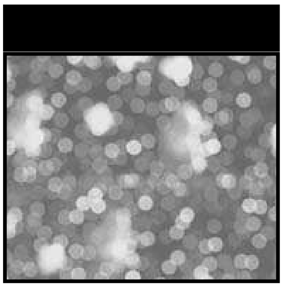

Contents

Acknowledgments xv

Foreword xvii

Introduction xxi

About the Authors xxvii

Chapter 1 Security Management Practices 1
- Sample Questions 29
- Bonus Questions 33
- Advanced Sample Questions 35

Chapter 2 Access Control Systems 43
- Rationale 43
- Controls 44
- Identification and Authentication 49
- Some Access Control Issues 65

Sample Questions 66
Bonus Questions 71
Advanced Sample Questions 73

Chapter 3 Telecommunications and Network Security 81
Our Goals 82
Domain Definition 83
Management Concepts 84
Sample Questions 159
Bonus Questions 165
Advanced Sample Questions 167

Chapter 4 Cryptography 175
Introduction 176
Cryptographic Technologies 189
Secret Key Cryptography (Symmetric Key) 194
Public (Asymmetric) Key Cryptosystems 203
Approaches to Escrowed Encryption 214
Internet Security Applications 218
Sample Questions 227
Bonus Questions 233
Advanced Sample Questions 235

Chapter 5 Security Architecture and Models 249
Security Architecture 249
Assurance 265
Information Security Models 272
Sample Questions 281
Bonus Questions 287
Advanced Sample Questions 290

Chapter 6 Operations Security 297
Our Goals 298
Domain Definition 298
Controls and Protections 299
Monitoring and Auditing 316
Threats and Vulnerabilities 321
Sample Questions 325

Bonus Questions 329
Advanced Sample Questions 331

Chapter 7 Applications and Systems Development 337

The Software Life Cycle Development Process 338
The Software Capability Maturity Model (CMM) 348
Object-Oriented Systems 350
Artificial Intelligence Systems 353
Database Systems 357
Application Controls 359
Sample Questions 363
Bonus Questions 368
Advanced Sample Questions 370

Chapter 8 Business Continuity Planning and Disaster Recovery Planning 377

Our Goals 378
Domain Definition 378
Business Continuity Planning 378
Disaster Recovery Planning 387
Sample Questions 402
Bonus Questions 405
Advanced Sample Questions 408

Chapter 9 Law, Investigation, and Ethics 415

Types of Computer Crime 415
Law 418
Investigation 431
Liability 437
Ethics 439
Sample Questions 444
Bonus Questions 449
Advanced Sample Questions 451

Chapter 10 Physical Security 459

Our Goals 460
Domain Definition 460

Threats to Physical Security 460
Controls for Physical Security 462
Sample Questions 486
Bonus Questions 490
Advanced Sample Questions 492

Appendix A A Process Approach to HIPAA Compliance through a HIPAA-CMM 497
Background 499
HIPAA Security Requirements Mappings to PAs 507
HPAs 508
Defining and Using the HIPAA-CMM 510
Conclusion 512
References 513
Appendix A: HIPAA-CMM PA Overview 514
Appendix B: Glossary (SSE-CMM v2.0) 524
Appendix C: The Ideal Approach to Process Improvement 527
Appendix D: SSE-CMM MAPPINGS and General Considerations 530

Appendix B The NSA InfoSec Assessment Methodology 532
History of the NIPC 533
About the ISSO 533
The InfoSec Assessment Methodology 534
PDD#63 536

Appendix C The Case for Ethical Hacking 543
Rationale 544
Roles and Responsibilities 544
Implementation 546
Summary 548

Appendix D The Common Criteria 549
Common Criteria: Launching the International Standard 549
Glossary 558
For More Information 559

Appendix E BS7799 561

Appendix F HIPAA Updates 563

Scope 563

Title II Administrative Simplification 564

Conclusion 570

Appendix G References for Further Study 571

Web Sites 573

Appendix H Answers to Sample and Bonus Questions 575

Chapter 1—Security Management Practices 575

Chapter 2—Access Control Systems and Methodology 583

Chapter 3—Telecommunications and Network Security 594

Chapter 4—Cryptography 605

Chapter 5—Security Architecture and Models 617

Chapter 6: Operations Security 629

Chapter 7—Applications and Systems Development 638

Chapter 8—Business Continuity Planning—Disaster Recovery Planning 647

Chapter 9—Law, Investigation, and Ethics 655

Chapter 10—Physical Security 664

Appendix I Answers to Advanced Sample Questions 673

Chapter 1—Security Management Practices 673

Chapter 2—Access Control Systems and Methodology 694

Chapter 3—Telecommunications and Network Security 713

Chapter 4—Cryptography 736

Chapter 5—Security Architecture and Models 767

Chapter 6—Operations Security 786

Chapter 7—Applications and Systems Development 809

Chapter 8—Business Continuity Planning—Disaster Recovery Planning 826

Chapter 9—Law, Investigation, and Ethics 845

Chapter 10—Physical Security 864

Notes 877

Appendix J What's on the CD-ROM 878

Glossary of Terms and Acronyms 881

Index 929