

Certified Information Systems Security Officer Course Summary

Description

The 5-day CISSO course is designed for a forward-thinking security professional or consultant that manages or plays a key role in an organization's information security department.

The CISSO addresses the broad range of industry best practices, knowledge and skills expected of a security leader. The Candidate will learn both the theory and the requirements for practical implementation of core security concepts, practices, monitoring and compliance. Through the use of a risk-based approach the CISSO is able to implement and maintain cost-effective security controls that are closely aligned with business requirements.

Mile2's C)ISSO, a Dual Initiative between the DOD and DND: CANCUS CDISM MOU – ID#1974100118.

Certification

- Certified ISSO - Information Systems Security Officer
- Mile2 Exam is included and can be taken any time after the course
- Format: Online, 100 questions
- Covers CISSP® exam requirements
- Covers CISM® exam requirement

Topics

- Risk Management
- Security Management
- Authentication
- Access Control
- Security Models and Evaluation Criteria
- Operations Security
- Symmetric Cryptography and Hashing
- Asymmetric Cryptography and PKI
- Network Connections
- Network Protocols and Devices
- Telephony, VPNs and Wireless
- Security Architecture and Attacks
- Software Development Security
- Database Security and System Development
- Malware and Software Attacks
- Business Continuity
- Disaster Recovery
- Incident Management, Law, and Ethics
- Physical Security

Audience

This course is designed for a forward-thinking security professional or consultant that manages or plays a key role in an organization's information security department.

Prerequisites

Experience in at least 2 modules of the outline is beneficial but not required

Duration

Five days

Certified Information Systems Security Officer

Course Outline

I. Risk Management

- A. What Is the Value of an Asset?
- B. What Is a Threat Source/Agent?
- C. What Is a Threat?
- D. What Is a Vulnerability?
- E. Examples of Some Vulnerabilities that Are Not Always Obvious
- F. What Is a Control?
- G. What Is Likelihood?
- H. What Is Impact?
- I. Control Effectiveness
- J. Risk Management
- K. Purpose of Risk Management
- L. Risk Assessment
- M. Why Is Risk Assessment Difficult?
- N. Types of Risk Assessment
- O. Different Approaches to Analysis
- P. Quantitative Analysis
- Q. ALE Values Uses
- R. Qualitative Analysis - Likelihood
- S. Qualitative Analysis - Impact
- T. Qualitative Analysis – Risk Level
- U. Qualitative Analysis Steps
- V. Management's Response to Identified Risks
- W. Comparing Cost and Benefit
- X. Cost of a Countermeasure

II. Security Management

- A. Enterprise Security Program
- B. Building A Foundation
- C. Planning Horizon Components
- D. Enterprise Security – The Business Requirements
- E. Enterprise Security Program Components
- F. Control Types
- G. "Soft" Controls
- H. Technical or Logical Controls
- I. Physical Controls
- J. Security Roadmap
- K. Senior Management's Role in Security
- L. Negligence and Liability
- M. Security Roles and Responsibilities
- N. Security Program Components
- O. Security and the Human Factors
- P. Employee Management
- Q. Human Resources Issues
- R. Importance to Security?
- S. Recruitment Issues
- T. Termination of Employment
- U. Informing Employees
- V. About Security

- W. Enforcement
- X. Security Enforcement Issues

III. Authentication

- A. Agenda
- B. Access Control Methodology
- C. Access Control Administration
- D. Accountability and Access Control
- E. Trusted Path
- F. Who Are You?
- G. Authentication Mechanisms
- H. Strong Authentication
- I. Authorization
- J. Access Criteria
- K. Fraud Controls
- L. Access Control Mechanisms
- M. Agenda
- N. Biometrics Technology
- O. Biometrics Enrollment Process
- P. Downfalls to Biometric Use
- Q. Biometrics Error Types
- R. Biometrics Diagram
- S. Biometric System Types
- T. Agenda
- U. Passwords and PINs
- V. Password "Shoulds"
- W. Password Attacks
- X. Countermeasures for Password Cracking
- Y. Cognitive Passwords
- Z. One-Time Password Authentication
- AA. Agenda
- BB. Synchronous Token
- CC. Asynchronous Token Device
- DD. Cryptographic Keys
- EE. Passphrase Authentication
- FF. Memory Cards
- GG. Smart Card
- HH. Agenda
- II. Single Sign-on Technology
- JJ. Different Technologies
- KK. Scripts as a Single Sign-on Technology
- LL. Directory Services as a Single Sign-on Technology
- MM. Thin Clients
- NN. Kerberos as a Single Sign-on Technology
- OO. Tickets
- PP. Kerberos Components Working Together
- QQ. Major Components of Kerberos
- RR. Kerberos Authentication Steps
- SS. Why Go Through All of this Trouble?
- TT. Issues Pertaining to Kerberos

