

Please note: 2 - CISSPs combined into one file effective dates January 1, 2009 and January 1, 2012. Please review appropriate version in accordance with your exam date (click grey button on right to view January 1, 2012 version)



CISSP®

Candidate Information Bulletin

Effective Date January 1, 2009 (Rev 09.7)





1) ACCESS CONTROL	5
Overview	5
Key Areas of Knowledge	5
2) TELECOMMUNICATIONS & NETWORK SECURITY	6
Overview	6
Key Areas of Knowledge	6
3) INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT	8
Overview	8
Key Areas of Knowledge	8
4) APPLICATION DEVELOPMENT SECURITY	11
Overview	11
Key Areas of Knowledge	11
5) CRYPTOGRAPHY	12
Overview	12
Key Areas of Knowledge	12
6) SECURITY ARCHITECTURE & DESIGN	14
Overview	14
Key Areas of Knowledge	14
7) OPERATIONS SECURITY	16
Overview	16
Key Areas of Knowledge	16
8) BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING	18
Overview	18
Key Areas of Knowledge	18
9) LEGAL, REGULATIONS, INVESTIGATIONS & COMPLIANCE	20
Overview	20
Key Areas of Knowledge	20
10) PHYSICAL (ENVIRONMENTAL) SECURITY	22



Overview	22
Key Areas of Knowledge	22
REFERENCES	23
SAMPLE EXAM QUESTIONS	28
GENERAL EXAMINATION INFORMATION	29
Any questions?	32



This Candidate Information Bulletin provides the following:

- exam blueprint to a limited level of detail that outlines major topics and sub- topics within the domains which are listed in alphabetical order,
- suggested reference list,
- description of the format of the items on the exam, and
- basic registration/administration policies

Applicants must have a minimum of five years of direct full-time security professional work experience in two or more of the ten domains of the (ISC)² CISSP® CBK® or four years of direct full-time security professional work experience in two or more of the ten domains of the CISSP® CBK® with a four-year college degree. Only one year experience exemption is granted for education.

CISSP professional experience includes:

- Work requiring special education or intellectual attainment, usually including a liberal education or college degree.
- Work requiring habitual memory of a body of knowledge shared with others doing similar work.
- Management of projects and/or other employees.
- Supervision of the work of others while working with a minimum of supervision of one's self.
- Work requiring the exercise of judgment, management decision-making, and discretion.
- Work requiring the exercise of ethical judgment (as opposed to ethical behavior).
- Creative writing and oral communication.
- Teaching, instructing, training and the mentoring of others.
- Research and development.
- The specification and selection of controls and mechanisms (i.e. identification and authentication technology) (does not include the mere operation of these controls).
- Applicable titles such as officer, director, manager, leader, supervisor, analyst, designer, cryptologist, cryptographer, cryptanalyst, architect, engineer, instructor, professor, investigator, consultant, salesman, representative, etc. Title may include programmer. It may include administrator, except where it applies to one who simply operates controls under the authority and supervision of others. Titles with the words "coder" or "operator" are likely excluded.



1) ACCESS CONTROL

Overview

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system.

The candidate should fully understand access control concepts, methodologies and implementation within centralized and decentralized environments across the enterprise's computer systems. Access control techniques, detective and corrective measures should be studied to understand the potential risks, vulnerabilities, and exposures.

Key Areas of Knowledge

A. Control access by applying the following concepts/methodologies/techniques

- A.1 Policies
- A.2 Types of controls (preventive, detective, corrective, etc.)
- A.3 Techniques (e.g., non-discretionary, discretionary and mandatory)
- A.4 Identification and Authentication
- A.5 Decentralized/distributed access control techniques
- A.6 Authorization mechanisms
- A.7 Logging and monitoring

B. Understand access control attacks

C. Assess effectiveness of access controls



2) TELECOMMUNICATIONS & NETWORK SECURITY

Overview

Telecommunications and Network Security domain encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media.

