

## An Introduction to the CISSP & SSCP Certifications

ACHIEVE THE HIGHEST STANDARD

Wilfred L. Camilleri, CISSP  
Secretary & Webmaster  
(ISC)<sup>2</sup> Inc.

w.camilleri@isc2.org


 ©Copyright 2000



## Agenda


- About (ISC)<sup>2</sup>
- Why Get Certified?
- Review of the CISSP™ Certification Program
- Code of Ethics
- Common Body of Knowledge (CBK)
- CBK Review Seminar
- Review of the SSCP™ Certification Program
- Additional Information
- Next Step

 ©Copyright 2000




## International Information Systems Security Certification Consortium, Inc.

- Not-for-profit / tax-exempt
- Sole purposes - certification and education
- Board of Directors
- Committees
- (ISC)<sup>2</sup> Services
- Testing Service - Schroeder Measurement Technologies


 ©Copyright 2000

3



## A Brief History

- Formed in 1989
- Consortium:
  - ISSA, DPMA, CIPS, IFIPS, CSI, Idaho State University.
- First public examination in 1995 In Toronto, Canada
- Certified thousands of information security practitioners in over twenty-seven countries

 ©Copyright 2000

4

## Why Get Certified?

GIVE YOUR CAREER  
THE CISSP / SSCP ADVANTAGE!

## Why Get Certified?


- Professional certification is a symbol of status and credibility in any profession.
- The CISSP certification is a public acknowledgment that the professional has devoted himself or herself to the field of information security or a closely related field, and passed a rigorous examination that encompasses all major elements of the industry's accepted and recognized information system security Common Body of Knowledge (CBK).



## Why Get Certified?


- An environment where demand for information security skills are fast becoming a commodity, as many organizations search for experienced and highly skilled information security professionals.

 ©Copyright 2000 7



## Why Get Certified?

- While there is a huge demand for information security practitioners, those with the right mix of education, experience and professional credentials are the most sought after for senior positions. These leading-edge careers also command the highest salaries.

 ©Copyright 2000 8

## Why Get Certified?

- Atlanta-based networking and Internet-security consulting firm requires its entire consultancy staff to seek certification through the International Information Systems Security Certification Consortium, (ISC)<sup>2</sup>
- FAA and NASA to certify all their InfoSec practitioners
- Many North American firms and government agencies now require/prefer CISSPs for senior InfoSec positions

## CISSP Certification

- Certified Information Systems Security Professional
- Minimum of three years cumulative experience in any or a combination of the CBK Domains
- CISSP Examination
- Code of Ethics
- Annual Maintenance Fees
- Continuing Professional Education (CPE) Credits

## CISSP Certification - Applicant Requirements

- Subscribe to the (ISC)<sup>2</sup> Code of Ethics
- Three years of work experience in one or more of the ten CBK domains:
  - Security Management Practices
  - Law, Investigation & Ethics
  - Physical Security
  - Operations Security
  - Business Continuity & Disaster Recovery Planning

## CISSP Certification - Applicant Requirements

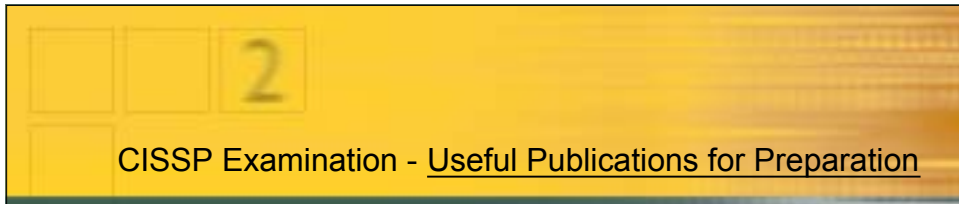
- Computer, System & Security Architecture
- Access Control Systems & Methodology
- Cryptography
- Telecommunications & Network Security
- Application Program Security

