Certified Tech Trainers CISSP™ Certification Preparation

Content Outline

- ***Security Domain: Security Management Practices***
  - **Security Management**
  - **Security management Responsibilities**
  - **Security Administration and Supporting Controls**
  - **Fundamental Principles of Security**
    - **Confidentiality**
    - **Integrity**
    - **Availability**
  - **Security Definitions**
  - **The Top-Down Approach**
  - **Organizational Security Model**
  - **Business Requirements – Private Industry versus Military Organizations**
  - **Risk Management**
  - **Risk Analysis**
    - **Risk Analysis Team**
    - **Value of Information and Assets**
    - **Costs That Make Up the Value**
    - **Identifying Threats**
    - **Quantitative Approach**
    - **Analysis Inputs and Data Gathering**
    - **Automated Risk Analysis Methods**
    - **Steps of a Risk Analysis**
    - **Results of a Risk Analysis**
    - **Qualitative Risk Analysis**

- **Quantitative versus Qualitative**
- **Protection Mechanisms**
- **Putting It Together**
- **Total Risk versus Residual Risk**
- **Handling Risk**

➢ **Policies, Procedures, Standards, and Guidelines**

- **Security Policy**
- **Standards**
- **Baselines**
- **Guidelines**
- **Procedures**
- **Implementation**

➢ **Data Classification**

- **Private Business versus Military Classifications**

➢ **Layers of Responsibility**

- **Data Owner**
- **Data Custodian**
- **User**
- **Personnel**
- **Structure**

➢ **Hiring Practices**

- **Operations**
- **Termination**

➢ **Security Awareness**

Content Outline

- **Summary**
- **Quick Tips**
  - **Questions & Answers**

- ***Security Domain: Access Control***
- ***Access Control***
- ***Security Principles***
  - **Confidentiality**
  - **Integrity**
  - **Availability**
- ***Identification, Authentication, Authorization, and Accountability***
  - **Identification**
  - **Authentication**
  - **Authorization**
  - **Single Sign-On**
- ***Access Control Models***
  - **Discretionary**
  - **Sensitivity Labels**
  - **Role-Based**
- ***Access Control Techniques and Technologies***
  - **Role-Based Access Control**
  - **Rule-Based Access Control**
  - **Restricted Interfaces**
  - **Access Control Matrix**
  - **Capability Tables**

Content Outline

- **Access Control Lists**
- **Content-Dependent Access Control**

- ***Access Control Administration***
  - **Centralized**
  - **Decentralized and Distributed Access Administration**
- ***Access Control Methods***
  - **Access Control Layers**
  - **Administrative**
  - **Physical Controls**
  - **Technical Controls**
  - **Administrative Controls**
  - **Physical Controls**
  - **Logical Controls**
- ***Access Control Types***
  - **Accountability**
- ***Access Control Practices***
  - **Unauthorized Disclosure of Information**
- ***Access Control Monitoring***
  - **Intrusion Detection**
- ***A Few Threats to Access Control***
  - **Dictionary Attack**
  - **Brute Force Attack**
  - **Spoofing at Login**
- ***Summary***

Content Outline

- ***Quick Tips***
  - **Questions & Answers**
- ***Security Domain: Security Models and Architecture***
  - **Security Models and Architecture**
  - **Computer Architecture**
    - **Central Processing Unit**
    - **Memory**
    - **CPU Modes and Protection Rings**
    - **Operating States**
    - **Multithreading, Multitasking, and Multiprocessing**
    - **Input/Output Device Management**
    - **Tying It Together**
  - **System Architecture**
    - **Defined Subset of Subjects and Objects**
    - **Trusted Computing Base**
    - **Security Perimeter**
    - **Reference Monitor and Security Kernel**
    - **Domains**
    - **Resource Isolation**
    - **Security Policy**
    - **Least Privilege**
    - **Layering, Data Hiding, and Abstraction**
  - **Security Models**
    - **State Machine Models**

- **Bell-LaPadula Model**
- **Biba**
- **Clark-Wilson Model**
- **Information Flow Model**
- **Noninterference Model**

➢ **Security Modes of Operation**

- **Dedicated Security Mode**
- **System-High Security Mode**
- **Compartmented Security Mode**
- **Multilevel Security Mode**
- **Trust and Assurance**

➢ **Systems Evaluation Methods**

➢ **The Orange Book**

- **Division D – Minimal Protection**
- **Division C – Discretionary Protection**
- **Division B – Mandatory Protection**
- **Division A – Verified Protection**

➢ **Rainbow Series**

- **Red Book**

➢ **Information Technology Security Evaluation Criteria**

➢ **Common Criteria**

➢ **Certification versus Accreditation**

- **Certification**
- **Accreditation**

- **Open versus Closed Systems**
  - **Open Systems**
  - **Closed Systems**
- **A Few Threats to Security Models and Architectures**
  - **Covert Channels**
  - **Countermeasures**
  - **Back Doors**
  - **Timing Issues**
  - **Buffer Overflows**
- **Summary**
- **Quick Tips**
  - **Questions & Answers**

