

Table of Contents

| | |
|--|----------|
| Table of Contents | 12 |
| List of Figures | 24 |
| List of Tables | 26 |
| Domain 1 – Governance and Risk Management | 1 |
| Governance..... | 3 |
| Knowledge Assumptions..... | 3 |
| 1. Define, Implement, Manage, and Maintain an Information Security Governance Program | 5 |
| 1.1. <i>Form of Business Organization</i> | 5 |
| 1.2. <i>Industry</i> | 6 |
| 1.3. <i>Organizational Maturity</i> | 6 |
| 2. Information Security Drivers | 7 |
| 3. Establishing an information security management structure..... | 8 |
| 3.1. <i>Organizational Structure</i> | 8 |
| 3.2. <i>Where does the CISO fit within the organizational structure?</i> | 8 |
| 3.3. <i>The Executive CISO</i> | 9 |
| 3.4. <i>Nonexecutive CISO</i> | 9 |
| 4. Laws/Regulations/Standards as drivers of Organizational Policy/Standards/Procedures | 10 |
| 5. Managing an enterprise information security compliance program | 10 |
| 5.1. <i>Security Policy</i> | 11 |
| 5.1.1. <i>Necessity of a Security Policy</i> | 12 |
| 5.1.2. <i>Security Policy Challenges</i> | 13 |
| 5.2. <i>Policy Content</i> | 13 |
| 5.2.1. <i>Types of Policies</i> | 14 |
| 5.2.2. <i>Policy Implementation</i> | 15 |
| 5.3. <i>Reporting Structure</i> | 17 |
| 5.4. <i>Standards and best practices</i> | 18 |
| 5.5. <i>Leadership and Ethics</i> | 19 |
| 5.6. <i>EC-Council Code of Ethics</i> | 20 |
| 6. Introduction to Risk Management | 21 |
| 6.1. <i>Risk Management Standards</i> | 22 |

| | |
|--|----|
| 6.2. <i>The Essentials of a Risk Management Program</i> | 24 |
| 6.3. <i>Where Risk Resides</i> | 25 |
| 6.4. <i>Risk Ownership</i> | 26 |
| 6.5. <i>Risk Assessment Types</i> | 27 |
| 6.6. <i>Risk Assessment Process</i> | 27 |
| 6.7. <i>Risk Categories</i> | 30 |
| 6.8. <i>Risk Treatment</i> | 31 |
| 6.9. <i>Risk Modification</i> | 33 |
| 6.10. <i>Risk Treatment Options</i> | 36 |
| 6.10.1. <i>Risk Modification or Mitigation</i> | 37 |
| 6.10.2. <i>Risk Retention or Risk Acceptance</i> | 37 |
| 6.10.3. <i>Risk Avoidance or Risk Elimination</i> | 38 |
| 6.10.4. <i>Risk Sharing or Risk Transfer</i> | 38 |
| 6.11. <i>Applying Compensating Controls to Reduce Risk</i> | 39 |
| 6.12. <i>Risk Calculation Formula</i> | 40 |
| 6.13. <i>Risk Management Frameworks</i> | 41 |
| 6.13.1. <i>ISO 27005</i> | 42 |
| 6.13.2. <i>Context Establishment</i> | 43 |
| 6.13.3. <i>Risk Assessment</i> | 44 |
| 6.13.4. <i>Risk Treatment</i> | 46 |
| 6.13.5. <i>Risk Acceptance</i> | 46 |
| 6.13.6. <i>Risk Feedback</i> | 47 |
| 6.13.7. <i>Risk Communication and Consultation</i> | 47 |
| 6.13.8. <i>Risk Monitoring and Review</i> | 48 |
| 6.13.9. <i>Risk Monitoring</i> | 48 |
| 6.13.10. <i>Risk Communications</i> | 49 |
| 6.14. <i>NIST Risk Management Framework (RMF)</i> | 49 |
| 6.14.1. <i>Step 1: Categorize the Information System</i> | 50 |
| 6.14.2. <i>Step 2: Select Security Controls</i> | 50 |
| 6.14.3. <i>Step 3: Implement Security Controls</i> | 50 |
| 6.14.4. <i>Step 4: Assess the Information System</i> | 50 |

