# Contents

Foreword xxv  
Introduction xxvii  

**DOMAIN 1: SECURITY AND RISK MANAGEMENT**  
1  
Understand and Apply Concepts of Confidentiality, Integrity, and Availability  
   Information Security 2  
Evaluating and Apply Security Governance Principles 6  
   Alignment of Security Functions to Business Strategy, Goals, Mission, and Objectives 6  
   Vision, Mission, and Strategy 6  
   Governance 7  
   Due Care 10  
Determine Compliance Requirements 11  
   Legal Compliance 12  
   Jurisdiction 12  
   Legal Tradition 12  
   Legal Compliance Expectations 13  
Understand Legal and Regulatory Issues That Pertain to Information Security in a Global Context 13  
   Cyber Crimes and Data Breaches 14  
   Privacy 36  
Understand, Adhere to, and Promote Professional Ethics 49  
   Ethical Decision-Making 49  
   Established Standards of Ethical Conduct 51  
   (ISC)² Ethical Practices 56  
Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines 57  
   Organizational Documents 58  
   Policy Development 61  
   Policy Review Process 61
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify, Analyze, and Prioritize Business Continuity Requirements</td>
<td>62</td>
</tr>
<tr>
<td>Develop and Document Scope and Plan</td>
<td>62</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>70</td>
</tr>
<tr>
<td>Business Impact Analysis</td>
<td>71</td>
</tr>
<tr>
<td>Develop the Business Continuity Plan</td>
<td>73</td>
</tr>
<tr>
<td>Contribute to and Enforce Personnel Security Policies and Procedures</td>
<td>80</td>
</tr>
<tr>
<td>Key Control Principles</td>
<td>80</td>
</tr>
<tr>
<td>Candidate Screening and Hiring</td>
<td>82</td>
</tr>
<tr>
<td>Onboarding and Termination Processes</td>
<td>91</td>
</tr>
<tr>
<td>Vendor, Consultant, and Contractor Agreements and Controls</td>
<td>96</td>
</tr>
<tr>
<td>Privacy in the Workplace</td>
<td>97</td>
</tr>
<tr>
<td>Understand and Apply Risk Management Concepts</td>
<td>99</td>
</tr>
<tr>
<td>Risk</td>
<td>99</td>
</tr>
<tr>
<td>Risk Management Frameworks</td>
<td>99</td>
</tr>
<tr>
<td>Risk Assessment Methodologies</td>
<td>108</td>
</tr>
<tr>
<td>Understand and Apply Threat Modeling Concepts and Methodologies</td>
<td>111</td>
</tr>
<tr>
<td>Threat Modeling Concepts</td>
<td>111</td>
</tr>
<tr>
<td>Threat Modeling Methodologies</td>
<td>112</td>
</tr>
<tr>
<td>Apply Risk-Based Management Concepts to the Supply Chain</td>
<td>116</td>
</tr>
<tr>
<td>Supply Chain Risks</td>
<td>116</td>
</tr>
<tr>
<td>Supply Chain Risk Management</td>
<td>119</td>
</tr>
<tr>
<td>Establish and Maintain a Security Awareness, Education, and Training Program</td>
<td>121</td>
</tr>
<tr>
<td>Security Awareness Overview</td>
<td>122</td>
</tr>
<tr>
<td>Developing an Awareness Program</td>
<td>123</td>
</tr>
<tr>
<td>Training</td>
<td>127</td>
</tr>
<tr>
<td>Summary</td>
<td>128</td>
</tr>
</tbody>
</table>

**DOMAIN 2: ASSET SECURITY**  

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Security Concepts</td>
<td>131</td>
</tr>
<tr>
<td>Data Policy</td>
<td>132</td>
</tr>
<tr>
<td>Data Governance</td>
<td>132</td>
</tr>
<tr>
<td>Data Quality</td>
<td>133</td>
</tr>
<tr>
<td>Data Documentation</td>
<td>134</td>
</tr>
<tr>
<td>Data Organization</td>
<td>136</td>
</tr>
<tr>
<td>Identify and Classify Information and Assets</td>
<td>139</td>
</tr>
<tr>
<td>Asset Classification</td>
<td>141</td>
</tr>
<tr>
<td>Determine and Maintain Information and Asset Ownership</td>
<td>145</td>
</tr>
<tr>
<td>Asset Management Lifecycle</td>
<td>146</td>
</tr>
<tr>
<td>Software Asset Management</td>
<td>148</td>
</tr>
</tbody>
</table>
Understand the Fundamental Concepts of Security Models 230
  Bell-LaPadula Model 232
  The Biba Integrity Model 234
  The Clark-Wilson Model 235
  The Brewer-Nash Model 235
Select Controls Based upon Systems Security Requirements 237
Understand Security Capabilities of Information Systems 241
  Memory Protection 241
  Virtualization 244
  Secure Cryptoprocessor 247
Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements 253
  Client-Based Systems 254
  Server-Based Systems 255
  Database Systems 257
  Cryptographic Systems 260
  Industrial Control Systems 267
  Cloud-Based Systems 271
  Distributed Systems 274
  Internet of Things 275
Assess and Mitigate Vulnerabilities in Web-Based Systems 278
  Injection Vulnerabilities 279
  Broken Authentication 280
  Sensitive Data Exposure 283
  XML External Entities 284
  Broken Access Control 284
  Security Misconfiguration 285
  Cross-Site Scripting 285
  Using Components with Known Vulnerabilities 286
  Insufficient Logging and Monitoring 286
  Cross-Site Request Forgery 287
Assess and Mitigate Vulnerabilities in Mobile Systems 287
  Passwords 288
  Multifactor Authentication 288
  Session Lifetime 289
  Wireless Vulnerabilities 290
  Mobile Malware 290
  Unpatched Operating System or Browser 290
Secure Network Components 411
  Firewalls 412
  Network Address Translation 418
  Intrusion Detection System 421
  Security Information and Event Management 422
  Network Security from Hardware Devices 423
  Transmission Media 429
  Endpoint Security 442
  Implementing Defense in Depth 447
  Content Distribution Networks 448