The candidate is expected to demonstrate an understanding of communications and network security as it relates to voice communications; data communications in terms of local area, wide area, and remote access; Internet/Intranet/Extranet in terms of Firewalls, Routers, and TCP/IP; and communications security management and techniques in terms of preventive, detective and corrective measures.

In today's global marketplace, the ability to communicate with others is a mandatory requirement. The data communications domain encompasses the network structure, transmission methods, transport formats and security measures used to maintain the integrity, availability, authentication and confidentiality of the transmitted information over both private and public communication networks.

The candidate is expected to demonstrate an understanding of communications and network security as it relates to data communications in local area and wide area networks; remote access; internet/intranet/extranet configurations, use of firewalls, network equipment and protocols (such as TCP/IP), VPNs, and techniques for preventing and detecting network based attacks.

Key Areas of Knowledge

A. Establish secure data communications

B. Understand secure network architecture and design

B.1 OSI and TCP/IP models

B.2 IP networking

C. Secure network components

B.1 Hardware (e.g., modems, switches, routers)

B.2 Transmission media



B.3 Filtering devices (e.g., firewalls, proxies)

B.4 End-point security

D. Establish secure communication channels

C.1 Voice over IP (VoIP)

C.2 Multimedia collaboration (e.g., remote meeting technology, instant messaging)

C.3 Virtual Private Networks (VPN)

C.4 Remote access

E. Understand network attacks



3) INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT

Overview

Information Security and Risk Management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify the threats, classify assets, and to rate their vulnerabilities so that effective security controls can be implemented.

Risk management is the identification, measurement, control, and minimization of loss associated with uncertain events or risks. It includes overall security review, risk analysis; selection and evaluation of safeguards, cost benefit analysis, management decision, safeguard implementation, and effectiveness review.

The candidate will be expected to understand the planning, organization, and roles of individuals in identifying and securing an organization's information assets; the development and use of policies stating management's views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security awareness training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary and private information; employment agreements; employee hiring and termination practices; and risk management practices and tools to identify, rate, and reduce the risk to specific resources.

Key Areas of Knowledge

A. Understand and align security function to goals, mission and objectives of the organization

B. Understand and apply security governance

- B.1 Organizational processes
- B.2 Define security roles and responsibilities
- B.3 Legislative and regulatory compliance
- B.4 Privacy requirements compliance



B.5 Control frameworks

B.6 Due care

B.7 Due diligence

C. Understand and apply concepts of confidentiality, integrity and availability

D. Develop and implement security policy

D.1 Security policies

D.2 Standards/baselines

D.3 Procedures

D.4 Guidelines

D.5 Documentation

E. Define and implement information classification and ownership

F. Ensure security in contractual agreements and procurement processes

G. Understand and apply risk management concepts

G.1 Identify threats and vulnerabilities

G.2 Risk assessment/analysis

G.3 Risk assignment/acceptance

G.4 Countermeasure selection

H. Evaluate personnel security

H.1 Background checks and employment candidate screening

H.2 Employment agreements and policies

H.3 Employee termination processes

H.4 Vendor, consultant and contractor controls

I. Develop and manage security education, training and awareness

J. Develop and implement information security strategies

K. Support certification and accreditation efforts

L. Assess the completeness and effectiveness of the security program

M. Understand professional ethics



- M.1 (ISC)² code of professional ethics
- M.2 Support organization's code of ethics

N. Manage the Security Function

- N.1 Budget
- N.2 Metrics
- N.3 Resources



4) APPLICATION DEVELOPMENT SECURITY

Overview

Application security refers to the controls that are included within systems and applications software and the steps used in their development. Applications refer to agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments.

The candidate should fully understand the security and controls of the systems development process, system life cycle, application controls, change controls, data warehousing, data mining, knowledge-based systems, program interfaces, and concepts used to ensure data and application integrity, security, and availability.

