The following is an outline of the content areas covered in the examination. The approximate percentage of the examination devoted to each content area is also noted.

I. Application & Systems Security – 15%
   a. Security Triad
   b. Accountability & non-repudiation
   c. Fundamentals of Cryptography
   d. Security development life cycle
   e. Best practices for migration from development environment to production
   f. Anti-virus protection and malware detection

II. Authentication, Authorization, & Access Controls – 12%
    a. Implementing authentication technologies
    b. Authorization
    c. Access controls

III. Policies, Compliance, & Governance – 12%
    a. Security architecture
    b. Risk assessment
    c. Outsources process governance
    d. Ethics and legal

IV. Operational Security – 10%
    a. Securing and monitoring the production environment
    b. Policies, standards and procedures

V. Network Security – 20%
    a. Protocols and services
    b. Analysis tools and management
    c. Infrastructure
    d. Wireless

VI. Vulnerability Management – 15%
Testing the network
Recognizing and mitigating threats
Tools

VII. **Physical & Environmental Security – 6%**
   - Physical access controls and management
   - Environmental controls

VIII. **Disaster Recovery & Business Continuity – 10%**
   - Fire backup, retention, offsite storage, archiving
   - Business impact analysis
   - Disaster recovery planning
   - Business continuity planning
   - Plan testing and maintenance

**REFERENCES**

Below is a list of reference publications that were either used as a reference to create the exam, or were used as textbooks in college courses of the same or similar title at the time the test was developed. You may reference either the current edition of these titles or textbooks currently used at a local college or university for the same class title. It is recommended that you reference more than one textbook on the topics outlined in this fact sheet.

You should begin by checking textbook content against the content outline provided before selecting textbooks that cover the test content from which to study.

Sources for study material are suggested but not limited to the following:


**SAMPLE QUESTIONS**

All test questions are in a multiple-choice format, with one correct answer and three incorrect options. The following are samples of the types of questions that may appear on the exam.

1. A company needs to digitally sign all of the data sent to its customers. What should the administrator use to digitally sign the data?
   a. Asymmetric Keys
   b. Standard Keys
   c. Symmetric Keys
   d. Quantitative Keys

2. What standard does a Certificate Authority (CA) use to create a certificate?
   a. X.509
   b. X.802
   c. X.423
   d. X129

3. The concept of comparing the best practices and performance metrics of other companies with a similar process is known as
a. Benchmarking
b. Gap Analysis
c. Baselining
d. Quantifying

4. If an intrusion detection system wanted to only monitor web traffic, what would the rules filter on?
   a. IP Address
   b. Port
   c. User Name
   d. Destination Name

5. What security technique can be used to identify malicious HTTPS (Secure Hyper Text Transport Protocol) tunnels?
   a. Detection inspection
   b. Context inspection
   c. Plain HTTP inspection
   d. SSL inspection

Answers to sample questions:
1-A; 2-A; 3-A; 4-B; 5-D