2.2.1. Geographic Location 293

2.2.2. Multi-tenancy 294

2.2.3. Building Materials 294

2.2.4. Barriers to Entry 294

2.2.5. Lighting 294

2.2.6. Door Locks 294

2.3. Guards 295

2.3.1. Alarm Systems..... 295

2.3.2. Perimeter Security..... 295

2.4. Personnel Security..... 295

2.4.1. Background Checks..... 296

2.4.2. On Boarding..... 296

2.4.3. Termination/Transfer..... 296

2.5. Physical Security Audits 297

2.6. Monitoring of Physical Security Controls 298

2.7. Physical Mobile Security..... 298

3. Disaster Recovery 298

3.1. Disaster Recovery vs. Business Continuity 299

3.2. Risk Appetite 299

3.3. Project Charters, Scope, Work Plans 300

3.4. Business Impact Analysis 300

3.5. Disaster Recovery Facilities 300

3.6. Disaster Recovery Testing 302

3.7. Data Backup and Recovery Solutions..... 303

3.8. Crisis Management..... 304

4. Network Security 304

4.1. Plans, Standards, and Best Practices 304

4.2. Network Planning 305

 4.2.1. Device Configuration..... 305

 4.2.2. Patches and Upgrades..... 305

 4.2.3. Network Discovery 305

 4.2.4. Multi-tiered Architectures 305

 4.2.5. Single Point of Failure 305

 4.2.6. Encryption over Open Networks 306

 4.2.7. Network Address Translation 306

4.3. Network Intrusion Detection and Intrusion Prevention 306

4.4. Network Access Control (NAC) 307

4.5. Virtual Private Networks (VPN) 308

4.6. Wireless Network Security..... 308

 4.6.1. Wireless Technology Risks..... 309

 4.6.2. Stealing Bandwidth..... 309

 4.6.3. Listening In 309

 4.6.4. Rogue Access Points 309

4.7. Securing the Network..... 310

4.8. Voice-over-IP (VoIP) Security..... 310

4.9. Network Architecture Models..... 311

 4.9.1. Local Area Network (LAN)..... 311

 4.9.2. Wide Area Network (WAN)..... 311

 4.9.3. Bus Topology..... 311

 4.9.4. Star Topology..... 312

 4.9.5. Ring Topology 312

 4.9.6. Mesh Topology..... 312

4.10. Network Standards and Protocols 312

 4.10.1. Layer 1 - Physical 312

 4.10.2. Layer 2 - Data-Link Layer 313

 4.10.3. Layer 3 - Network Layer..... 313

 4.10.4. Layer 4 - Transport Layer..... 313

4.10.5. Layer 5 - Session Layer	313
4.10.6. Layer 6 - Presentation Layer	313
4.10.7. Layer 7 - Application Layer.....	313
5. Threat and Vulnerability Management	314
5.1. Human Threats.....	314
5.2. Environmental/Physical Threats.....	315
5.3. Technical Threats.....	315
5.4. Natural Threats.....	316
5.5. Vulnerability Management.....	317
5.6. Monitoring and Alerting	317
5.7. Patch Management.....	318
5.8. Vulnerability Scanning.....	318
5.9. Penetration Testing.....	319
5.9.1. Black Box Testing.....	319
5.9.2. White Box Testing.....	320
5.9.3. Gray Box Testing	320
5.10. Social Engineering.....	320
5.11. Human Social Engineering.....	321
5.11.1. Eavesdropping	321
5.11.2. Shoulder Surfing	321
5.11.3. Dumpster Diving.....	321
5.11.4. In-Person	322
5.11.5. Third Party Authorization	322
5.12. Computer-based Social Engineering.....	322
5.12.1. Pop-up Windows	322
5.12.2. Mail Attachments/Websites.....	322
5.12.3. Phishing.....	322
5.13. Social Media Countermeasures.....	322
6. Application Security.....	323
6.1. Systems Development Life Cycle (SDLC) Practices	324
6.2. Phases of the Systems Development Life Cycle (SDLC).....	324
6.2.1. Initiation/Requirements/Planning Stage.....	324
6.2.2. Analysis Stage.....	326