## CISSP Examination

- Format
  - 250 multiple choice questions
  - Up to 6 hours to complete
- Fees (See Web Page)
- Scheduling
  - Major Information Security Conferences
  - CBK Review Seminar Locations
  - Hosted Events

## CISSP Examination - Useful Publications for Preparation

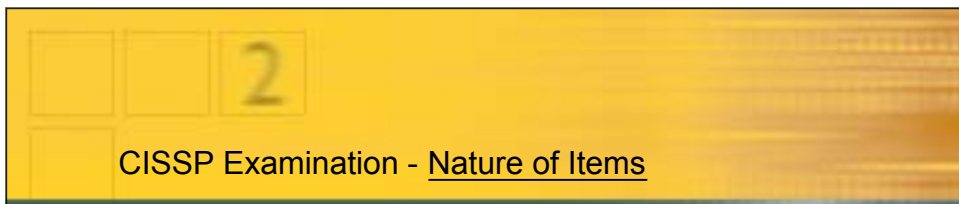
- Study Guide & Reference Materials
- [https://www.isc2.org/study\\_guide.html#reference](https://www.isc2.org/study_guide.html#reference)
- Publications listed were cited by some of the item writers when developing questions for use on the CISSP® Certification Examination. Others were recommended by CISSPs.



## CISSP Examination - Useful Publications for Preparation

- This list does not represent every reference used to create test items on the examination.
- This list is not a direct or indirect endorsement of the (ISC)<sup>2</sup> or its Board of Directors.

(ISC)<sup>2</sup> ©Copyright 2000 16



## CISSP Examination - Nature of Items

- Information Security Concepts
- Vendor and product independent
- Oriented toward *experienced* information security professionals
- Intersection of CBK and the literature

(ISC)<sup>2</sup> ©Copyright 2000 17

2

## CISSP Examination - References

- Publicly available
  - open source
  - moderate cost
- Best authority
  - law, regulation, or standard
  - refereed sources
  - other authoritative sources


(ISC) ©Copyright 2000 18

2

## CISSP Examination - Philosophy & Structure


- multiple choice
- no tricks
- no time pressure
- measures habitual knowledge, not skill

(ISC) ©Copyright 2000 19




## CISSP Examination - Philosophy & Structure

- measures professional, not special knowledge
- ten domains
- 250 questions




©Copyright 2000

20




## CISSP Examination - Domains

- Security Management Practices
  - Policies, Standards, Guidelines & Procedures
  - Information Classification/Categorization
  - Organization Architecture
  - Information Security Awareness Training Program
  - Risk Analysis




©Copyright 2000


21



## CISSP Examination - Domains


- Law, Investigation, and Ethics
  - Law & Crime
  - Investigation
  - Ethics

 ©Copyright 2000 22



## CISSP Examination - Domains

- Physical Security
  - Facility Planning
  - Physical Security
  - General Facility Construction
  - Electrical Power
  - Fire Suppression

 ©Copyright 2000 23

## CISSP Examination - Domains

- Physical Security (cont'd)
  - External Boundary Protection
  - Personnel Access Controls
  - Biometric Identification
  - Distributed Processing Impact On Physical Security

## CISSP Examination - Domains

- Operations Security
  - Operational Security Issue
  - Definitions
  - Network Administrator Privileges
  - Violation Analysis
  - Operator Privileges
  - Potential Abuses
  - Types of Controls
  - Hardware/Software Asset Management

## CISSP Examination - Domains

- Operations Security (cont'd)
  - Problem Management
  - Change Control Management
  - Secure System Operation
  - Rotation of Duties
  - Trusted Facility Management
  - Trusted Recovery
  - Trusted Recovery Procedures

## CISSP Examination - Domains

- BCP & DRP
  - Disaster Definition
  - Recovery Planning Definition
  - BCP vis-à-vis DRP
  - DRP Objectives
  - Recovery Planning Methodology
  - Vulnerability Assessment Goals & Process
  - Identifying Essential Business Functions
  - System Backup Alternatives