| | |
|---|-----------|
| 6.14.5. Step 5: Authorize the Information System | 51 |
| 6.14.6. Step 6: Monitor Security Controls | 51 |
| 6.15. NIST Risk Management and Assessment | 51 |
| 6.16. NIST Risk Management Hierarchy | 51 |
| 6.17. NIST Risk Assessment Process | 52 |
| 6.18. Other Frameworks | 53 |
| 6.18.1. COBIT Risk Management | 53 |
| 6.18.2. COSO Enterprise Risk Management Integrated Framework | 53 |
| 6.18.3. Information Technology Infrastructure Library (ITIL) | 54 |
| 6.18.4. Factor Analysis of Information Risk (FAIR) | 54 |
| 6.18.5. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) | 55 |
| 6.18.6. Threat Agent Risk Assessment (TARA) | 56 |
| 6.19. Risk Management Policies and Procedures | 57 |
| 6.20. Risk Management Lifecycle | 59 |
| 6.21. Risk Management Program Implementation Use Case | 61 |
| 6.22. Risk Management Program Review | 66 |
| 6.23. Conclusion | 67 |
| Domain 2 – Information Security Controls, Compliance and Audit Management | 69 |
| Introduction | 71 |
| Knowledge Assumptions | 71 |
| 1. INFORMATION SECURITY CONTROLS | 72 |
| 1.1. Identifying the Organization’s Information Security Needs | 72 |
| 1.1.1. Identifying the Optimum Information Security Framework | 72 |
| 1.1.2. Designing Security Controls | 76 |
| 1.1.3. Control Lifecycle Management | 77 |
| 1.1.4. Control Classification | 78 |
| 1.1.5. Control Selection and Implementation | 81 |
| 1.1.6. Control Catalog | 82 |
| 1.1.7. Control Maturity | 83 |
| 1.1.8. Monitoring Security Controls | 84 |
| 1.1.9. Remediating Control Deficiencies | 85 |

| | |
|--|-----|
| 1.1.10. Maintaining Security Controls..... | 85 |
| 1.1.11. Reporting Controls | 85 |
| 1.1.12. Information Security Service Catalog..... | 85 |
| 2. COMPLIANCE MANAGEMENT | 86 |
| 2.1. Acts, Laws, and Statutes | 88 |
| 2.1.1. FISMA..... | 88 |
| 2.2. Regulations | 90 |
| 2.2.1. GDPR..... | 90 |
| 2.3. Standards | 91 |
| 2.3.1. ASD—Information Security Manual | 91 |
| 2.3.2. Basel III..... | 91 |
| 2.3.3. FFIEC | 92 |
| 2.3.4. ISO 27000 Family of Standards..... | 92 |
| 2.3.5. NERC-CIP..... | 96 |
| 2.3.6. PCI DSS..... | 97 |
| 2.3.7. NIST Special Publications..... | 97 |
| 2.3.8. Statement on Standards for Attestation Engagements No. 16 (SSAE 16) | 100 |
| 3. GUIDELINES, GOOD AND BEST PRACTICES..... | 101 |
| 3.1. CIS..... | 101 |
| 3.1.1. OWASP..... | 102 |
| 4. AUDIT MANAGEMENT | 103 |
| 4.1. Audit Expectations and Outcomes..... | 103 |
| 4.2. IS Audit Practices..... | 103 |
| 4.2.1. ISO/IEC Audit Guidance | 104 |
| 4.2.2. Internal versus External Audits | 106 |
| 4.2.3. Partnering with the Audit Organization | 107 |
| 4.2.4. Audit Process | 108 |
| 4.2.5. General Audit Standards | 109 |
| 4.2.6. Compliance-Based Audits..... | 112 |
| 4.2.7. Risk-Based Audits | 112 |
| 4.2.8. Managing and Protecting Audit Documentation | 113 |