Key Areas of Knowledge

A. Understand and apply security in the system life cycle

- A.1 Systems Development Life Cycle (SDLC)
- A.2 Maturity models
- A.3 Operation and maintenance
- A.4 Change management
- A.5 Perform Risk Analysis

B. Understand the application environment and security controls

- B.1 Security of the application environment
- B.2 Security issues of programming languages
- B.3 Security issues in source code (e.g., buffer overflow)
- B.4 Configuration management

C. Assess the effectiveness of application security

- C.1 Certification and accreditation
- C.2 Auditing and logging
- C.3 Corrective actions



5) CRYPTOGRAPHY

Overview

The Cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity.

The candidate will be expected to know basic concepts within cryptography; public and private key algorithms in terms of their applications and uses; algorithm construction, key distribution and management, and methods of attack; and the applications, construction and use of digital signatures to provide authenticity of electronic transactions, and non-repudiation of the parties involved.

Key Areas of Knowledge

A. Understand the application and use of cryptography

- A.1 Data at rest (e.g., Hard Drive)
- A.2 Data in transit (e.g., "On the wire")

B. Understand encryption concepts

- B.1 Foundational concepts
- B.2 Symmetric cryptography
- B.3 Asymmetric cryptography
- B.4 Hybrid cryptography
- B.5 Message digests
- B.6 Hashing

C. Understand key management processes

- C.1 Creation/distribution
- C.2 Storage/destruction
- C.3 Recovery
- C.4 Key escrow

D. Understand digital signatures

E. Understand non-repudiation



F. Understand methods of cryptanalytic attacks

- F.1 Chosen plain-text
- F.2 Social engineering for key discovery
- F.3 Brute Force
- F.4 Cipher-text only
- F.5 Known plaintext
- F.6 Frequency analysis
- F.7 Chosen cipher-text
- F.8 Implementation attacks

G. Employ cryptography in network security

H. Use cryptography to maintain e-mail security

I. Understand Public Key Infrastructure (PKI)

J. Understand certificate related issues

K. Understand information hiding alternatives (e.g., steganography, watermarking)



6) SECURITY ARCHITECTURE & DESIGN

Overview

The Security Architecture and Design domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.

The candidate should understand security models in terms of confidentiality, integrity, information flow; system models in terms of the Common Criteria; technical platforms in terms of hardware, firmware, and software; and system security techniques in terms of preventative, detective, and corrective controls.

Key Areas of Knowledge

- A. Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multi-level Models)***
- B. Understand the components of information systems security evaluation models***
 - B.1 Product evaluation models (e.g., common criteria)
 - B.2 Industry and international security implementation guidelines (e.g., PCI-DSS, ISO)
- C. Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module)***
- D. Understand the vulnerabilities of security architectures***
 - D.1 System (e.g., covert channels, state attacks, emanations)
 - D.2 Technology and process integration (e.g., single point of failure, service oriented architecture)
- E. Understand application and system vulnerabilities and threats***
 - E.1 Web-based (e.g., XML, SAML)
 - E.2 Client-based (e.g., applets)
 - E.3 Server-based (e.g., data flow control)



E.4 Database security (e.g., inference, aggregation, data mining)

F. Understand countermeasure principles (e.g., defense in depth)



7) OPERATIONS SECURITY

Overview

Operations Security is used to identify the controls over hardware, media, and the operators with access privileges to any of these resources. Audit and monitoring is the mechanisms, tools and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

The candidate will be expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms available, the potential for abuse of access, the appropriate controls, and the principles of good practice.

Key Areas of Knowledge

A. Understand the following security concepts

- A.1 Need-to-know/least privilege
- A.2 Separation of duties and responsibilities
- A.3 Monitor special privileges (e.g., operators, administrators)
- A.4 Job rotation
- A.5 Marking, handling, storing and destroying of sensitive information
- A.6 Record retention

B. Employ resource protection

- B.1 Media management
- B.2 Asset management
- B.3 Personnel privacy and safety

C. Manage incident response

- C.1 Detection
- C.2 Response
- C.3 Reporting
- C.4 Recovery



C.5 Remediation

- D. Prevent or respond to attacks (e.g., malicious code, zero-day exploit, denial of service)*
- E. Implement and support patch and vulnerability management*
- F. Understand configuration management concepts (e.g., versioning, baselining)*
- G. Understand fault tolerance requirements*



8) BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING

Overview

The Business Continuity and Disaster Recovery Planning domain addresses the preservation of the business in the face of major disruptions to normal business operations. BCP and DRP involve the preparation, testing and updating of specific actions to protect critical business processes from the effect of major system and network failures.

