

## **CISSP EXAM CRAM 2**

### **1. The CISSP Certification Exam.**

- Introduction.
- Assessing Exam Readiness.
- Taking the Exam.
- Multiple-Choice Question Format.
- Exam Strategy.
- Question-Handling Strategies.
- Mastering the Inner Game.
- Need to Know More?

### **2. Physical Security.**

- Introduction.
- Physical Security Risks.
  - Natural Disasters.
  - Man-Made Threats.
  - Emergency Situations.
- Requirements for New Site Locations.
  - Location.
  - Construction.
  - Doors, Walls, Windows, and Ceilings.
- Building Defense in Depth.
  - Perimeter Controls.
  - Server Placement.
  - Intrusion Detection.
- Environmental Controls.
- Electrical Power.
  - Uninterruptible Power Supply (UPS).
- Equipment Life Cycle.
- Fire Prevention, Detection, and Suppression.
  - Fire-Detection Equipment.
  - Fire Suppression.
- Exam Prep Questions.
- Answers to Exam Prep Questions.
- Need to Know More?

### **3. Security-Management Practices.**

- Introduction.
- The Risk of Poor Security Management.
- The Role of CIA.
- Risk Assessment.
  - Risk Management.
- Policies, Procedures, Standards, Baselines, and Guidelines.
  - Security Policy.
  - Standards.
  - Baselines.
  - Guidelines.
  - Procedures.
- Implementation.
  - Data Classification.
  - Roles and Responsibility.

**BUY ONLINE FROM:** <http://www.itgovernance.co.uk/products/497>

- Security Controls.
- Training and Education.
  - Security Awareness.
- Auditing Your Security Infrastructure.
- Exam Prep Questions.
- Answers to Exam Prep Questions.
- Need to Know More?

#### **4. Access-Control Systems and Methodology.**

- Introduction.
- Threats Against Access Control.
  - Password Attacks.
  - Emanation Security.
  - Denial of Service/Distributed Denial of Service (DoS/DDoS).
- Access-Control Types.
  - Administrative Controls.
  - Technical Controls.
  - Physical Controls.
- Identification, Authentication, and Authorization.
  - Authentication.
    - Single Sign-On.
      - Kerberos.
      - SESAME.
  - Access-Control Models.
- Data Access Controls.
  - Discretionary Access Control (DAC).
  - Mandatory Access Control (MAC).
  - Role-Based Access Control (RBAC).
  - Other Types of Access Controls.
- Intrusion-Detection Systems (IDS).
  - Network-Based Intrusion-Detection Systems (NIDS).
  - Host-Based Intrusion-Detection Systems (HIDS).
  - Signature-Based and Behavior-Based IDS Systems.
- Penetration Testing.
- Honeypots.
- Exam Prep Questions.
- Answers to Exam Prep Questions.
- Need to Know More?

#### **5. System Architecture and Models.**

- Introduction.
- Common Flaws in the Security Architecture.
  - Buffer Overflow.
  - Back Doors.
  - Asynchronous Attacks.
  - Covert Channels.
  - Incremental Attacks.
- Computer System Architecture.
  - Central Processing Unit (CPU).
  - Storage Media.
- Security Mechanisms.
  - Process Isolation.
  - Operation States.
  - Protection Rings.

**BUY ONLINE FROM:** <http://www.itgovernance.co.uk/products/497>

- Trusted Computer Base.
- Security Models of Control.
  - Integrity.
  - Confidentiality.
  - Other Models.
  - Open and Closed Systems.
- Documents and Guidelines.
  - The Rainbow Series.
  - The Red Book: Trusted Network Interpretation.
  - Information Technology Security Evaluation Criteria (ITSEC).
  - Common Criteria.
  - British Standard 7799.
- System Validation.
  - Certification and Accreditation.
- Exam Prep Questions.
- Answers to Exam Prep Questions.
- Need to Know More?

## **6. Telecommunications and Network Security.**

- Introduction.
- Threats to Network Security.
  - DoS Attacks.
  - Disclosure Attacks.
  - Destruction, Alteration, or Theft.
- LANs and Their Components.
  - LAN Communication Protocols.
  - Network Topologies.
  - LAN Cabling.
  - 802.11 Wireless Networking.
  - Bluetooth.
- WANS and Their Components.
  - Packet Switching.
  - Circuit Switching.
- Network Models and Standards.
  - OSI Model.
  - TCP/IP.
- Network Equipment.
  - Hubs.
  - Bridges.
  - Switches.
  - Routers.
- Access Methods and Remote Connectivity.
  - Point-to-Point Protocol (PPP).
  - Password Authentication Protocol (PAP).
  - Virtual Private Networks (VPNs).
  - Remote Authentication Dial-in User Service (RADIUS).
  - Terminal Access Controller Access Control System (TACACS).
  - IPSec.
- Message Privacy.
  - PGP.
  - S/MIME.
  - Privacy Enhanced Mail (PEM).
- Network Access Controls.
  - Firewalls.
  - Demilitarized Zone (DMZ).

**BUY ONLINE FROM:** <http://www.itgovernance.co.uk/products/497>

Exam Prep Questions.  
Answers to Exam Prep Questions.  
Need to Know More?