| | |
|---|------------|
| 4.2.9. Performing an Audit | 113 |
| 4.2.10. Evaluating Audit Results and Report | 114 |
| 4.2.11. Remediating Audit Findings | 114 |
| 4.2.12. Leverage GRC Software to Support Audits | 115 |
| 5. SUMMARY | 116 |
| Domain 3: Security Program Management and Operations | 117 |
| Introduction | 119 |
| Knowledge Assumptions..... | 119 |
| 1. PROGRAM MANAGEMENT..... | 120 |
| 1.1. <i>Defining a Security Charter, Objectives, Requirements, Stakeholders, and Strategies</i> . | 120 |
| 1.1.1. <i>Security Program Charter</i> | 120 |
| 1.1.2. <i>Security Program Objectives</i> | 122 |
| 1.1.3. <i>Security Program Requirements</i> | 122 |
| 1.1.4. <i>Security Program Stakeholders</i> | 123 |
| 1.1.5. <i>Security Program Strategy Development</i> | 123 |
| 1.2. <i>Executing an Information Security Program</i> | 124 |
| 1.3. <i>Defining and Developing, Managing and Monitoring the Information Security Program</i> | 125 |
| 1.4. <i>Defining and Developing Information Security Program Staffing Requirements</i> | 126 |
| 1.5. <i>Managing the People of a Security Program</i> | 128 |
| 1.5.1. <i>Resolving Personnel and Teamwork Issues [72]</i> | 128 |
| 1.5.2. <i>Managing Training and Certification of Security Team Members</i> | 130 |
| 1.5.3. <i>Clearly Defined Career Path</i> | 130 |
| 1.5.4. <i>Designing and Implementing a User Awareness Program</i> | 130 |
| 1.6. <i>Managing the Architecture and Roadmap of the Security Program</i> | 131 |
| 1.6.1. <i>Information Security Program Architecture</i> | 131 |
| 1.6.2. <i>Information Security Program Roadmap</i> | 131 |
| 1.7. <i>Program Management and Governance</i> | 132 |
| 1.7.1. <i>Understanding Project Management Practices and Controls</i> | 132 |
| 1.7.2. <i>Identifying and Managing Project Stakeholders</i> | 133 |
| 1.7.3. <i>Measuring the Effectives of Projects</i> | 134 |

| | |
|---|-----|
| 1.8. Business Continuity Management (BCM) and Disaster Recovery Planning (DRP) | 135 |
| 1.9. Data Backup and Recovery | 135 |
| 1.10. Backup Strategy..... | 136 |
| 1.11. ISO BCM Standards..... | 136 |
| 1.11.1. Business Continuity Management (BCM) | 138 |
| 1.11.2. Disaster Recovery Planning (DRP)..... | 139 |
| 1.12. Continuity of Security Operations..... | 140 |
| 1.12.1. Integrating the Confidentiality, Integrity and Availability (CIA) Model | 140 |
| 1.13. BCM Plan Testing..... | 141 |
| 1.14. DRP Testing | 141 |
| 1.15. Contingency Planning, Operations, and Testing Programs to Mitigate Risk and Meet Service Level Agreements (SLAs)..... | 142 |
| 1.16. Computer Incident Response | 142 |
| 1.16.1. Incident Response Tools | 142 |
| 1.16.2. Incident Response Management | 142 |
| 1.16.3. Incident Response Communications | 143 |
| 1.16.4. Post-Incident Analysis | 144 |
| 1.16.5. Testing Incident Response Procedures..... | 144 |
| 1.17. Digital Forensics..... | 144 |
| 1.17.1. Crisis Management | 144 |
| 1.17.2. Digital Forensics Life Cycle | 145 |
| 2. OPERATIONS MANAGEMENT | 148 |
| 2.1. Establishing and Operating a Security Operations (SecOps) Capability | 148 |
| 2.2. Security Monitoring and Security Information and Event Management (SIEM) | 150 |
| 2.3. Event Management..... | 151 |
| 2.4. Incident Response Model | 153 |
| 2.4.1. Developing Specific Incident Response Scenarios | 155 |
| 2.5. Threat Management | 156 |
| 2.6. Threat Intelligence | 157 |
| 2.6.1. Information Sharing and Analysis Centers (ISAC) [83] | 158 |
| 2.7. Vulnerability Management | 159 |

