

CONTENTS

	<i>Introduction</i>	<i>xiii</i>
PART I	DOMAIN 1: SECURITY PRINCIPLES	1
CHAPTER 1	Confidentiality, Integrity, Availability, and Non-repudiation	3
CHAPTER 2	Authentication, Authorization, and Accounting (AAA)	13
CHAPTER 3	Privacy	25
CHAPTER 4	Risk Management	37
CHAPTER 5	Governance Concepts	47
CHAPTER 6	Cybersecurity Controls	55
CHAPTER 7	Professional and Ethical Conduct	61
PART II	DOMAIN 2: SECURITY GOVERNANCE	71
CHAPTER 8	Governance, Risk, and Compliance	73
CHAPTER 9	Business Continuity	81
CHAPTER 10	Disaster Recovery	93
CHAPTER 11	Security Awareness	103
CHAPTER 12	Measuring Cybersecurity Effectiveness	113
PART III	DOMAIN 3: IDENTITY AND ACCESS MANAGEMENT (IAM) CONCEPTS	121
CHAPTER 13	Identity Life Cycle Management	123
CHAPTER 14	Logical Access Controls	131

PART IV	DOMAIN 4: NETWORKING AND CLOUD SECURITY CONCEPTS	137
CHAPTER 15	Network Security	139
CHAPTER 16	Network Security Architecture	155
CHAPTER 17	Cloud Security	163
PART V	DOMAIN 5: SECURITY OPERATIONS AND INCIDENT RESPONSE	171
CHAPTER 18	Encryption	173
CHAPTER 19	Data Handling	185
CHAPTER 20	Security Operations	193
CHAPTER 21	Incident Response	205
CHAPTER 22	Asset Protection	215
CHAPTER 23	Security Testing	225
CHAPTER 24	Artificial Intelligence	233
	<i>Index</i>	243