Certified Information Systems Security Officer

Course Outline (cont'd)

- UU. SESAME as a Single Sign-on Technology
- VV. Federated Authentication
- WW. Agenda
- XX. IDS
- YY. Network IDS Sensors
- ZZ. Types of IDSs
- AAA. Behavior-Based IDS
- BBB. IDS Response Mechanisms
- CCC. IDS Issues
- DDD. Trapping an Intruder

IV. Access Control

- A. Role of Access Control
- B. Definitions
- C. More Definitions
- D. Layers of Access Control
- E. Layers of Access Controls
- F. Access Control Mechanism Examples
- G. Access Control Characteristics
- H. Preventive Control Types
- I. Control Combinations
- J. Administrative Controls
- K. Controlling Access
- L. Other Ways of Controlling Access
- M. Technical Access Controls
- N. Physical Access Controls
- O. Accountability
- P. Information Classification
- Q. Information Classification Criteria
- R. Declassifying Information
- S. Types of Classification Levels
- T. Models for Access
- U. Discretionary Access Control Model
- V. Enforcing a DAC Policy
- W. Mandatory Access Control Model
- X. MAC Enforcement Mechanism – Labels
- Y. Where Are They Used?
- Z. Role-Based Access Control (RBAC)
- AA. Acquiring Rights and Permissions
- BB. Rule-Based Access Control
- CC. Access Control Matrix
- DD. Access Control Administration
- EE. Access Control Methods
- FF. Remote Centralized Administration
- GG. RADIUS Characteristics
- HH. RADIUS
- II. TACACS+ Characteristics
- JJ. Diameter Characteristics
- KK. Decentralized Access
- LL. Control Administration

V. Security Models and Evaluation Criteria

- A. System Protection – Trusted Computing Base
- B. System Protection– Reference Monitor
- C. Security Kernel Requirements
- D. Security Modes of Operation
- E. System Protection– Levels of Trust
- F. System Protection– Process Isolation
- G. System Protection – Layering
- H. System Protection - Application Program Interface
- I. System Protection- Protection Rings
- J. What Does It Mean to Be in a Specific Ring?
- K. Security Models
- L. State Machine
- M. Information Flow
- N. Bell-LaPadula
- O. Rules of Bell-LaPadula
- P. Biba
- Q. Clark-Wilson Model
- R. Non-interference Model
- S. Brewer and Nash – Chinese Wall
- T. Take-Grant Model
- U. Trusted Computer System Evaluation Criteria (TCSEC)
- V. TCSEC Rating Breakdown
- W. Evaluation Criteria - ITSEC
- X. ITSEC Ratings
- Y. ITSEC – Good and Bad
- Z. Common Criteria
- AA. Common Criteria Components
- BB. First Set of Requirements
- CC. Second Set of Requirements
- DD. Package Ratings
- EE. Common Criteria Outline
- FF. Certification vs. Accreditation

VI. Operations Security

- A. Operations Issues
- B. Role of Operations
- C. Administrator Access
- D. Computer Operations – Systems Administrators
- E. Security Administrator
- F. Operational Assurance
- G. Audit and Compliance
- H. Some Threats to Computer Operations
- I. Specific Operations Tasks
- J. Product Implementation Concerns
- K. Logs and Monitoring
- L. Records Management
- M. Change Control
- N. Resource Protection

Certified Information Systems Security Officer

Course Outline (cont'd)