Business Continuity Plans counteract interruptions to business activities and should be available to protect critical business processes from the effects of major failures or disasters. It deals with the natural and man-made events and the consequences if not dealt with promptly and effectively.

Business Impact Assessment determines the proportion of impact an individual business unit would sustain subsequent to a significant interruption of computing or telecommunication services. These impacts may be financial, in terms of monetary loss, or operational, in terms of inability to deliver.

Disaster Recovery Plans contain procedures for emergency response, extended backup operation and post-disaster recovery should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objective of the Disaster Recovery Plan is to provide the capability to process mission-essential applications, in a degraded mode, and return to normal mode of operation within a reasonable amount of time.

The candidate will be expected to know the difference between business continuity planning and disaster recovery; business continuity planning in terms of project scope and planning, business impact analysis, recovery strategies, recovery plan development, and implementation. The candidate should understand disaster recovery in terms of recovery plan development, implementation and restoration.

Key Areas of Knowledge

A. Understand business continuity requirements

A.1 Develop and document project scope and plan

B. Conduct business impact analysis

B.1 Identify and prioritize critical business functions



- B.2 Determine maximum tolerable downtime and other criteria
- B.3 Assess exposure to outages (e.g., local, regional, global)
- B.4 Define recovery objectives

C. Develop a recovery strategy

- C.1 Implement a backup storage strategy (e.g., offsite storage, electronic vaulting, tape rotation)
- C.2 Recovery site strategies

D. Understand disaster recovery process

- D.1 Response
- D.2 Personnel
- D.3 Communications
- D.4 Assessment
- D.5 Restoration

E. Provide training

F. Test, update, assess and maintain the plan (e.g., version control, distribution)



9) LEGAL, REGULATIONS, INVESTIGATIONS & COMPLIANCE

Overview

The Legal, Regulations, Compliance and Investigations domain addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed, and methods to gather evidence.

Incident handling provides the ability to react quickly and efficiently to malicious technical threats or incidents.

The candidate will be expected to know the methods for determining whether a computer crime has been committed; the laws that would be applicable for the crime; laws prohibiting specific types of computer crime; methods to gather and preserve evidence of a computer crime, investigative methods and techniques; and ways to address compliance.

Key Areas of Knowledge

A. Understand legal issues that pertain to information security internationally

- A.1 Computer crime
- A.2 Licensing and intellectual property (e.g., copyright, trademark)
- A.3 Import/Export
- A.4 Trans-border data flow
- A.5 Privacy

B. Understand and support investigations

- B.1 Policy
- B.2 Incident handling and response
- B.3 Evidence collection and handling (e.g., chain of custody, interviewing)
- B.4 Reporting and documenting

C. Understand forensic procedures

- C.1 Media analysis
- C.2 Network analysis



C.3 Software analysis

D. Understand compliance requirements and procedures

D.1 Regulatory environment

D.2 Audits

D.3 Reporting



10) PHYSICAL (ENVIRONMENTAL) SECURITY

Overview

The Physical (Environmental) Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information. These resources include people, the facility in which they work, and the data, equipment, support systems, media, and supplies they utilize.

The candidate will be expected to know the elements involved in choosing a secure site, its design and configuration, and the methods for securing the facility against unauthorized access, theft of equipment and information, and the environmental and safety measures needed to protect people, the facility, and its resources.

Key Areas of Knowledge

- A. Participate in site and facility design considerations*
- B. Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)*
- C. Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)*
- D. Support the implementation and operation of facilities security*
 - D.1 Communications and server rooms
 - D.2 Restricted and work area security
 - D.3 Data center security
 - D.4 Utilities and HVAC considerations
 - D.5 Water issues (e.g., leakage, flooding)
 - D.6 Fire prevention, detection and suppression
- E. Support the protection and securing of equipment*



REFERENCES

This reference list is **NOT** intended to be an all-inclusive collection representing the CISSP® Core Body of Knowledge (CBK®). Its purpose is to provide candidates a starting point for their studies in domains which need supplementary learning in order to complement their associated level of work and academic experience. Candidates may also consider other references, which are not on this list but adequately cover domain content.