- ***Security Domain: Physical Security***
  - **Physical Security**
  - **Planning Process**
  - **Facilities Management**
    - **Physical Attributes of the Facility**
    - **Construction**
    - **Facility Components**
    - **Computer and Equipment Rooms**
  - **Physical Security Risks**
  - **Physical Security Component Selection Process**
    - **Security Musts**
    - **Security Shoulds**

- **Backups**

➢ **Environmental Issues**

- **Ventilation**
- **Fire Prevention, Detection, and Suppression**
- **Types of Fire Detection**
- **Fire Suppression**

➢ **Administrative Controls**

- **Emergency Response and Reactions**

➢ **Perimeter Security**

- **Facility Access Control**
- **Personnel Access Controls**
- **External Boundary Protection Mechanisms**
- **Intrusion Detection Systems**

➢ **Summary**

➢ **Quick Tips**

- **Questions & Answers**

❖ ***Security Domain: Telecommunications and Networking Security***

➢ **Telecommunications and Network Security**

➢ **Open System Interconnect Model**

- **Application Layer**
- **Presentation Layer**
- **Session Layer**
- **Transport Layer**
- **Network Layer**

- **Data Link Layer**
- **Physical Layer**
- **Tying the Layers Together**

- **TCP/IP**
  - **Data Structures**
  - **IP Addressing**
- **Networking**
  - **LAN Media Access Technologies**
  - **Cabling**
  - **Cabling Problems**
- **Types of Transmission**
  - **Analog and Digital**
  - **Asynchronous and Synchronous**
  - **Broadband and Baseband**
  - **LAN Transmission Methods**
- **Network Topology**
  - **Ring Topology**
  - **Bus Topology**
  - **Star Topology**
  - **Mesh Topology**
- **LAN Media Access Technologies**
  - **Token Passing**
  - **CSMA**
  - **Collision Domains**

- **Polling**

- **Protocols**
  - **Address Resolution Protocol**
  - **Reverse Address Resolution Protocol**
  - **Internet Control Message Protocol**
- **Networking Devices**
  - **Repeaters**
  - **Bridges**
  - **Forwarding Tables**
  - **Routers**
  - **Routing**
  - **Switches**
  - **VLAN**
  - **Brouters**
  - **Gateways**
  - **PBX**
  - **Firewalls**
- **Network Segregation and Isolation**
- **Networking Services**
  - **Network Operating Systems**
  - **DNS**
  - **Internet DNS and Domains**
  - **Directory Services**
- **Intranets and Extranets**

- **Private IP Addresses**
- **Network Address Translation**

- **Metropolitan Area Network**
- **Wide Area Network**
  - **Telecommunications Evolution**
  - **Dedicated Links**
  - **T-carriers**
  - **S/WAN**
  - **WAN Technologies**
  - **Multiservice Access**
- **Remote Access**
  - **Dial-Up and RAS**
  - **ISDN**
  - **DSL**
  - **Cable Modems**
  - **VPN**
  - **Tunneling Protocols**
- **Network and Resource Availability**
  - **Single Points of Failure**
  - **RAID**
  - **Clustering**
  - **Backups**
- **Wireless Technologies**
  - **Wireless Communications**

- **Wireless Personal Area Network**

- **Summary**
- **Quick Tips**
  - **Questions & Answers**

- ***Security Domain: Cryptography***
  - **Cryptography**
  - **History of Cryptography**
  - **Cryptography Definitions**
  - **Strength of Cryptosystem**
  - **Goals of Cryptosystems**
  - **Types of Ciphers**
    - **Substitution Cipher**
    - **Transposition Cipher**
    - **Running and Concealment Ciphers**
  - **Steganography**
  - **The Government's Involvement with Cryptography**
    - **Clipper Chip**
    - **Key Escrow**
  - **Methods of Encryption**
    - **Symmetric versus Asymmetric Algorithms**
    - **Stream and Block Ciphers**
    - **Types of Symmetric Systems**
    - **Asymmetric Encryption Algorithms**
    - **Hybrid Encryption Methods**

Content Outline

- **Public Key Infrastructure (PKI)**
  - **Certificate Authorities**
  - **Certificates**
  - **Registration Authority**
  - **PKI Steps**
- **One-Way Function**
- **Message Integrity**
  - **One-Way Hash**
  - **Digital Signatures**
  - **Digital Signature Standard (DSS)**
  - **Different Hashing Algorithms**
  - **Attacks Against One-Way Hash Functions**
  - **One-Time Pad**
- **Key Management**
  - **Key Management Principles**
- **Link versus End-to-End Encryption**
  - **Hardware versus Software Cryptography Systems**
- **E-mail Standards**
  - **Privacy-Enhanced Mail**
  - **Message Security Protocol**
  - **Pretty Good Privacy (PGP)**
- **Internet Security**
  - **Start with the Basics**
- **Attacks**

- **Ciphertext-Only Attack**
- **Known-Plaintext Attack**
- **Chosen-Plaintext Attack**
- **Chosen-Ciphertext Attack**
- **Man-in-the-Middle Attack**
- **Dictionary Attacks**
- **Replay Attack**