6.2.3. Design Stage.....	327
6.2.4. Testing and Implementation Stage.....	328
6.2.5. Operations and Maintenance.....	328
6.3. Top-10 Application Vulnerabilities.....	329
6.3.1. Injection Flaws.....	329
6.3.2. Broken Authentication and Session Management.....	329
6.3.3. Cross-Site Scripting (XSS).....	329
6.3.4. Insecure Direct Object References.....	329
6.3.5. Security Mis-configuration.....	330
6.3.6. Sensitive Data Exposure.....	330
6.3.7. Missing Function Level Access Control.....	330
6.3.8. Cross-Site Request Forgery (CSRF).....	330
6.3.9. Using Components with Known Vulnerabilities.....	330
6.3.10. Unvalidated Redirects and Forwards.....	330
6.3.11. Code Reviews.....	330
6.4. Dynamic and Static Application Security Testing.....	331
6.5. Change Management.....	331
6.5.1. Data Sanitization.....	332
6.6. Separation of Production, Development, and Test Environments.....	332
6.7. Other SDLC Considerations.....	333
7. Systems Security.....	333
7.1. Plans.....	333
7.1.1. Standards.....	333
7.1.2. Procedures.....	334
7.1.3. Baselines.....	335
7.2. Best Practices.....	336
7.3. OS Hardening.....	337
7.4. Application Hardening.....	337
7.5. Database Hardening.....	337
7.6. Vulnerability Assessment.....	338
7.7. Configuration Management.....	338
7.8. Asset Management.....	339
7.9. Change Control.....	339

7.10. Logging.....	339
8. Encryption	340
8.1. Encryption Algorithms.....	340
8.1.1. Symmetric Encryption.....	341
8.1.2. Asymmetric Encryption	341
8.1.3. Hashing.....	341
8.2. Digital Signatures	342
8.3. Public Key Infrastructure.....	342
8.4. Secure Sockets Layer/Transport Layer Security.....	342
8.5. Security Protocols	343
8.5.1. Key Management.....	343
9. Computer Forensics and Incident Response	343
9.1. Development of Incident Response Procedures.....	344
9.1.1. Defining an Incident.....	344
9.1.2. Policies	345
9.1.3. Plans	345
9.1.4. Standard Operating Procedures	346
9.2. Responsibilities and Escalation Processes.....	346
9.2.1. Incident Response Steps.....	347
9.2.2. Preparation Phase.....	347
9.2.3. Detection Phase.....	348
9.2.4. Containment Phase	348
9.2.5. Eradication Phase.....	349
9.2.6. Recovery Phase.....	349
9.2.7. Lessons-Learned Phase.....	349
9.3. Testing Incident Response Procedures.....	350
9.4. Coordination with Law Enforcement and Other External Entities.....	350
9.5. Computer Forensics Process.....	351
9.5.1. Collection Phase	351
9.5.2. Examination Phase.....	352
9.5.3. Analysis Phase.....	352
9.5.4. Reporting Phase.....	352
9.6. Chain of Custody	353

