

Contents at a Glance

<i>Introduction</i>		<i>xxxvii</i>
<i>Assessment Test</i>		<i>lix</i>
Chapter 1	Security Governance Through Principles and Policies	1
Chapter 2	Personnel Security and Risk Management Concepts	43
Chapter 3	Business Continuity Planning	113
Chapter 4	Laws, Regulations, and Compliance	143
Chapter 5	Protecting Security of Assets	179
Chapter 6	Cryptography and Symmetric Key Algorithms	219
Chapter 7	PKI and Cryptographic Applications	263
Chapter 8	Principles of Security Models, Design, and Capabilities	309
Chapter 9	Security Vulnerabilities, Threats, and Countermeasures	353
Chapter 10	Physical Security Requirements	447
Chapter 11	Secure Network Architecture and Components	495
Chapter 12	Secure Communications and Network Attacks	581
Chapter 13	Managing Identity and Authentication	637
Chapter 14	Controlling and Monitoring Access	677
Chapter 15	Security Assessment and Testing	723
Chapter 16	Managing Security Operations	763
Chapter 17	Preventing and Responding to Incidents	801
Chapter 18	Disaster Recovery Planning	861
Chapter 19	Investigations and Ethics	909
Chapter 20	Software Development Security	941
Chapter 21	Malicious Code and Application Attacks	993
Appendix A	Answers to Review Questions	1041
Appendix B	Answers to Written Labs	1099
<i>Index</i>		<i>1117</i>