➢ **Summary**

➢ **Quick Tips**

- **Questions & Answers**

❖ ***Security Domain: Disaster Recovery and Business Continuity***

➢ **Business Continuity and Disaster Recovery**

➢ **Make It Part of the Security Policy and Program**

➢ **Business Impact Analysis**

- **Interdependencies**

➢ **Contingency Planning Requirements**

- **Developing Goals for Contingency Plans**
- **Developing the Team**
- **Enterprisewide**
- **Plan Development**
- **Identifying Business Critical Functions**
- **Identifying the Resources and Systems That Support the Critical Functions**
- **Estimating Potential Disasters**
- **Selecting Planning Strategies**

- **Implementing Strategies**
- **Testing and Revising the Plan**

- **End-User Environment**
- **Backup Alternatives**
  - **Hardware Backup**
  - **Software Backup**
- **Choosing a Software Backup Facility**
  - **Documentation**
- **Recovery and Restoration**
  - **Testing and Drills**
  - **Checklist Test**
  - **Structured Walk-Through Test**
  - **Simulation Test**
  - **Parallel Test**
  - **Other Types of Training**
- **Emergency Response**
- **Summary**
- **Quick Tips**
  - **Questions**
  - **Answers**

- ***Security Domain: Law, Investigation, and Ethics***
  - **Laws, Investigation, and Ethics**
  - **Ethics**
    - **Code of Ethics Summary**

- **Computer Ethics Institute**
- **Internet Activities Board**
- **Generally Accepted System Security Principles (GASSP)**
- **Motivations, Opportunities, and Means**

- **Hackers and Crackers**
  - **Operations Security**
  - **Dumpster Diving**
  - **Emanations Capturing**
  - **Wiretapping**
  - **Social Engineering**
  - **Masquerading**
- **Well-Known Computer Crimes**
  - **Cuckoo's Egg**
  - **Kevin Mitnick**
  - **Chaos Computer Club**
  - **Cult of the Dead Cow**
  - **Phone Phreakers**
- **Identification, Protection, and Prosecution**
- **Liability and Its Ramifications**
  - **Personal Information**
  - **Hacker Intrusion**
- **Types of Laws**
  - **Intellectual Property Laws**
- **Discarding Equipment and Software Issues**

Content Outline

- **Computer Crime Investigations**
  - **A Different Approach**
  - **Computer Forensics and Proper Collection of Evidence**
  - **Incident Handling**
  - **What Is Admissible in Court?**
  - **Surveillance, Search, and Seizure**
  - **Interviewing and Interrogating**
- **Import and Export Laws**
- **Privacy**
- **Laws, Directives, and Regulations**
  - **Health Insurance Portability and Accountability Act (HIPPA)**
  - **Gramm Leach Bliley Act of 1999**
  - **Computer Fraud and Abuse Act**
  - **Federal Privacy Act of 1974**
  - **Computer Security Act of 1987**
  - **Security and Freedom Through Encryption Act**
  - **Federal Sentencing Guidelines**
  - **Economic Espionage Act of 1996**
- **International Cooperation Efforts**
  - **G8**
  - **Interpol**
  - **European Union**
- **Summary**
- **Quick Tips**

- **Questions & Answers**

❖ ***Security Domain: Application and System Development***

- **Applications and System Development**
- **Device versus Software Security**
- **Different Environments Demand Different Security**
  - **E-Commerce**
  - **Client/Server Model**
- **Environment versus Application Controls**
- **Complexity of Functionality**
- **Data Types, Format, and Length**
- **Implementation and Default Issues**
  - **Implementation**
- **Failure States**
- **Database Management**
  - **Database Management Software**
  - **Database Models**
  - **Relational Database Components**
  - **Data Dictionary**
  - **Integrity**
  - **Database Security Issues**
  - **Data Warehousing and Data Mining**
- **System Development**
  - **Management of Development**
  - **Life Cycle Phases**

- **System Design Specifications**
- **Change Control**

➢ **Application Development Methodology**

- **Object-Oriented Concepts**
- **Data Modeling**
- **Software Architecture**
- **Data Structures**
- **ORBs and COBRAs**
- **Computer-Aided Software Engineering (CASE)**
- **Prototyping**
- **COM and DCOM**
- **Open Database Connectivity (ODBC)**
- **Object Linking and Embedding (OLE)**
- **Dynamic Data Exchange**
- **Distributed Computing Environment**
- **Expert Systems and Knowledge-Based Systems**
- **Artificial Neural Networks**
- **Java**
- **ActiveX**
- **Malicious Code**
- **Attacks**

➢ **Summary**

➢ **Quick Tips**

- **Questions & Answers**

Content Outline

- ***Security Domain: Operations Security***
  - **Operational Security**
    - **Administrative Management**
    - **Accountability**
    - **Security Operations and Product Evaluation**
    - **Input and Output Controls**
  - **Electronic Mail Security**
    - **Facsimile Security**
    - **Hack and Attack Methods**
    - **Operations Department**
  - **Summary**
  - **Quick Tips**
    - **Questions & Answers**