- O. Contingency Planning
- P. System Controls
- Q. Trusted Recovery
- R. Fault-Tolerance Mechanisms
- S. Duplexing, Mirroring, Check Pointing
- T. Redundant Array of Independent Disks (RAID)
- U. Fault Tolerance
- V. Redundancy Mechanism
- W. Backups
- X. Backup Types
- Y. Remote Access
- Z. Facsimile Security
- AA. Email Security
- BB. Before Carrying Out Vulnerability Testing
- CC. Vulnerability Assessments
- DD. Methodology
- EE. Penetration Testing
- FF. Penetration Testing
- GG. Hack and Attack Strategies
- HH. Protection Mechanism – Honeypot
- II. Threats to Operations
- JJ. Data Leakage – Social Engineering
- KK. Data Leakage – Object Reuse
- LL. Object Reuse
- MM. Why Not Just Delete File or Format the Disk?
- NN. Data Leakage – Keystroke Logging
- OO. Data Leakage – Emanation
- PP. Controlling Data Leakage – TEMPEST
- QQ. Controlling Data Leakage – Control Zone
- RR. Controlling Data Leakage – White Noise
- SS. Summary

VII. Symmetric Cryptography and Hashing

- A. Cryptography Objectives
- B. Cryptographic Definitions
- C. A Few More Definitions
- D. Need Some More Definitions?
- E. Symmetric Cryptography – Use of Secret Keys
- F. Cryptography Uses Yesterday and Today
- G. Historical Uses of Symmetric Cryptography
- H. Historical Uses of Symmetric Cryptography – Scytale Cipher
- I. Historical Uses of Symmetric Cryptography: Substitution Cipher
- J. Caesar Cipher Example
- K. Historical Uses of Symmetric Cryptography: Vigenere Cipher
- L. Polyalphabetic Substitution
- M. Vigenere Table Example
- N. Example Continued

- O. Historical Uses of Symmetric Cryptography: Enigma Machine
- P. Historical Uses of Symmetric Cryptography: Vernam Cipher
- Q. Historical Uses of Symmetric Cryptography: Running Key and Concealment
- R. One-Time Pad Characteristics
- S. Binary Mathematical Function
- T. Key and Algorithm Relationship
- U. Why Does a 128-Bit Key Provide More Protection than a 64-Bit Key?
- V. Ways of Breaking Cryptosystems – Brute Force
- W. Ways of Breaking Cryptosystems – Frequency Analysis
- X. Determining Strength in a Cryptosystem
- Y. Characteristics of Strong Algorithms
- Z. Open or Closed More Secure?
- AA. Types of Ciphers Used Today
- BB. Encryption/Decryption Methods
- CC. Type of Symmetric Cipher – Block Cipher
- DD. S-Boxes Used in Block Ciphers
- EE. Type of Symmetric Cipher – Stream Cipher
- FF. Encryption Process
- GG. Symmetric Characteristics
- HH. Sender and Receiver Must Generate the Same Keystream
 - II. They both must have the same key and IV
- JJ. Strength of a Stream Cipher
- KK. Let's Dive in Deeper
- LL. Symmetric Key Cryptography
- MM. Symmetric Key Management Issue
- NN. Symmetric Algorithm Examples
- OO. Symmetric Downfalls
- PP. Secret Versus Session Keys
- QQ. Symmetric Ciphers We Will Dive Into
- RR. Symmetric Algorithms – DES
- SS. Evolution of DES
- TT. Block Cipher Modes – CBC
- UU. Different Modes of Block Ciphers – ECB
- VV. Block Cipher Modes – CFB and OFB
- WW. CFB and OFB Modes
- XX. Symmetric Cipher – AES
- YY. Other Symmetric Algorithms
- ZZ. Hashing Algorithms
- AAA. Protecting the Integrity of Data
- BBB. Data Integrity Mechanisms
- CCC. Weakness in Using Only Hash Algorithms
- DDD. More Protection in Data Integrity
- EEE. MAC – Sender
- FFF. MAC – Receiver
- GGG. Security Issues in Hashing

Certified Information Systems Security Officer

Course Outline (cont'd)

