BCS CISMP Study Guide

Learn the definitions in the Glossary and make sure you understand the concepts.

Chapter 1
Understand the definition of:

- Risk
- Threat
- Vulnerability

Understand the purpose of the controls:

- Avoidance
- Reduction
- Transfer
- Acceptance

Understand Accountability, Auditing and Compliance

Apply and understand CIA of Security

Chapter 2
Know the categories of Threat and Vulnerability

Understand the controls of risk:

- Detective
- Corrective
- Directive

Understand the operational controls:

- Physical
- Procedural
- Technical

Chapter 3
Understand GDPR

Understand the following ISOs:

- 27001
- 27002
- 15408
- 17025

Know the phases of incident handling:

- Reporting
- Investigation

- Assessment
- Corrective Action
- Review

Understand ACPO Guidelines

Understand technical standards (Common Criteria, ETSI, FIPS)

Chapter 4
Understand the data and information life cycle
- Acquisition
- Utilisation
- Disposal

Understand change control

Understand Agile and Waterfall methods

Chapter 5
Understand general controls:
- Physical
- Technical
- Procedural

Know:
What is a Security Culture
What is Security Awareness

Understand Contracts and Policies:
- Employment
- Codes of Conduct
- Acceptable Usage Policy
- Segregation of Duties
- BYOD

Understand Authentication and Authorisation concepts

Understand data classification system and be familiar with the UK Government system:
- Top Secret
- Secret
- Official

Understand User Training and Awareness and approaches to training and promoting awareness

Chapter 6
Know types of malicious software

Understand zero day exploits

Know malware counter measures:

- WAF
- AV
- Sheepdip

Understand the main sources of malware infection:

- Phishing
- USB devices
- Trojan

Understand partitioning networks and DMZs

Understand the function of:
Firewall
IDS
IPS

Understand the concepts of Penetration Testing

Understand cloud computing

- SaaS
- IaaS
- PaaS
- IDaaS
- Public Cloud
- Private Cloud
- Hybrid
- Community Cloud

Understand third party contracts (Flow Through)

Understand the relationship between supplier commercial risk and purchaser risk

Understand Configuration Management and Change Control

Chapter 7
Understand the concepts of Physical security

Understand clear screen/desk policy

Understand secure disposal techniques

Understand access control techniques:

- Mantraps

Chapter 8

Understand (and define)

- Resilience
- Redundancy

Understand BCP and testing

- Desk check
- Walk through
- Enactment
- Simulation

Understand offsite storage of vital material

Chapter 9

Understand the use of forensic services

Understand the basic concepts of cryptography

- Symmetric
- Asymmetric
- Digital signatures
- Hashing

Understand PGP

Understand Cyber Threat Intelligence and sources