

CONTENTS

| | |
|--|-----|
| EXECUTIVE SUMMARY | 1 |
| SECTION 1: CYBERSECURITY INTRODUCTION AND OVERVIEW | 3 |
| Topic 1—Introduction to Cybersecurity | 5 |
| Topic 2—Difference Between Information Security and Cybersecurity | 9 |
| Topic 3—Cybersecurity Objectives | 11 |
| Topic 4—Cybersecurity Roles | 13 |
| Topic 5—Cybersecurity Domains..... | 17 |
| Section 1—Knowledge Check | 19 |
| SECTION 2: CYBERSECURITY CONCEPTS | 21 |
| Topic 1—Risk..... | 23 |
| Topic 2—Common Attack Types and Vectors | 27 |
| Topic 3—Policies and Procedures..... | 33 |
| Topic 4—Cybersecurity Controls | 37 |
| Section 2—Knowledge Check | 40 |
| SECTION 3: SECURITY ARCHITECTURE PRINCIPLES | 41 |
| Topic 1—Overview of Security Architecture | 43 |
| Topic 2—The OSI Model..... | 47 |
| Topic 3—Defense in Depth..... | 51 |
| Topic 4—Firewalls | 53 |
| Topic 5—Isolation and Segmentation..... | 59 |
| Topic 6—Monitoring, Detection and Logging | 61 |
| Topic 7A—Encryption Fundamentals | 65 |
| Topic 7B—Encryption Techniques | 67 |
| Topic 7C—Encryption Applications..... | 73 |
| Section 3—Knowledge Check | 75 |
| SECTION 4: SECURITY OF NETWORKS, SYSTEMS, APPLICATIONS AND DATA | 77 |
| Topic 1—Process Controls—Risk Assessments..... | 79 |
| Topic 2—Process Controls—Vulnerability Management..... | 83 |
| Topic 3—Process Controls—Penetration Testing..... | 85 |
| Topic 4—Network Security..... | 87 |
| Topic 5—Operating System Security | 95 |
| Topic 6—Application Security | 101 |
| Topic 7—Data Security | 107 |
| Section 4—Knowledge Check | 111 |
| SECTION 5: INCIDENT RESPONSE | 113 |
| Topic 1—Event vs. Incident..... | 115 |
| Topic 2—Security Incident Response..... | 117 |
| Topic 3—Investigations, Legal Holds and Preservation..... | 121 |
| Topic 4—Forensics | 123 |
| Topic 5—Disaster Recovery and Business Continuity Plans..... | 127 |
| Section 5—Knowledge Check | 131 |

SECTION 6: SECURITY IMPLICATIONS AND ADOPTION OF EVOLVING TECHNOLOGY 133

- Topic 1—Current Threat Landscape..... 135
- Topic 2—Advanced Persistent Threats 137
- Topic 3—Mobile Technology—Vulnerabilities, Threats and Risk 141
- Topic 4—Consumerization of IT and Mobile Devices 147
- Topic 5—Cloud and Digital Collaboration..... 149
- Section 6—Knowledge Check 153

APPENDICES 155

- Appendix A—Knowledge Statements 157
- Appendix B—Glossary 159
- Appendix C—Knowledge Check Answers..... 183
- Appendix D—Additional Resources 189