| | |
|---|------------|
| 2.7.1. Vulnerability Assessments | 159 |
| 2.7.2. Vulnerability Management in Practice | 160 |
| 2.7.3. Penetration Testing | 160 |
| 2.7.4. Security Testing Teams | 161 |
| 2.7.5. Remediation | 162 |
| 2.8. Threat Hunting | 163 |
| 3. Summary..... | 165 |
| Domain 4: Information Security Core Competencies | 167 |
| Introduction | 169 |
| Knowledge Assumptions..... | 169 |
| 1. ACCESS CONTROL | 170 |
| 1.1. Authentication, Authorization, and Auditing..... | 170 |
| 1.2. Authentication | 171 |
| 1.3. Authorization | 173 |
| 1.4. Auditing..... | 173 |
| 1.5. User Access Control Restrictions | 174 |
| 1.6. User Access Behavior Management | 174 |
| 1.7. Types of Access Control Models | 175 |
| 1.8. Designing an Access Control Plan | 176 |
| 1.9. Access Administration | 177 |
| 2. PHYSICAL SECURITY | 178 |
| 2.1. Designing, Implementing, and Managing Physical Security Program..... | 178 |
| 2.1.1. Physical Risk Assessment..... | 178 |
| 2.2. Physical Location Considerations..... | 179 |
| 2.3. Obstacles and Prevention | 179 |
| 2.4. Secure Facility Design..... | 181 |
| 2.4.1. Security Operations Center..... | 181 |
| 2.4.2. Sensitive Compartmented Information Facility..... | 182 |
| 2.4.3. Digital Forensics Lab..... | 182 |
| 2.4.4. Datacenter | 183 |
| 2.5. Preparing for Physical Security Audits | 184 |

| | |
|--|-----|
| 3. NETWORK SECURITY..... | 185 |
| 3.1. Network Security Assessments and Planning | 185 |
| 3.2. Network Security Architecture Challenges..... | 185 |
| 3.3. Network Security Design | 186 |
| 3.4. Network Standards, Protocols, and Controls..... | 186 |
| 3.4.1. Network Security Standards | 186 |
| 3.4.2. Protocols..... | 188 |
| 3.4.3. Network Security Controls | 192 |
| 3.5. Wireless (Wi-Fi) Security | 195 |
| 3.5.1. Wireless Risks | 195 |
| 3.5.2. Wireless Controls | 195 |
| 3.6. Voice over IP Security..... | 196 |
| 4. ENDPOINT PROTECTION..... | 196 |
| 4.1. Endpoint Threats..... | 197 |
| 4.2. Endpoint Vulnerabilities..... | 198 |
| 4.3. End User Security Awareness..... | 198 |
| 4.4. Endpoint Device Hardening..... | 199 |
| 4.5. Endpoint Device Logging..... | 199 |
| 4.6. Mobile Device Security..... | 199 |
| 4.6.1. Mobile Device Risks | 199 |
| 4.6.2. Mobile Device Security Controls | 201 |
| 4.7. Internet of Things Security (IoT)..... | 201 |
| 4.7.1. Protecting IoT Devices | 202 |
| 5. APPLICATION SECURITY..... | 202 |
| 5.1. Secure SDLC Model..... | 202 |
| 5.2. Separation of Development, Test, and Production Environments..... | 203 |
| 5.3. Application Security Testing Approaches..... | 203 |
| 5.4. DevSecOps..... | 204 |
| 5.5. Waterfall Methodology and Security..... | 206 |
| 5.6. Agile Methodology and Security | 207 |
| 5.7. Other Application Development Approaches..... | 207 |