Note: (ISC)² does not endorse any particular text or author and does not imply that any or all references be acquired or consulted. (ISC)² does not imply nor guarantee that the study of these references will result in an examination pass.

Domain	Supplementary Reference
Access Control	Bertino, E., K. Takahashi, (2010). <i>Identity Management: Concepts, Technologies, and Systems</i>
	Chin, S-K., S.B. Older (2010). <i>Access Control, Security, and Trust: A Logical Approach</i>
	Ferraiolo, D.F., D.R. Kuhn, R. Chandramouli, (2007). <i>Role-Based Access Control (2nd Edition)</i>
	Kayem, A.V., S.G. Akl, P. Martin, (2010). <i>Adaptive Cryptographic Access Control</i>
	Konicek, J., (1997). <i>Security, ID Systems and Locks: The Book on Electronic Access Control</i>
	Links, C.L., (2008). <i>IAM Success Tips (Volumes 1-3)</i>
	Newman, R., (2009). <i>Security and Access Control Using Biometric Technologies: Application, Technology, and Management</i>
	Rankl, W., W. Effing, (2010). <i>Smart Card Handbook</i>
	Tipton, H.F., M.K. Nozaki, (2011). <i>Information Security Management Handbook (2011 CD-ROM Edition)</i> ¹
	Vacca, J.R., (2010). <i>Biometric Technologies and Verification Systems</i>
Telecommunications & Network Security	Cheswick, W.R., S.M. Bellovin, A.D. Rubin, (2003). <i>Firewalls and Internet Security: Repelling the Wily Hacker (2nd Edition)</i>
	Daniel V. Hoffman, D.V., (2008). <i>Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control</i>
	Davis, C., (2001). <i>IPSec: Securing VPNs</i>

¹ This reference can be used for multiple domains.



Telecommunications & Network Security (cont'd)	Hogg, S., E. Vyncke, (2008). <i>IPv6 Security</i>
	Kadrich, M., (2007). <i>Endpoint Security</i>
	Luotonen, A., (1997). <i>Web Proxy Servers</i>
	Porter, T., J. Kanclirz, B. Baskin, (2006). <i>Practical VoIP Security</i>
	Prowell, S., R.Kraus, M. Borkin, (2010). <i>Seven Deadliest Network Attacks</i>
	Stevens, W.R., G.R. Wright, (2001). <i>TCP/IP Illustrated (3 Volume Set)</i>
	Wetteroth, D., (2001). <i>OSI Reference Model for Telecommunications</i>
Information Security Governance and Risk Management	(ISC) ² , <i>Code of Ethics</i> (https://www.isc2.org/ethics/default.aspx)
	Bacik, S., (2008). <i>Building an Effective Information Security Policy Architecture</i>
	Brotby, K., (2010). <i>Information Security Governance</i>
	Calder, A., S. Watkins, (2008). <i>IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002</i>
	Hayden, L., (2010). <i>IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data</i>
	Herold, R., (2010). <i>Managing an Information Security and Privacy Awareness and Training Program, (2nd Edition)</i>
	Jaquith, A., (2007). <i>Security Metrics: Replacing Fear, Uncertainty, and Doubt</i>
	Landoll, D.J., (2005). <i>The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments</i>
	Thomas L. Norman, T.L., (2009). <i>Risk Analysis and Security Countermeasure Selection</i>
Application Development Security	Tipton, H.F., (2009). <i>Official (ISC)² Guide to the CISSP CBK, (2nd Edition)²</i>
	Whitman, M.E., H.J. Mattord, (2010). <i>Management of Information Security (3rd Edition)</i>
	Allen, J.A., S.J. Barnum, R.J. Ellison, G. McGraw, N.R. Mead, (2008). <i>Software Security Engineering: A Guide for Project Managers</i>
	Chess, B., J. West, (2007). <i>Secure Programming with Static Analysis</i>
	Clarke, J., (2009). <i>SQL Injection Attacks and Defense</i>
	Dowd, M., J. McDonald, J. Schuh, (2006). <i>The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities</i>
	Dwivedi, H., (2010). <i>Mobile Application Security</i>
Howard, M., D. LeBlanc, J. Viega, (2009). <i>24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them</i>	
Howard, M., S. Lipner, (2006). <i>The Security Development Lifecycle: SDL: A</i>	