## CISSP Examination - Domains

- BCP & DRP (cont'd)
  - Recovery Plan Components
  - Regular Drills & Testing
  - Plan Testing
  - Why Plans Get Out of Date
  - Importance of Prevention
  - Off-Site Storage Facilities
  - Data & Applications Backup Alternatives

## CISSP Examination - Domains

- Computer, System & Security Architecture
  - **TCSEC/ITSEC/Common Criteria**
  - **Trusted Computing Base**
  - **Platform Protection**
    - **Operation System**
    - **Memory**
    - **File**
  - **Mainframe Protection**
  - **Network Protection**
  - **Models**

## CISSP Examination - Domains

- Access Control
  - Techniques
  - Identification & Authentication
  - Accountability
  - Authorization
  - Methods of Attack
  - Intrusion Detection
  - Penetration Testing

## CISSP Examination - Domains

- Cryptography
  - Stream/Block Ciphers
  - Symmetric/Asymmetric Algorithms
  - Message Authentication/Hashing
  - Certificate Authority
  - Digital Signatures/Message Digests
  - Key Management
  - Attacks

## CISSP Examination - Domains

- Application Program Security
  - Application Issues (Mobile code/Viruses/etc.)
  - Databases & Data Warehousing
  - Knowledge Based Systems
  - System Development Controls
  - Methods of Attack

## CISSP Examination - Domains

- Telecommunications & Network Security
  - Internet/Intranet/Extranet
  - Firewalls
  - OSI & TCP/IP
  - Protocols (IPSEC/SSL/SET/PEM/etc.)
  - LAN/WAN/VPN
  - Remote Access
  - Transmission Protocols & Services
  - Network Attacks & Countermeasures

## Code of Ethics - Preamble

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this code is a condition of certification.

## Code of Ethics - Certificate holders will:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

2

## Common Body of Knowledge - History

- Committee named by ISSA - 1990
- Anticipated CISSP
- Independent
- Judgment of the authors


(ISC) ©Copyright 2000 37

2

## Common Body of Knowledge - Committee


- Experienced and Professionally Recognized
- Articulate
- Members:
  - Robert H. Courtney, Jr.
  - Harry B. DeMaio
  - Toni B. Fish
  - Jerome M. Lobel
  - Sandra M. Lambert
  - William H. Murray (Chair)
  - Martin Silverman
  - Dennis Steinauer
  - Harold F. Tipton


(ISC) ©Copyright 2000 38



## Common Body of Knowledge


- Is a document
- Is a description
- Is not the knowledge
- Is not the identity


 ©Copyright 2000 39



## Common Body of Knowledge - Description


- Professional knowledge
- Expected of our professional peers
- Not expected of our management peers
- Not expected of our technology peers
- Seventeen areas identified


 ©Copyright 2000 40



## Common Body of Knowledge - Professional Knowledge


- Knowledge that distinguishes professions
- Used in their work
- Facilitates communication among the professionals
- Existence indicates profession
- Expected of members

 ©Copyright 2000 41



## Exam Overview & CBK Review Seminar

- One-day “Intro to the CISSP Exam & CBK”
- Five-day “CBK Review Seminar”
  - Public Sessions announced on Web Page
  - In-house & hosted sessions are available

 ©Copyright 2000 42

## Five Functional Areas Within Each Domain

- Information Protection Requirements
- Information Protection Environment
- Security Technology and Tools
- Assurance, Trust, and Confidence Mechanisms
- Information Protection and Management Services

## CBK Review Seminar – Five Days

- Five Sections/Ten Domains:
  - Security Management Practices
  - Access Control Systems & Methodology
  - Law, Investigation & Ethics
  - Physical Security
  - Business Continuity & Disaster Recovery Planning
  - Computer, System & Security Architecture