| | |
|---|-----|
| 5.8. Application Hardening | 207 |
| 5.9. Application Security Technologies | 208 |
| 5.10. Version Control and Patch Management | 209 |
| 5.11. Database Security | 209 |
| 5.12. Database Hardening | 210 |
| 5.13. Secure Coding Practices | 210 |
| 6. ENCRYPTION TECHNOLOGIES | 211 |
| 6.1. Encryption and Decryption | 211 |
| 6.2. Cryptosystems | 211 |
| 6.2.1. Blockchain | 211 |
| 6.2.2. Digital Signatures and Certificates | 212 |
| 6.2.3. PKI | 212 |
| 6.2.4. Key Management | 212 |
| 6.3. Hashing | 213 |
| 6.4. Encryption Algorithms | 213 |
| 6.5. Encryption Strategy Development | 214 |
| 6.5.1. Determining Critical Data Location and Type | 214 |
| 6.5.2. Deciding What to Encrypt | 215 |
| 6.5.3. Determining Encryption Requirements | 215 |
| 6.5.4. Selecting, Integrating, and Managing Encryption Technologies | 216 |
| 7. VIRTUALIZATION SECURITY | 217 |
| 7.1. Virtualization Overview | 217 |
| 7.2. Virtualization Risks | 218 |
| 7.3. Virtualization Security Concerns | 220 |
| 7.4. Virtualization Security Controls | 220 |
| 7.5. Virtualization Security Reference Model | 221 |
| 8. CLOUD COMPUTING SECURITY | 222 |
| 8.1. Overview of Cloud Computing | 222 |
| 8.2. Security and Resiliency Cloud Services | 224 |
| 8.3. Cloud Security Concerns | 224 |
| 8.4. Cloud Security Controls | 225 |

| | |
|--|-----|
| 8.5. <i>Cloud Computing Protection Considerations [111]</i> | 226 |
| 9. TRANSFORMATIVE TECHNOLOGIES | 228 |
| 9.1. <i>Artificial Intelligence</i> | 228 |
| 9.2. <i>Augmented Reality</i> | 228 |
| 9.3. <i>Autonomous SOC</i> | 229 |
| 9.4. <i>Dynamic Deception</i> | 229 |
| 9.5. <i>Software-Defined Cybersecurity</i> | 229 |
| 10. Summary | 230 |
| Domain 5 – Strategic Planning, Finance, Procurement and Vendor Management | 231 |
| Introduction | 233 |
| Knowledge Assumptions..... | 233 |
| 1. STRATEGIC PLANNING | 234 |
| 1.1. <i>Understanding the Organization</i> | 234 |
| 1.1.1. <i>Understanding the Business Structure</i> | 235 |
| 1.1.2. <i>Determining and Aligning Business and Information Security Goals</i> | 236 |
| 1.1.3. <i>Identifying Key Sponsors, Stakeholders, and Influencers</i> | 236 |
| 1.1.4. <i>Understanding Organizational Financials</i> | 237 |
| 1.2. <i>Creating an Information Security Strategic Plan</i> | 239 |
| 1.2.1. <i>Strategic Planning Basics [125]</i> | 240 |
| 1.2.2. <i>Alignment to Organizational Strategy and Goals</i> | 241 |
| 1.2.3. <i>Defining Tactical Short, Medium, and Long-Term Information Security Goals</i> | 241 |
| 1.2.4. <i>Information Security Strategy Communication</i> | 242 |
| 1.2.5. <i>Creating a Culture of Security</i> | 243 |
| 2. Designing, Developing, and Maintaining an Enterprise Information Security Program | 244 |
| 2.1. <i>Ensuring a Sound Program Foundation</i> | 245 |
| 2.2. <i>Architectural Views</i> | 246 |
| 2.3. <i>Creating Measurements and Metrics</i> | 247 |
| 2.4. <i>Balanced Scorecard</i> | 248 |
| 2.5. <i>Continuous Monitoring and Reporting Outcomes</i> | 248 |
| 2.6. <i>Continuous Improvement</i> | 249 |
| 2.7. <i>Information Technology Infrastructure Library (ITIL) Continual Service Improvement</i> | |