- HHH. Birthday Attack
- III. Example of a Birthday Attack

VIII. Asymmetric Cryptography and PKI

- A. Asymmetric Cryptography
- B. Public Key Cryptography Advantages
- C. Asymmetric Algorithm Disadvantages
- D. Symmetric versus Asymmetric
- E. Asymmetric
- F. Asymmetric Algorithm – Diffie-Hellman
- G. Asymmetric Algorithm – RSA
- H. Asymmetric Algorithms – El Gamal and ECC
- I. Example of Hybrid Cryptography
- J. When to Use Which Key
- K. Using the Algorithm Types Together
- L. Digital Signatures
- M. Digital Signature and MAC Comparison
- N. What if You Need All of the Services?
- O. U.S. Government Standard
- P. Why Do We Need a PKI?
- Q. PKI and Its Components
- R. CA and RA Roles
- S. Let's Walk Through an Example
- T. Digital Certificates
- U. What Do You Do with a Certificate?
- V. Components of PKI – Repository and CRLs
- W. Steganography
- X. Key Management
- Y. Link versus End-to-End Encryption
- Z. End-to-End Encryption
- AA. E-mail Standards
- BB. Encrypted message
- CC. Secure Protocols
- DD. SSL and the OSI Model
- EE. SSL Hybrid Encryption
- FF. SSL Connection Setup
- GG. Secure E-mail Standard
- HH. SSH Security Protocol
- II. Network Layer Protection
- JJ. IPSec Key Management
- KK. Key Issues Within IPSec
- LL. IPSec Handshaking Process
- MM. SAs in Use
- NN. IPSec Is a Suite of Protocols
- OO. IPSec Modes of Operation
- PP. IPsec Modes of Operation
- QQ. Attacks on Cryptosystems
- RR. More Attacks

IX. Network Connections

- A. Network Topologies– Physical Layer

- B. Topology Type – Bus
- C. Topology Type – Ring
- D. Topology Type – Star
- E. Network Topologies – Mesh
- F. Summary of Topologies
- G. LAN Media Access Technologies
- H. One Goal of Media Access Technologies
- I. Transmission Types – Analog and Digital
- J. Transmission Types – Synchronous and Asynchronous
- K. Transmission Types – Baseband and Broadband
- L. Two Types of Carrier Sense Multiple Access
- M. Transmission Types– Number of Receivers
- N. Media Access Technologies - Ethernet
- O. Media Access Technologies – Token Passing
- P. Media Access Technologies – Polling
- Q. Cabling
- R. Signal and Cable Issues
- S. Cabling Types – Coaxial
- T. Cabling Types – Twisted Pair
- U. Types of Cabling – Fiber
- V. Cabling Issues – Plenum-Rated
- W. Types of Networks
- X. Network Technologies
- Y. Network Technologies
- Z. Network Configurations
- AA. MAN Technologies – SONET
- BB. Wide Area Network Technologies
- CC. WAN Technologies Are Circuit or Packet Switched
- DD. WAN Technologies – ISDN
- EE. ISDN Service Types
- FF. WAN Technologies – DSL
- GG. WAN Technologies– Cable Modem
- HH. WAN Technologies– Packet Switched
- II. WAN Technologies – X.25
- JJ. WAN Technologies – Frame Relay
- KK. WAN Technologies – ATM
- LL. Multiplexing

X. Network Protocols and Devices

- A. OSI Model
- B. An Older Model
- C. Data Encapsulation
- D. OSI – Application Layer
- E. OSI – Presentation Layer
- F. OSI – Session Layer
- G. Transport Layer
- H. OSI – Network Layer
- I. OSI – Data Link
- J. OSI – Physical Layer
- K. Protocols at Each Layer

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Certified Information Systems Security Officer**Course Outline (cont'd)**

