

CISSP CBK REVIEW SEMINAR

Available Dates: **Request Dates**

Class Length: **5 day**

Cost: **\$2,495**

[Email Computer Visions about this class](#)

Class Outline:

Information Security and Risk Management
Introduction to (ISC)2 and the exam process
The AIC (availability, integrity, confidentiality) triad
Security awareness training and education
Risk mitigation, quantitative and qualitative risk assessment, countermeasure selection
Ethics: personal, corporate, professional
Access Control
Definitions
Need to know, least privilege, separation of duties
Information classification
Access control categories and types
Threats: external and internal, natural, man-made
Technologies: single sign on, Kerberos, temporal, biometrics
Assurance mechanisms: IDS, IPS, logs, audits
Cryptography
Key concepts
History: manual, mechanical, electronic, quantum systems
Encryption systems: stream cipher, block ciphers
Symmetric and asymmetric algorithms
Integrity controls
MD5
SHA-1
CBC-MAC
Digital signatures: DSS
Cryptographic systems: keys, recovery, PKI, trust models
Attacks: plaintext and ciphertext, slide, side channel
Physical Security
Definitions
Guards
Fences
Locks
Site location
The Layered Defense Model
Infrastructure support systems
Equipment protection: theft, damage
Security Architecture and Design
Components and principles
System security: zones, domains, ring-based protection
Hardware: CPU, memory, communications devices
Software: operating systems, utilities, applications
Security models and architecture theory
Bell LaPadula
Biba
Clark-Wilson
Integrity models
Security evaluation methods and criteria
Business Continuity Planning and Disaster Recovery Planning
Project scope development and planning
Business impact analysis
Emergency assessment: incident response, mitigation
Continuity and recovery strategy
Plan, design and development
Implementation: testing techniques, awareness

Restoration: rebuilding and return to normal
Plan management: updating
Telecommunications and Network Security
Central concepts
Analog vs. digital
Synchronous vs. asynchronous
Circuit vs. packet switched traffic
Networks:
LAN
WAN
DMZ
Internet
Remote access: RADIUS, TACACS+
Network components: switch, router, ATM, MPLS
Telephony: VoIP, PBX
Application Security
System life cycle security
SDLC phases
Application environment and security controls
Applications
Programming languages and tools: compilers, interpreters
Databases and data warehouses: data mining and DBMS
Applications systems threats and vulnerabilities: malware
Applications security controls: implementation testing
Operations Security
Resource protection: equipment, operations areas, personnel
Change control management
Physical security controls: controlled access
Privileged entity control: administrators, operators
Legal, Regulations, Compliance and Investigation
Major legal systems: intellectual property, computer crime
Legal concepts: due care versus due diligence
Regulatory issues: privacy, financial compliance
Investigation: chain of custody and evidence gathering
Computer forensics and investigation