| | |
|--|-----|
| (CSI) | 249 |
| 3. Understanding the Enterprise Architecture (EA) | 250 |
| 3.1. EA Types | 251 |
| 3.1.1. The Zachman Framework: | 251 |
| 3.1.2. The Open Group Architecture Framework (TOGAF) | 252 |
| 3.1.3. Sherwood Applied Business Security Architecture (SABSA) | 254 |
| 3.1.4. Federal Enterprise Architecture Framework (FEAF) | 255 |
| 4. FINANCE | 257 |
| 4.1. Understanding Security Program Funding | 257 |
| 4.2. Analyzing, Forecasting, and Developing a Security Budget | 257 |
| 4.2.1. Resource Requirements | 259 |
| 4.2.2. Define Financial Metrics | 260 |
| 4.2.3. Technology Refresh | 260 |
| 4.2.4. New Project Funding | 260 |
| 4.2.5. Contingency Funding | 261 |
| 4.3. Managing the information Security Budget | 262 |
| 4.3.1. Obtain Financial Resources | 262 |
| 4.3.2. Allocate Financial Resources | 263 |
| 4.3.3. Information Security Program Financial Management | 263 |
| 4.3.4. Developing an Information Security Program Budget | 264 |
| 4.3.5. Managing an Information Security Program Budget | 265 |
| 4.3.7. Report Metrics to Sponsors and Stakeholders | 266 |
| 4.3.8. Balancing the Information Security Budget | 266 |
| 5. PROCUREMENT | 267 |
| 5.1. Procurement Program Terms and Concepts | 267 |
| 5.1.1. Statement of Objectives (SOO) | 267 |
| 5.1.2. Statement of Work (SOW) | 267 |
| 5.1.3. Total Cost of Ownership (TCO) | 267 |
| 5.1.4. Request for Information (RFI) | 267 |
| 5.1.5. Request for Proposal (RFP) | 267 |
| 5.1.6. Master Service Agreement (MSA) | 268 |

| | |
|--|-----|
| 5.1.7. <i>Service Level Agreement (SLA)</i> | 268 |
| 5.1.8. <i>Terms and Conditions (T&C)</i> | 268 |
| 5.2. <i>Understanding the Organization’s Procurement Program</i> | 268 |
| 5.2.1. <i>Internal Policies, Processes, and Requirements</i> | 268 |
| 5.2.2. <i>External or Regulatory Requirements</i> | 269 |
| 5.2.3. <i>Local Versus Global Requirements</i> | 270 |
| 5.3. <i>Procurement Risk Management</i> | 270 |
| 5.3.1. <i>Standard Contract Language</i> | 271 |
| 6. VENDOR MANAGEMENT | 271 |
| 6.1. <i>Understanding the Organization’s Acquisition Policies and Procedures</i> | 271 |
| 6.1.1. <i>Procurement Life cycle</i> | 271 |
| 6.2. <i>Applying Cost-Benefit Analysis (CBA) During the Procurement Process</i> | 274 |
| 6.3. <i>Vendor Management Policies</i> | 274 |
| 6.4. <i>Contract Administration Policies</i> | 275 |
| 6.4.1. <i>Service and Contract Delivery Metrics</i> | 275 |
| 6.4.2. <i>Contract Delivery Reporting</i> | 275 |
| 6.4.3. <i>Change Requests</i> | 275 |
| 6.4.4. <i>Contract Renewal</i> | 275 |
| 6.4.5. <i>Contract Closure</i> | 275 |
| 6.5. <i>Delivery Assurance</i> | 276 |
| 6.5.1. <i>Validation of Meeting Contractual Requirements</i> | 276 |
| 6.5.2. <i>Formal Delivery Audits</i> | 276 |
| 6.5.3. <i>Periodic Random Delivery Audits</i> | 276 |
| 6.5.4. <i>Third-Party Attestation Services (TPRM)</i> | 276 |
| 7. Summary | 277 |
| References | 279 |
| Index | 291 |