Implement Secure Communication Channels According to Design 449
  Secure Voice Communications 449
  Multimedia Collaboration 452
  Remote Access 458
  Data Communications 466
  Virtualized Networks 470

Summary 481

**DOMAIN 5: IDENTITY AND ACCESS MANAGEMENT** 483

Control Physical and Logical Access to Assets 484
  Information 485
  Systems 486
  Devices 487
  Facilities 488

Manage Identification and Authentication of People, Devices, and Services 492
  Identity Management Implementation 494
  Single Factor/Multifactor Authentication 496
  Accountability 511
  Session Management 511
  Registration and Proofing of Identity 513
  Federated Identity Management 520
  Credential Management Systems 524

Integrate Identity as a Third-Party Service 525
  On-Premise 526
  Cloud 527
  Federated 527

Implement and Manage Authorization Mechanisms 528
  Role-Based Access Control 528
  Rule-Based Access Control 529
Mandatory Access Control 530
Discretionary Access Control 531
Attribute-Based Access Control 531

Manage the Identity and Access Provisioning Lifecycle 533
User Access Review 534
System Account Access Review 535
Provisioning and Deprovisioning 535
Auditing and Enforcement 536
Summary 537

DOMAIN 6: SECURITY ASSESSMENT AND TESTING 539
Design and Validate Assessment, Test, and Audit Strategies 540
Assessment Standards 543
Conduct Security Control Testing 545
Vulnerability Assessment 546
Penetration Testing 554
Log Reviews 564
Synthetic Transactions 565
Code Review and Testing 567
Misuse Case Testing 571
Test Coverage Analysis 573
Interface Testing 574

Collect Security Process Data 575
Account Management 577
Management Review and Approval 579
Key Performance and Risk Indicators 580
Backup Verification Data 583
Training and Awareness 584
Disaster Recovery and Business Continuity 585

Analyze Test Output and Generate Report 587
Conduct or Facilitate Security Audits 590
Internal Audits 591
External Audits 591
Third-Party Audits 592
Integrating Internal and External Audits 593
Auditing Principles 593
Audit Programs 594
Summary 596
DOMAIN 7: SECURITY OPERATIONS

Understand and Support Investigations
   Evidence Collection and Handling
   Reporting and Documentation
   Investigative Techniques
   Digital Forensics Tools, Techniques, and Procedures

Understand Requirements for Investigation Types
   Administrative
   Criminal
   Civil
   Regulatory
   Industry Standards

Conduct Logging and Monitoring Activities
   Define Auditable Events
   Time
   Protect Logs
   Intrusion Detection and Prevention
   Security Information and Event Management
   Continuous Monitoring
   Ingress Monitoring
   Egress Monitoring

Securely Provision Resources
   Asset Inventory
   Asset Management
   Configuration Management

Understand and Apply Foundational Security Operations Concepts
   Need to Know/Least Privilege
   Separation of Duties and Responsibilities
   Privileged Account Management
   Job Rotation
   Information Lifecycle
   Service Level Agreements

Apply Resource Protection Techniques to Media
   Marking
   Protecting
   Transport
   Sanitization and Disposal
Conduct Incident Management 650
  An Incident Management Program 651
Detection 653
Response 656
Mitigation 657
Reporting 658
Recovery 661
Remediation 661
Lessons Learned 661
Third-Party Considerations 662

Operate and Maintain Detective and Preventative Measures 663
  White-listing/Black-listing 665
Third-Party Security Services 665
Honeypots/Honeynets 667
Anti-Malware 667

Implement and Support Patch and Vulnerability Management 670
Understand and Participate in Change Management Processes 672

Implement Recovery Strategies 673
  Backup Storage Strategies 673
Recovery Site Strategies 676
Multiple Processing Sites 678
System Resilience, High Availability, Quality of Service, and Fault Tolerance 679

Implement Disaster Recovery Processes 679
  Response 680
Personnel 680
Communications 682
Assessment 682
Restoration 683
Training and Awareness 684

Test Disaster Recovery Plans 685
  Read-Through/Tabletop 686
Walk-Through 687
Simulation 687
Parallel 687
Full Interruption 688

Participate in Business Continuity Planning and Exercises 688

Implement and Manage Physical Security 689
  Physical Access Control 689
The Data Center 692
Address Personnel Safety and Security Concerns 693
  Travel 693
  Duress 693
Summary 694

DOMAIN 8: SOFTWARE DEVELOPMENT SECURITY 695

Understand and Integrate Security in the Software Development Lifecycle 696
  Development Methodologies 696
  Maturity Models 753
  Operations and Maintenance 768
  Change Management 770
  Integrated Product Team 773

Identify and Apply Security Controls in Development Environments 776
  Security of the Software Environment 777
  Configuration Management as an Aspect of Secure Coding 796
  Security of Code Repositories 798

Assess the Effectiveness of Software Security 802
  Logging and Auditing of Changes 802
  Risk Analysis and Mitigation 817

Assess the Security Impact of Acquired Software 835
  Acquired Software Types 835
  Software Acquisition Process 842
  Relevant Standards 845
  Software Assurance 848
  Certification and Accreditation 852

Define and Apply Secure Coding Standards and Guidelines 853
  Security Weaknesses and Vulnerabilities at the Source-Code Level 854
  Security of Application Programming Interfaces 859
  Secure Coding Practices 868

Summary 874

Index 875