- L. Devices Work at Different Layers
 - M. Networking Devices
 - N. Repeater
 - O. Hub
 - P. Bridge
 - Q. Switch
 - R. Virtual LAN
 - S. Router
 - T. Gateway
 - U. Bastion Host
 - V. Firewalls
 - W. Firewall – First line of defense
 - X. Firewall Types – Packet Filtering
 - Y. Firewall Types – Proxy Firewalls
 - Z. Firewall Types – Circuit-Level Proxy Firewall
 - AA. Type of Circuit- Level Proxy – SOCKS
 - BB. Firewall Types – Application-Layer Proxy
 - CC. Firewall Types – Stateful
 - DD. Firewall Types – Dynamic Packet-Filtering
 - EE. Firewall Types – Kernel Proxies
 - FF. Firewall Placement
 - GG. Firewall Architecture Types – Screened Host
 - HH. Firewall Architecture Types – Multi- or Dual-Homed
 - II. Firewall Architecture Types – Screened Subnet
 - JJ. IDS – Second line of defense
 - KK. IPS – Last line of defense?
 - LL. HIPS
 - MM. Unified Threat Management
 - NN. UMT Product Criteria
 - OO. Protocols
 - PP. TCP/IP Suite
 - QQ. Port and Protocol
 - RR. Relationship
 - SS. Conceptual Use of Ports
 - TT. UDP versus TCP
 - UU. Protocols – ARP
 - VV. Protocols – ICMP
 - WW. Protocols – SNMP
 - XX. Protocols – SMTP
 - YY. Protocols – FTP, TFTP, Telnet
 - ZZ. Protocols – RARP and BootP
 - AAA. Network Service – DNS
 - BBB. Network Service – NAT
 - FF. Dial-Up Protocol – PPP
 - G. Authentication Protocols – PAP and CHAP
 - H. Authentication Protocol – EAP
 - I. Voice Over IP
 - J. Private Branch Exchange
 - K. PBX Vulnerabilities
 - L. PBX Best Practices
 - M. Virtual Private
 - N. Network Technologies
 - O. What Is a Tunnelling Protocol?
 - P. Tunnelling Protocols – PPTP
 - Q. Tunnelling Protocols – L2TP
 - R. Tunnelling Protocols – IPsec
 - S. IPsec - Network Layer Protection
 - T. IPsec
 - U. IPsec
 - V. SSL/TLS
 - W. Wireless Technologies– Access Point
 - X. Standards Comparison
 - Y. Wireless Network Topologies
 - Z. Wi-Fi Network Types
 - AA. Wireless Technologies – Access Point
 - BB. Wireless Technologies – Service Set ID
 - CC. Wireless Technologies – Authenticating to an AP
 - DD. Wireless Technologies – WEP
 - EE. WEP
 - FF. Wireless Technologies –
 - GG. More WEP Woes
 - HH. Weak IV Packets
 - II. More WEP Weaknesses
 - JJ. How WPA Improves on WEP
 - KK. How WPA Improves on WEP
 - LL. TKIP
 - MM. The WPA MIC Vulnerability
 - NN. 802.11i – WPA2
 - OO. WPA and WPA2 Mode Types
 - PP. WPA-PSK Encryption
 - QQ. Wireless Technologies – WAP
 - RR. Wireless Technologies – WTLS
 - SS. Wireless Technologies – Common Attacks
 - TT. Wireless Technologies – War Driving
 - UU. Kismet
 - VV. Wireless Technologies – Countermeasures
 - WW. Network Based Attacks
 - XX. ARP Attack
 - YY. DDoS Issues
 - ZZ. Man-in-the Middle
 - AAA. Traceroute Operation
- XI. Telephony, VPNs and Wireless**
- A. PSTN
 - B. Remote Access
 - C. Dial-Up Protocols and Authentication
 - D. Protocols
 - E. Dial-Up Protocol – SLIP

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Certified Information Systems Security Officer

Course Outline (cont'd)

XII. Security Architecture and Attacks

- A. ESA Definition...
- B. What is Architecture?
- C. Architecture Components
- D. Key Architecture Concepts - Plan
- E. Objectives of Security Architecture
- F. Technology Domain Modeling
- G. Integrated Security is Designed Security
- H. Security by Design
- I. Architectural Models
- J. Virtual Machines
- K. Cloud Computing
- L. Memory Types
- M. Virtual Memory
- N. Memory Management
- O. Accessing Memory Securely
- P. Different States that Processes Work In
- Q. System Functionality
- R. Types of Compromises
- S. Disclosing Data in an Unauthorized Manner
- T. Circumventing Access Controls
- U. Attacks
- V. Attack Type – Race Condition
- W. Attack Type - Data Validation
- X. Attacking Through Applications
- Y. How Buffers and Stacks Are Supposed to Work
- Z. How a Buffer Overflow Works
- AA. Attack Characteristics
- BB. Attack Types
- CC. More Attacks
- DD. Host Name Resolution Attacks
- EE. More Attacks (2)
- FF. Watching Network Traffic
- GG. Traffic Analysis
- HH. Cell Phone Cloning
- II. Illegal Activities