² This reference can be used for multiple domains.



Application Development Security (cont'd)	<i>Process for Developing Demonstrably More Secure Software</i>
	Ligh, M., S. Adair, B. Hartstein, M. Richard, (2010). <i>Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code</i>
	Stuttard, D., M. Pinto, (2007). <i>The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws</i>
	Viega, J., G. McGraw, (2001). <i>Building Secure Software: How to Avoid Security Problems the Right Way</i>
Cryptography	Boudriga, N., (2009). <i>Security of Mobile Communications</i>
	Cole, E., (2003). <i>Hiding in Plain Sight: Steganography and the Art of Covert Communication</i>
	D. Hankerson, A.J. Menezes, S. Vanstone, (2010). <i>Guide to Elliptic Curve Cryptography</i>
	Daemen, J., V. Rijmen, (2002). <i>The Design of Rijndael: AES - The Advanced Encryption Standard</i>
	Garfinkel, S., (1994). <i>PGP: Pretty Good Privacy</i>
	Karamanian, A., S. Tenneti, (2011). <i>PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks</i>
	Menezes, A.J., P. van Oorschot, S. Vanstone, (1996). <i>Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)</i>
	Schneier, B., (1996). <i>Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd Edition)</i>
	Tennoe, L.M., M.T. Hensonow, S.F. Surhone, (2010). <i>Tokenization (Data Security)</i>
	W. Stallings, (2010). <i>Cryptography and Network Security: Principles and Practice (5th Edition)</i>
Security Architecture & Design	Anderson, R.J., (2008). <i>Security Engineering: A Guide to Building Dependable Distributed Systems³</i>
	Challener, C., K. Yoder, R. Catherman, D. Safford, L.V. Doorn, (2008). <i>A Practical Guide to Trusted Computing</i>
	Gillis, T., (2010). <i>Securing the Borderless Network: Security for the Web 2.0 World</i>
	Higaki, W.H., Y. Higaki, (2010). <i>Successful Common Criteria Evaluations: A Practical Guide for Vendors</i>
	Kanneganti, R., P.R. Chodavarapu, (2008). <i>SOA Security</i>
	Kenan, K., (2005). <i>Cryptography in the Database: The Last Line of</i>

³ This reference can be used for multiple domains.