9.7. Collecting and Preserving Digital Evidence..... 353

Summary 354

Suggested Reading 354

Domain 5: Strategic Planning & Finance

Introduction to Security Strategic Planning 359

1. Alignment with Business Goals and Risk Tolerance 361

1.1. Compliance as Security..... 361

1.2. Ethics 362

2. Relationship between Security, Compliance, & Privacy 363

3. Leadership..... 366

3.1. Visibility & Accessibility..... 367

3.2. Intimacy..... 368

3.3. Responsibility..... 369

3.4. Accountability..... 369

3.5. Education, Mentoring, and Guidance..... 369

3.6. Team Building 370

3.7. How Are Teams Most Effective? 370

3.8. Effective Team Characteristics 371

3.9. Common Misconceptions about Teams..... 373

3.10. Dysfunctional Teams 374

3.11. Key Elements of High Performance Teams 375

4. Enterprise Information Security Architecture (EISA) Models, Frameworks and Standards 376

4.1. EISA Goals 378

4.2. EISA Methodology..... 379

4.3. SABSA 381

4.4. US Department of Defense (DoD) Architecture Framework (DoDAF) 381

4.5. Federal Enterprise Architecture..... 382

4.6. Cap Gemini’s Integrated Architecture Framework..... 383

4.7. UK Ministry of Defense (MOD) Architecture Framework (MODAF)..... 383

4.8. Zachman Framework 384

4.9. The Open Group Architecture Framework (TOGAF)	384
5. Emerging Trends in Security	385
5.1. Inevitability of Breach	385
5.2. Getting Integrated.....	385
5.3. Control Systems	385
5.4. Philosophy Clash.....	385
5.5. Big Data, Big Threats	385
5.6. Cloud Computing Security	387
5.7. Consumerization	388
5.8. Mobile Devices in the Enterprise	388
5.9. Ransomware.....	389
5.10. Social Media.....	389
5.11. Hacktivism.....	390
5.12. Advanced Persistent Threat	390
6. It's all about the Data (Stradley 2009)	391
6.1. The Need to Protect Data and Information	391
6.2. How Data Leaks Occur	393
6.3. How to Protect Against Data Leaks.....	393
6.4. Technology Controls to Protect Data and Information	394
6.5. The DRM – DLP Conundrum	395
6.6. Reducing the Risk of Data Loss	397
6.7. Key Performance Indicators (KPI)	397
7. Systems Certification and Accreditation Process.....	398
7.1. PHASE 1: PRE-CERTIFICATION	400
7.2. PHASE 2: INITIATION	400
7.3. PHASE 3: SECURITY CERTIFICATION	400
7.4. PHASE 4: SECURITY ACCREDITATION	401
7.5. PHASE 5: MAINTENANCE	401
7.6. PHASE 6: DISPOSITION	402
8. Resource Planning	402
8.1. Full-time Employees.....	403
8.2. Operationalize Security Resources	403
8.3. Staff Augmentation.....	403

8.4. Consulting Firms	403
8.5. Outsourcing	404
8.6. How to proceed?	404
9. Financial Planning	404
9.1. Development of Business Cases for Security	405
9.2. Long Term Planning – Road Map	405
9.3. Analyze, Forecast And Develop Capital Expense Budget	405
9.4. Analyze, forecast and Develop Operating Expense Budget	406
9.5. Return on Investment (ROI) and Cost-Benefit Analysis	406
10. Procurement	406
10.1. Solution Selection	407
10.2. Technology acquisition life-cycle	407
11. Vendor Management	408
11.1. Pre Sales	408
11.2. Post Sales	409
11.3. Vendor Management Office	409
12. Request for Proposal (RFP) Process	410
12.1. Competitive Environment	411
12.2. Accentuate the Positive Aspects of the Deal	411
12.3. Tell the Vendors What You Hope to Achieve	411
12.4. Provide Opportunity for the Vendors to Differentiate Themselves	412
12.5. Ensure the Vendors Understand The Overall Environment	412
12.6. Demonstrate the Importance of the Transition Period	412
12.7. Clearly Define the Solution Being Procured	413
12.7.1. Know What You Are Looking For	413
12.7.2. Define the Boundaries of the Solution	413
12.7.3. Define the Performance Criteria	414
12.7.4. Take the Vendor’s Perspective	414
12.8. Enable the Objective Evaluation of Vendor Responses	415
12.8.1. Establish Discrete Requirements	415
12.8.2. Understand the Relative Importance of the Requirements	415
12.8.3. Define the Proposal Pricing Format	416
12.9. Achieve the Optimal Terms, Conditions, and Pricing in the Competitive Environment ..	416

12.9.1. Make It Clear that RFP Responses Will Become Contractually Binding 417

12.9.2. Where Appropriate, Use Contract-ready Requirements in the RFP..... 417

12.9.3. Consider Including the Master Services Agreement as Part of the RFP..... 417

12.9.4. Avoid Procrastination 417

12.10. Develop a Robust RFP 418

13. Integrate Security Requirements into the Contractual Agreement and Procurement Process 418

13.1. Section 1 – Definitions 418

13.2. Section 2 - Standard of Care 419

13.3. Section 3 - Restrictions on Disclosure to Third Parties..... 420

13.4. Section 4 - Security Breach Procedures..... 422

13.5. Section 5 - Oversight of Security Compliance 423

13.6. Section 6 - Return or Destruction of Personal Information..... 424

13.7. Section 7 - Equitable Relief..... 424

13.8. Section 8 – Material Breach 425

13.9. Section 9 – Indemnification..... 425

14. Statement of Work..... 425

15. Service Level Agreements 427

15.1. What is an SLA?..... 427

15.2. Why are SLAs needed? 427

15.3. Who Provides the SLA? 428

15.4. What's in an SLA? 428

15.5. What Are Key Components of an SLA?..... 428

15.6. Indemnification..... 428

15.7. Is an SLA Transferable? 429

15.8. Verification of Service Levels 429

15.9. Monitoring of Metrics..... 429

15.10. Metrics Selection..... 430

15.11. When Should We Review our SLAs? 430

Bibliography 431

Index 433