XIII. Software Development Security

- A. How Did We Get Here?
- B. Device vs. Software Security
- C. Why Are We Not Improving at a Higher Rate?
- D. Usual Trend of Dealing with Security
- E. Where to Implement Security
- F. The Objective
- G. Security of Embedded Systems
- H. Development Methodologies
- I. Maturity Models
- J. Security Issues
- K. OWASP Top Ten (2011)
- L. Modularity of Objects
- M. Object-Oriented Programming Characteristic

- N. Module Characteristics
- O. Linking Through COM
- P. Mobile Code with Active Content
- Q. World Wide Web OLE
- R. ActiveX Security
- S. Java and Applets
- T. Common Gateway Interface
- U. How CGI Scripts Work
- V. Cookies
- W. PCI Requirements
- X. Virtualization - Type 1
- Y. Virtualization – Type 2

XIV. Database Security and System Development

- A. Database Model
- B. Database Models – Hierarchical
- C. Database Models – Distributed
- D. Database Models – Relational
- E. Database Systems
- F. Database Models – Relational Components
- G. Foreign Key
- H. Database Component
- I. Database Security Mechanisms
- J. Database Data Integrity Controls
- K. Add-On Security
- L. Database Security Issues
- M. Controlling Access
- N. Database Integrity
- O. Data Warehousing
- P. Data Mining
- Q. Artificial Intelligence
- R. Expert System Components
- S. Artificial Neural Networks
- T. Software Development Models
- U. Project Development – Phases III, IV, and V
- V. Project Development–Phases VI and VII
- W. Verification versus Validation
- X. Evaluating the Resulting Product
- Y. Controlling How Changes Take Place
- Z. Change Control Process
- AA. Administrative Controls
- BB. Malware
- CC. Virus
- DD. More Malware
- EE. Rootkits and Backdoors
- FF. DDoS Attack Types
- GG. Escalation of Privilege
- HH. Protect against privilege escalation
- II. DDoS Issues
- JJ. DDoS
- KK. Buffer Overflow Definition

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Certified Information Systems Security Officer

Course Outline (cont'd)

- LL. Overflow Illustration
- MM. Mail Bombing
- NN. E-Mail Links
- OO. Phishing
- PP. Spear Phishing
- QQ. Replay Attack
- RR. Cross-Site Scripting Attack
- SS. Timing Attacks
- TT. More Advanced Attacks
- UU. Summary

XV. Malware and Software Attacks

- A. Malware
- B. Virus
- C. More Malware
- D. Rootkits and Backdoors
- E. DDoS Attack Types
- F. Escalation of Privilege
- G. DDoS Issues
- H. DDoS
- I. Buffer Overflow Definition
- J. Overflow Illustration
- K. Buffer Overflows
- L. Mail Bombing
- M. E-Mail Links
- N. Phishing
- O. Spear Phishing
- P. Replay Attack
- Q. Cross-Site Scripting Attack
- R. Timing Attacks
- S. More Advanced Attacks
- T. Summary

XVI. Business Continuity

- A. Phases of Plan
- B. Who Is Ready?
- C. Pieces of the BCP
- D. BCP Development
- E. Where Do We Start?
- F. Why Is BCP a Hard Sell to Management?
- G. Understanding the Organization
- H. Critical products and services
- I. Dependencies
- J. Supply chain
- K. Between departments
- L. Personnel
- M. Information
- N. Equipment
- O. Facilities
- P. BCP Committee
- Q. BCP Risk Analysis

- R. Identify Vulnerabilities and Threats
- S. Categories
- T. How to Identify the Most Critical Company Functions
- U. Loss Criteria
- V. Interdependencies
- W. Identifying Functions' Resources
- X. How Long Can the Company Be Without These Resources?
- Y. Calculating MTD
- Z. Recovery Point Objective
- AA. Calculation of maximum data loss
- BB. Determines backup strategy
- CC. Defines the most current state of data upon recovery
- DD. Recovery Strategies
- EE. Based on the results of the BIA
- FF. May be different for each department
- GG. Must be less than MTD
- HH. Sets the RTO
- II. What Items Need to Be Considered in a Recovery?
- JJ. Facility Backups – Hot Site
- KK. Facility Backups – Warm Site
- LL. Facility Backups – Cold Site
- MM. Compatibility Issues with Offsite Facility
- NN. Which Do We Use?
- OO. Choosing Offsite Services
- PP. Subscription Costs
- QQ. Choosing Site Location
- RR. Other Offsite Approaches
- SS. BCP Plans Commonly and Quickly Become Out of Date
- TT. Summary

XVII. Disaster Recovery

- A. Proper Planning
- B. Executive Succession Planning
- C. Preventing a Disaster
- D. Preventive Measures
- E. Backup/Redundancy Options
- F. Disk Shadowing
- G. Backing Up Over Telecommunication
- H. Serial Lines
- I. HSM
- J. SAN
- K. Co-Location
- L. Other Options
- M. Review - Results from the BIA
- N. Review - Results from
- O. Recovery Strategy
- P. Now What?

