Preparing for the CISSP

Sept 15, 05

Dr Van B. Le, CISSP

IEEE GOLD VA Officer

Agenda

1. Why certify for CISSP?
2. CISSP domains of knowledge
3. CISSP exam & requirements
4. Preparation & keeping your certification current

1. Why certify CISSP?

- CISSP (Certified Information Systems Security Professional)
- Benefits to the Professional
  - Demonstrate a working knowledge of information security
  - Offers international differentiator, solid credibility and undisputable marketability to career
- Benefits to the Enterprise
  - Establishes a standard of best practices
  - Offers broad understanding of security as described in body of knowledge

2. CISSP Body Of Knowledge (CBK)

- (ISC)^2 International Information System Security Certification Consortium
- CBK is comprised of ten (10) domains or subject areas
- A CISSP candidate must understand the principles, practices, and functions in each of these domains

2. Domain 1 – Information Security Management

- Concepts & Objectives of security C-I-A triad
- Management tools (such as data classification, security awareness training, risk assessment and risk analysis)
- Risk Management is the identification, measurement, control and minimization of loss associated with uncertain events or risks

2. Domain 2 - Security Architecture & Models

- Define security models by C-I-A
- Identify security issues and controls associated with architectures and designs
- Principles, structures and standards used to design implement, monitor and secure operating systems, equipment, networks, applications

2. Domain 3 - Access Control Systems & Methodology

- Outlines information security options
- Builds on Domain 1 precepts, with emphasis on various administrative, physical and technical/logical controls

2. Domain 4 - Applications & Systems Development

- Security concepts that apply during software development, operation, change control and maintenance processes
- Security applied as a system level attribute
- Security Goals & Threats:
  - Knowledge of malicious codes and how they can be introduced in the computing environment
  - Tools and techniques to prevent, detect, and correct malicious code attacks

2. Domain 5 - Operations Security

- Operations Security identifies controls
  - over hardware, media
  - and operators/administrators with access privileges to these resources
- Process of safeguarding information assets
- Recovery actions in the event of a security incident

2. Domain 6 - Cryptography

Cryptography as

- principles
- means
- and methods

of disguising information to ensure its confidentiality, integrity, and *authenticity*

2. Domain 7 – Physical Security

- Protection techniques for the entire facility
  - from the outer perimeter
  - to the inside office space
  - including data center or server room

2. Domain 8 - Telecommunications & Network Security

- Describes telecommunications and network security elements as related to transmission of information in LAN, WAN, and remote access
- Defines firewalls, gateways and protocols as associated with Internet, intranet and extranet
- Identifies communication security management and techniques to prevent, detect, and correct errors to ensure information protection over networks

2. Domain 9 – Business Continuity Planning

- Business Continuity Planning (BCP): addresses the capability to process critical business systems in the event of disruption to normal business data processing operations
- Preparation, testing, maintenance of actions to address BCP
  - Program Management
  - Vulnerability Assessment
  - Plan Development & Maintenance
  - Plan Testing
  - Prevention
- Disaster Recovery Planning
- Recovery Planning Process

2. Domain 10 - Law, Investigations, Ethics

Addresses

- computer laws and regulations
- investigative measures
- techniques used to determine existence of a crime,
- methods to gather evidences

3. The CISSP exam

- Register online www.isc2.org
- 250 questions, MCQ (4 options)
- Six (6) hours

3. Requirements to become a CISSP

1. Pass the CISSP exam
2. Be endorsed by a CISSP
   - If no CISSP can be found, another qualified professional with knowledge of information systems or an officer of the candidates corporation can be used to validate the candidate's professional experience
3. Have experience fitting one of the following descriptions
   - Four (4) years of direct work experience in one or more of the ten domains of the CISSP Common Body of Knowledge (CBK)

   or:
   - Three (3) years of direct work experience in one or more of the ten domains of the CBK, PLUS a bachelor’s degree

4. Preparation

Study approaches:

- Self study
  - Dedicate sufficient study time to each domain
  - Official (ISC)^2 Guide to the CISSP exam, Auerbach Publications ISBN 08931707X
  - Cross-check and read other references
- (ISC)^2 CISSP CBK Review Seminar
- (ISC)^2 vendor
- Independent instructors

4. After obtaining the CISSP certification

Need to obtain 120 Continued Professional Education credits over 3 years in order to keep the certification current :

- Attending educational courses or seminars
- Attending security conferences
- Being a member of an association chapter and attending meetings
- Completing university/college courses
- Providing security training
- Publishing security articles or books
- Serving on industry boards
- Self-study
- Completing volunteer work, including serving on (ISC)^2 volunteer committees

Good luck

vanble@alumni.gwu.edu