Getting your CISSP Certification

Intro to the 10 CISSP domains of the Common Body of Knowledge

In this e-guide

In this e-guide:

The Certified Information Systems Security Professional (CISSP) is an information security certification that was developed by the International Information Systems Security Certification Consortium, also known as (ISC)².

The CISSP exam covers 10 individual subject areas, which are referred to as domains. The 10 domains make up (ISC)² 's Common Body of Knowledge (CBK), which is a framework and collection of information security best practices, methodologies, technologies and concepts.

Jump to any of the 10 domains of the CISSP CBK listed in this guide:

Domain 1: Information Security Governance and Risk Management
Domain 2: Access Control
Domain 3: Cryptography
Domain 4: Security Architecture and Design
Domain 5: Telecommunications and Network Security
Domain 6: Software Development Security
Domain 7: Business Continuity and Disaster Recover Planning
Domain 8: Legal, Regulations, Investigations, and Compliance
Domain 9: Physical Security
Domain 10: Operations Security

SearchSecurity partnered with Logical Security and Shon Harris, the information security leading certification preparation instructor, to create SearchSecurity's **CISSP Essentials Security School.**

SearchSecurity's CISSP Essentials Security School offers free training that covers critical topics in each of these 10 domains to help practitioners prepare for the 6 hour exam which asks 250 questions. Each of the 10 lessons feature videos, tutorials and an exclusive quiz offering prep questions similar those on the real CISSP exam.

For a deeper introduction to the (ISC)² CISSP certification in the areas of:
- **CISSP: The "gold standard" of the information security industry**
- **CISSP exam subject areas**
- **Anatomy of the exam and its "interactive" evolution**
- **Mapping the exam to security models**
- **Why simply knowing the material isn't enough**

Go to: **An introduction to the CISSP security certification exam**

🚩 # DOMAIN 1 - Information Security Governance and Risk Management

While hacking, new malware and computer crimes grab all the news headlines, sound organizational security practices and the development of an enterprise security architecture are the foundations of any organization's security success. CISSP Domain 1 explores:

- Security management responsibilities
- Asset identification and classification
- Risk management
- Information classification
- Personnel security
- Security governance
- Enterprise architectural development
- Policies and procedures
- Security embedded into vendor contracts
- Security education and awareness training

Go to Domain 1: Information Security Governance and Risk Management

DOMAIN 2 - Access Control

A cornerstone of any information security program is controlling how resources are accessed by users, applications and other systems to ensure they can be properly protected from unauthorized modification or disclosure. CISSP Domain 2 tackles topics including:

- The fundamental principles of access control

- The concepts of "subjects" and "objects"

- Identity management

- The four steps of authentication

- Two-factor authentication

- User access vs. device access

- Intrusion prevention and detection systems

- Access control models

- Authentication protocols

Go to Domain 2: Access Control

◤ DOMAIN 3 - Cryptography

Cryptography is one of the essential elements in the protection of electronic data. Cryptography is built into almost every network protocol, software application, operating system, embedded systems and integrated more and more at the chip and silicon level. Cryptography provides confidentiality, integrity and authenticity services. CISSP Essentials domain 3 covers:

- Cryptographic components and their relationships

- Symmetric, asymmetric and hashing algorithm types

- Public key infrastructure (PKI) mechanisms

- Cryptosystems implementation

- Cryptanalysis and attack types

Go to Domain 3: Cryptography

🔖 DOMAIN 4 - Security Architecture and Design

Architecting and implementing security into the design of various types of software, devices and enterprising is complex – but critical. Security must be designed, implemented, monitored and improved throughout each entity's lifecycle. CISSP Essentials domain 4 offers an in-depth review of:

- Formal system architecture development

- Kernel and trusted computing base security

- Hardware and operating system architectures

- Memory management and protection

- Security within virtualization and cloud computing

- Formal security control models

- Security criterion and ratings

- Certification and accreditation processes

Go to Domain 4: Security Architecture and Design

🔖 DOMAIN 5 - Telecommunications and Network Security

This session prepares students for the CISSP exam by focusing on the "glue" of network security: how networks work, how data is transmitted from one device to another, how protocols work, transmission methods and transport formats. Topics to be featured in this session include:

- OSI model and protocol structure

- Security protocols

- LAN, MAN and WAN technologies

- Cabling and data transmission types

- Network devices and security services

- Network architecture and design

- Telecommunication protocols and devices

- Remote access methodologies and technologies

- Wireless, mobile, and cloud technologies

- Network attack types

Go to Domain 5: Telecommunications and Network Security

DOMAIN 6 - Software Development Security

Applications and computer systems are usually developed for functionality first, not security. But it's always more effective to build security into every system from the outset rather than "bolt" it on afterward. The exact reasons why are revealed in this CISSP domain through topics focused on:

- Systems development life cycle (SDLC)

- Secure coding and testing

- Programming languages and security issues

- Database types and protection components

- Data warehousing and data mining

- Software life cycle development processes

- Web-based security

- Expert systems and artificial intelligence

- Software oriented threats and attacks

Go to Domain 6: Software Development Security

◤ DOMAIN 7 - Business Continuity and Disaster Recovery Planning

One of the fundamental objectives of security is "availability" -- the ability to access data and computing environments whenever necessary. This session focuses on one of the often overlooked but critical aspects of availability: business continuity planning and disaster recovery. Topics in this CISSP certification prep section focus on:

- Business impact analysis

- Disruption types and associated threats

- Operational and financial ramifications

- Contingency and redundancy technologies

- Selecting, developing and implementing disaster and contingency plans

- Backup and offsite facilities

Go to Domain 7: Business Continuity and Disaster Recovery Planning

🔖 DOMAIN 8 - Legal, Regulations, Investigations, and Compliance

Fraud, theft and embezzlement have always been an unfortunate fact of life, but the digital age has brought on new opportunities for a different and more malicious set of thieves and criminals. While many security professionals focus on "preventing" cyber attacks, the CISSP CBK teaches that it's equally important to understand how to investigate a computer crime and gather evidence -- that's exactly what this session addresses. Additional topics highlighted are information security regulations, laws and ethics that guide the practice:

- Computer crimes and computer law
- International legal system types
- Forensics, investigation processes and evidence collection
- Incident-handling program development
- Prosecution process and associated threats
- Industry regulations and compliance requirements
- Ethics and best practices for security professionals

Go to Domain 8: Legal, Regulations, Investigations, and Compliance

In this e-guide

🔖 DOMAIN 9 - Physical Security

Physical security has taken on added importance in the continuing wake of September 11, 2001. While most IT professionals are focused on digital systems — computers, networks, systems, devices — a comprehensive security program must address critical physical risks, too. The convergence of physical and digital systems makes this practice even more important. CISSP Essentials domain 9 covers:

- Administrative, technical and physical controls pertaining to physical security

- Facility location, construction and management

- Physical security risks, threats and countermeasures

- Fire prevention, detection and suppression

- Intrusion detection, CCTV, monitoring and lighting technologies

- Threat types and associated risks

Go to Domain 9: Physical Security

🔖 # DOMAIN 10 - Operations Security

Operations security pertains to everything needed to keep a network, computer system and environment up and running in a secure and protected manner. Since networks are "evolutionary" and always changing, it's essential that security pros understand the fundamental procedures for managing security continuity and consistency in an operational environment. CISSP Essentials domain 10 reveals essential answers centered on key operations security topics:

- Resource, media and data protection technologies

- Incident response and situational awareness

- Patch, configuration and vulnerability management

- Operational assurance methods and measurements

- Trusted recovery technologies

- Attack prevention and response approaches

Go to Domain 10: Operations Security

Continue Reading About Certified Information Systems Security Professional (CISSP)

- SearchSecurity partnered with (ISC)² to help you study for your CISSP certification exam. **Take the CISSP practice test here**.
- At our free Security School featuring full-length video seminars and review quizzes, you can earn CPE credits. **Go to the Security School**.
- Visit the **(ISC)² website**, which offers more information about the CISSP certification and study materials.
- Go to all 10 CISSP Domain lessons:
  Domain 1: Information Security Governance and Risk Management
  Domain 2: Access Control
  Domain 3: Cryptography
  Domain 4: Security Architecture and Design
  Domain 5: Telecommunications and Network Security
  Domain 6: Software Development Security
  Domain 7: Business Continuity and Disaster Recovery Planning
  Domain 8: Legal, Regulations, Investigations, and Compliance
  Domain 9: Physical Security
  Domain 10: Operations Security

🔖 **About SearchSecurity**

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure.

We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading, visit us at http://SearchSecurity.com/

Images; Fotalia