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Certified Information Systems Security Officer

Course Outline (cont'd)

- Q. Priorities
- R. Plan Objectives
- S. Defining Roles
- T. The Plan
- U. Recovery
- V. Return to Normal Operations
- W. Environment
- X. Operational Planning
- Y. Emergency Response
- Z. Reviewing Insurance
- AA. When Is the Danger Over?
- BB. Now What?
- CC. Testing and Drills
- DD. Types of Tests to Choose From
- EE. What Is Success?
- FF. Summary

XVIII. Incident Management, Law, and Ethics

- A. Seriousness of Computer Crimes
- B. Incidents
- C. Incident Management Priorities
- D. Incident Response Capability
- E. Incident Management Requires
- F. Preparing for a Crime Before It Happens
- G. Incident Response Phases
- H. Types of Law
- I. Foundational Concepts of Law
- J. Common Laws – Criminal
- K. Common Laws – Civil
- L. Common Laws – Administrative
- M. Intellectual Property Laws
- N. More Intellectual Property Laws
- O. Software Licensing
- P. Digital Millennium Copyright Act
- Q. Historic Examples of Computer Crimes
- R. Who Perpetrates These Crimes?
- S. The Evolving Threat
- T. Types of Motivation for Attacks
- U. A Few Attack Types
- V. Telephone Fraud
- W. Identification Protection & Prosecution
- X. Computer Crime and Its Barriers
- Y. Countries Working Together
- Z. Security Principles for International Use
- AA. Determine if a Crime Has Indeed Been Committed
- BB. When Should Law Enforcement Get Involved?
- CC. Citizen versus Law Enforcement Investigation
- DD. Investigation of Any Crime
- EE. Role of Evidence in a Trial
- FF. General Rules for Evidence
- GG. Evidence Requirements
- HH. Evidence Collection Topics
- II. Chain of Custody

- JJ. How Is Evidence Processed?
- KK. Evidence Types
- LL. Hearsay Rule Exception
- MM. Privacy of Sensitive Data
- NN. Privacy Issues – U.S. Laws as Examples
- OO. European Union Principles on Privacy
- PP. Routing Data Through Different Countries
- QQ. Employee Privacy Issues
- RR. Computer Forensics
- SS. Trying to Trap the Bad Guy
- TT. Companies Can Be Found Liable
- UU. Sets of Ethics
- VV. Ethics – mile2
- WW. Ethics – Computer Ethics Institute
- XX. Ethics – Internet Architecture Board
- YY. GAISP- Generally Accepted Information Security Principles

XIX. Physical Security

- A. Physical Security – Threats
- B. Different Types of Threats & Planning
- C. Facility Site Selection
- D. Facility Construction
- E. Devices Will Fail
- F. Controlling Access
- G. Possible Threats
- H. External Boundary Protection
- I. Lock Types
- J. Facility Access
- K. Piggybacking
- L. Securing Mobile Devices
- M. Entrance Protection
- N. Perimeter Protection – Fencing
- O. Perimeter Protection – Lighting
- P. Perimeter Security – Security Guards
- Q. Surveillance/Monitoring
- R. Types of Physical IDS
- S. Electro-Mechanical Sensors
- T. Volumetric Sensors
- U. Facility Attributes
- V. Electrical Power
- W. Problems with Steady Power Current
- X. Power Interference
- Y. Power Preventive Measures
- Z. Environmental Considerations
- AA. Fire Prevention
- BB. Automatic Detector Mechanisms
- CC. Fire Detection
- DD. Fire Types
- EE. Suppression Methods
- FF. Fire Extinguishers
- GG. Fire Suppression
- HH. Fire Extinguishers