Candidate Information Bulletin

Effective Date 1 January 2009

Security Architecture & Design (cont'd)	<i>Defense</i>
	Petkovic, M., W. Jonker, (2010). <i>Security, Privacy, and Trust in Modern Data Management</i>
	Santos, O., (2007). <i>End-to-End Network Security: Defense-in-Depth</i>
	Shimonski, R., W. Schmied, V. Chang, T.W. Shinder, (2003). <i>Building DMZs For Enterprise Networks</i>
	Swiderski, F., W. Snyder, (2004). <i>Threat Modeling</i>
Operations Security	Aiello, R., (2010). <i>Configuration Management Best Practices: Practical Methods that Work in the Real World</i>
	Bejtlich, R., (2005). <i>Extrusion Detection: Security Monitoring for Internal Intrusions</i>
	Bosworth, S., M. E. Kabay, E. Whyne, (2009). <i>Computer Security Handbook (2 Volume Set)</i>
	Cole, E., S. Ring, (2006). <i>Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft</i>
	Foreman, P. (2009). <i>Vulnerability Management</i>
	Fry, C., M. Nystrom, (2009). <i>Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks</i>
	Hadnagy, C., (2010). <i>Social Engineering: The Art of Human Hacking</i>
	Koren, I., C.M. Krishna, (2007). <i>Fault-Tolerant Systems</i>
	Rajnovic, D., (2010). <i>Computer Incident Response and Product Security</i>
	Trost, R., (2009). <i>Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century</i>
Business Continuity & Disaster Recovery Planning	Bowman, R.H., (2008). <i>Business Continuity Planning for Data Centers and Systems: A Strategic Implementation Guide</i>
	Buffington, J., (2010). <i>Data Protection for Virtual Data Centers</i>
	Clark, T., (2005). <i>Storage Virtualization: Technologies for Simplifying Data Storage and Management</i>
	Hiles, A., P. Barnes, (2001). <i>The Definitive Handbook of Business Continuity Management</i>
	Little, D.B., D.A. Chapa, (2003). <i>Implementing Backup and Recovery: The Readiness Guide for the Enterprise</i>
	National Fire Protection Association, (2007). <i>NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity</i>
	Preston, C., (2007). <i>Backup & Recovery: Inexpensive Backup Solutions for Open Systems</i>
	Schmidt, K., (2010). <i>High Availability and Disaster Recovery: Concepts, Design, Implementation</i>



Candidate Information Bulletin

Effective Date 1 January 2009

Business Continuity & Disaster Recovery Planning (cont'd)	Snedaker, S., (2007). <i>Business Continuity and Disaster Recovery Planning for IT Professionals</i>
	Toigo, J.W., (2002). <i>Disaster Recovery Planning: Preparing for the Unthinkable (3rd Edition)</i>
Legal, Regulations, Investigations & Compliance	Barrett, D., G. Kipper, (2010). <i>Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments</i>
	Casey, E., (2011). <i>Digital Evidence and Computer Crime, Forensic Science, Computers, and the Internet (3rd Edition)</i>
	Ermann, M.D., M.S. Shauf, (2002). <i>Computers, Ethics, and Society, (3RD Edition)</i>
	Garner, B.A., (2009). <i>Black's Law Dictionary (9th edition)</i>
	Kuner, C., (2007). <i>European Data Protection Law: Corporate Regulation and Compliance</i>
	Mather, T., S. Kumaraswamy, S. Latif, (2009). <i>Cloud Security and Privacy</i>
	Moeller, R.R., (2010). <i>IT Audit, Control, and Security (2 Edition)</i>
	Nissenbaum, H., (2009). <i>Privacy in Context: Technology, Policy, and the Integrity of Social Life</i>
	Proise, C., K. Mandia, (2003). <i>Incident Response and Computer Forensics (2nd Edition)</i>
Van Lindberg, V., (2008). <i>Intellectual Property and Open Source: A Practical Guide to Protecting Code</i>	
Physical (Environmental) Security	Alger, D., (2005). <i>Build the Best Data Center Facility for Your Business</i>
	Arata, A., (2005). <i>Perimeter Security</i>
	Damjanovski, V., (2005). <i>CCTV, Networking and Digital Technology, (2nd Edition)</i>
	Fennelly, L., (2003). <i>Effective Physical Security, (3rd Edition)</i>
	Garcia, M.L., (2005). <i>Vulnerability Assessment of Physical Protection Systems</i>
	Khairallah, M., (2005). <i>Physical Security Systems Handbook: The Design and Implementation of Electronic Security Systems</i>
	Nilsson, F., (2008). <i>Intelligent Network Video: Understanding Modern Video Surveillance Systems</i>
	Schulz, G., (2009). <i>The Green and Virtual Data Center</i>
	Snevely, R. (2002). <i>Enterprise Data Center Design and Methodology</i>



SAMPLE EXAM QUESTIONS

1. Which one of the following is the MOST important security consideration when selecting a new computer facility?

- (A) Local law enforcement response times
- (B) Adjacent to competitors' facilities
- (C) Aircraft flight paths
- (D) Utility infrastructure

Answer - D

2. Which one of the following describes a SYN flood attack?

- (A) Rapid transmission of Internet Relay Chat (IRC) messages
- (B) Creating a high number of half-open connections
- (C) Disabling the Domain Name Service (DNS) server
- (D) Excessive list linking of users and files

Answer - B

3. The typical function of Secure Sockets Layer (SSL) in securing Wireless Application Protocol (WAP) is to protect transmissions

- (A) between the WAP gateway and the wireless device.
- (B) between the web server and WAP gateway.
- (C) from the web server to the wireless device.
- (D) between the wireless device and the base station.