## **7. Applications and Systems-Development Security.**

Introduction.  
Malicious Code.  
  Viruses and Worms.  
  Buffer Overflow.  
  Denial of Service (DoS).  
  Distributed Denial of Service (DDoS).  
  Malformed Input (SQL Injection).  
  Spyware.  
  Back Doors and Trapdoors.  
  Change Detection.  
Failure States.  
The System Development Life Cycle.  
  Project Initiation.  
  Development and Acquisition.  
  Acceptance Testing/Implementation.  
  Operations/Maintenance.  
  Disposal.  
Software-Development Methods.  
  The Waterfall Model.  
  The Spiral Model.  
  Joint Application Development (JAD).  
  Rapid Application Development (RAD).  
  Computer-Aided Software Engineering (CASE).  
Change Management.  
Programming Languages.  
  Object-Oriented Programming.  
  CORBA.  
Database Management.  
  Transaction Processing.  
  Database Terms.  
  Data Warehousing.  
  Data Mining.  
  Knowledge Management.  
Exam Prep Questions.  
Answers to Exam Prep Questions.  
Need to Know More?

## **8. Operations Security.**

Introduction.  
Hack Attacks.  
  Common Attack Methodologies.  
  Phreakers and Their Targets.  
Operational Security.  
  New-Hire Orientation.  
  Separation of Duties.  
  Job Rotation.  
  Least Privilege.  
  Mandatory Vacations.  
  Termination.

**BUY ONLINE FROM:** <http://www.itgovernance.co.uk/products/497>

- Auditing and Monitoring.
  - Auditing.
  - Clipping Levels.
  - Intrusion Detection.
  - Keystroke Monitoring.
  - Facility Access Control.
- Categories of Control.
- Fax Control.
- Ethical Hacking.
  - Penetration Testing.
- Contingency Planning, Backup, and Recovery.
  - RAID.
  - Backups.
- Exam Prep Questions.
- Answers to Exam Prep Questions.
- Need to Know More?

## **9. Business Continuity Planning.**

- Introduction.
- The Risks of Poor Business Planning.
- Business Continuity Management.
- Business Continuity Plan (BCP).
  - Project Management and Initiation.
  - Business Impact Analysis (BIA).
  - Recovery Strategy.
  - Plan Design and Development.
  - Testing, Maintenance, Awareness, and Training.
- Disaster Recovery Planning (DRP).
  - Alternative Sites and Hardware Backup.
  - Software Backups.
- Exam Prep Questions.
- Answers to Exam Prep Questions.
- Need to Know More?

## **10. Law, Investigations, and Ethics.**

- Introduction.
- Computer Crimes.
  - Software Piracy.
  - Terrorism.
  - Pornography.
- Common Attacks.
  - Keystroke Logging.
  - Wiretapping.
  - Spoofing Attacks.
  - Manipulation Attacks.
  - Social Engineering.
  - Dumpster Diving.
- Ethics.
  - ISC2 Code of Ethics.
  - Computer Ethics Institute.
  - Internet Activities Board.
- International Property Laws.
  - Privacy Laws.
- Parameters of Investigation.

**BUY ONLINE FROM:** <http://www.itgovernance.co.uk/products/497>

- Computer Crime Investigation.
- Incident-Response Procedures.
- Incident-Response Team.
- Forensics.
  - Handling Evidence.
  - Drive Wiping.
  - Standardization of Forensic Procedures.
- Major Legal Systems.
  - Evidence Types.
  - Trial.
- Exam Prep Questions.
- Answers to Exam Prep Questions.
- Need to Know More?

## **11. Cryptography.**

- Introduction.
- Cryptographic Basics.
- History of Encryption.
- Symmetric Encryption.
  - Data Encryption Standard (DES).
  - Triple-DES (3DES).
  - Advanced Encryption Standard (AES).
  - International Data Encryption Algorithm (IDEA).
  - Other Symmetric Algorithms.
- Asymmetric Encryption.
  - RSA.
  - Diffie-Hellman.
  - El Gamal.
  - Elliptical Curve Cryptosystem (ECC).
  - Merkle-Hellman Knapsack.
- Integrity and Authentication.
  - Message Digests.
  - MD Series.
  - Digital Signatures.
- Steganography.
- Public Key Infrastructure (PKI).
  - Certificate Authority (CA).
  - Registration Authority (RA).
  - Certificate Revocation List (CRL).
  - Digital Certificates.
  - The Client's Role in PKI.
- Cryptographic Services.
  - Secure Email.
  - Secure TCP/IP Protocols.
- Cryptographic Attacks.
- Exam Prep Questions.
- Answers to Exam Prep Questions.
- Need to Know More?

## **12. Practice Exam 1.**

- Practice Exam Questions.

**BUY ONLINE FROM:** <http://www.itgovernance.co.uk/products/497>

### **13. Answers to Practice Exam 1.**

Answer Key.  
Answers to Practice Exam Questions.

### **14. Practice Exam 2.**

Practice Exam Questions.

### **15. Answers to Practice Exam 2.**

Answer Key.  
Answers to Practice Exam Questions.

### Appendix A: What's on the CD.

Multiple Test Modes.

Study Mode.

Certification Mode.

Custom Mode.

Adaptive Mode.

Missed Question Mode.

Non-Duplicate Mode.

Question Types.

Random Questions and Order of Answers.

Detailed Explanations of Correct and Incorrect Answers.

Attention to Exam Objectives.

Installing the CD.

Creating a Shortcut to the MeasureUp Practice Tests.

Technical Support.

Glossary.

Index.