## CBK Review Seminar - Continued

- Domains continued:
  - Cryptography
  - Telecommunications & Network Security
  - Application Program Security
  - Operations Security

## CBK Review Seminar - Cost & Hosting

- Fees:
  - See Web Page
  - Early registration discounts available
- Hosting:
  - Reduction in fees for host employees

## SSCP Certification

- Systems Security Certified Practitioner
- Minimum of one year cumulative experience in any or a combination of the CBK Domains
- SSCP Examination
- Code of Ethics
- Annual Maintenance Fees
- Continuing Professional Education (CPE) Credits

## SSCP Certification - Applicant Requirements

- Subscribe to the (ISC)<sup>2</sup> Code of Ethics
- One year of work experience in one or more of the seven test domains
- An information systems security administrator is expected to have knowledge in each of the seven practice areas, including an understanding of the governing principles, individual components and applicable technologies used to implement, monitor and maintain each practice area.

## SSCP Certification - Applicant Requirements

- The CBK covers the following seven knowledge areas:
  - Access Control
  - Administration
  - Audit & Monitoring
  - Risk, Response & Recovery
  - Cryptography
  - Data Communications
  - Malicious Code

## SSCP Examination - Domains

- Access Controls
  - The access controls area includes the mechanisms that allow a system manager to specify what users and processes can do, which resources they can access, and what operations they can perform.

## SSCP Examination - Domains

- Administration
  - The administration area encompasses the security principles, policies, standards, procedures and guidelines used to identify, classify and ensure the confidentiality, integrity and availability of an organization's information assets.

## SSCP Examination - Domains

- Administration
  - It also includes roles and responsibilities, configuration management, change control, security awareness, and the application of accepted industry practices.

## SSCP Examination - Domains

- Audit and Monitoring
  - The monitoring area includes those mechanisms, tools and facilities used to identify, classify, prioritize, respond to, and report on security events and vulnerabilities. The audit function provides the ability to determine if the system is being operated in accordance with accepted industry practices, and in compliance with specific organizational policies, standards, and procedures.

## SSCP Examination - Domains

- Risk, Response and Recovery
  - The risk, response and recovery area encompasses the roles of a security administrator in the risk analysis, emergency response, disaster recovery and business continuity processes, including the assessment of system vulnerabilities, the selection and testing of safeguards, and the testing of recovery plans and procedures.

## SSCP Examination - Domains

- Risk, Response and Recovery
  - It also addresses knowledge of incident handling including the acquisition, protection and storage of evidence.

## SSCP Examination - Domains

- Cryptography
  - The cryptography area addresses the principles, means and methods used to disguise information to ensure its integrity, confidentiality, authenticity and non-repudiation.

## SSCP Examination - Domains

- Data Communications
  - The data communications area encompasses the structures, transmission methods, transport formats and security measures used to provide integrity, availability, authentication and confidentiality for data transmitted over private and public communications paths.

## SSCP Examination - Domains

- Malicious Code
  - The malicious code area encompasses the principles, means and methods used by programs, applications and code segments to infect, abuse or otherwise impact the proper operation of an information processing system or network.

## Additional Information

- Study Guide Requests:
  - complete and submit Web Form at [https://www.isc2.org/study\\_guide.html](https://www.isc2.org/study_guide.html)
- Phone/Fax Info:
  - Contacts Page:
    - <http://www.isc2.org/cgi-bin/contact.cgi>
- E-mail: [info@isc2.org](mailto:info@isc2.org)
- Web page: [www.isc2.org](http://www.isc2.org)

## Summary



“Are you ready to take the  
CISSP™ or the SSCP™ exam?”

2

## Next Step

- Contact (ISC)<sup>2</sup> to request information and register interest in the CISSP & SSCP Certification Programs and/or the CBK Review Seminar
- Approximately 20-30 candidates required to schedule a local examination
- Approximately 10-20 registrations required to schedule a local CBK Review seminar