Answer - B



GENERAL EXAMINATION INFORMATION

General Information The doors to all examination rooms will open at 8:00a.m. Examination instructions will begin promptly at 8:30a.m. All examinations will begin at approximately 9:00a.m.

The CISSP® exam will end at approximately 3:00 p.m. All other exams except the CSSLP will end at approximately 12:00 noon. The CSSLP exam will end at approximately 1:00 pm.

Please note there will be no lunch break during the testing period of 9:00 a.m. through 3:00 p.m. However, you are permitted to bring a snack with you. You may, at your option, take a break and eat your snack at the back of the examination room. No additional time will be allotted for breaks.

Examination Admittance Please arrive at 8:00 a.m. when the doors open. Please bring your admission letter to the examination. In order to be admitted, photo identification is also required. You will not be admitted without proper identification. The only acceptable forms of identification are a driver's license, government-issued identification card, or passport. No other written forms of identification will be accepted.

Examination Security Failure to follow oral and written instructions will result in your application being voided and forfeiture of your application fee. Conduct that results in a violation of security or disrupts the administration of the examination could result in the confiscation of your test and dismissal from the examination. In addition, your examination will be considered void and will not be scored. Examples of misconduct include, but are not limited to, the following: writing on anything other than designated examination materials, writing after time is called, looking at another candidate's examination materials, talking with other candidates at any time during the examination period, failing to turn in all examination materials before leaving the testing room.

You must not discuss or share reference materials or any other examination information with any candidate during the entire examination period. You are particularly cautioned not to do so after you have completed the exam and checked out of the test room, as other candidates in the area might be taking a break and still not have completed the examination. You may not attend the examination only to review or audit test materials. You may not copy any portion of the examination for any reason. No examination materials may leave the test room under any circumstances and all examination materials must be turned in and accounted for before leaving the testing room. No unauthorized persons will be admitted into the testing area.

Please be further advised that all examination content is strictly confidential. You may only communicate about the test, or questions on the test, using the appropriate comment forms provided by the examination staff at the test site. At no other time, before, during or after



the examination, may you communicate orally, electronically or in writing with any person or entity about the content of the examination or individual examination questions.

Reference Material Candidates writing on anything other than examination materials distributed by the proctors will be in violation of the security policies above. Reference materials are not allowed in the testing room. Candidates are asked to bring as few personal and other items as possible to the testing area.

Hard copy language translation dictionaries are permitted for the examination, should you choose to bring one to assist you with language conversions. Electronic dictionaries will not be permitted under any circumstances. The Examination Supervisor will fully inspect your dictionary at check-in. Your dictionary may not contain any writing or extraneous materials of any kind. If the dictionary contains writing or other materials or papers, it will not be permitted in the examination room. Additionally, you are not permitted to write in your dictionary at any time during the examination, and it will be inspected a second time prior to dismissal from the examination. Finally, (ISC)² takes no responsibility for the content of such dictionaries or interpretations of the contents by a candidate.

Examination Protocol While the site climate is controlled to the extent possible, be prepared for either warm or cool temperatures at the testing center. Cellular phones and beepers are prohibited in the testing area. The use of headphones inside the testing area is prohibited. Electrical outlets will not be available for any reason. Earplugs for sound suppression are allowed. No smoking or use of tobacco will be allowed inside the testing area. Food and drinks are only allowed in the snack area located at the rear of the examination room. You must vacate the testing area after you have completed the examination. If you require special assistance, you must contact (ISC)² Candidate Services (see address at the bottom of this document) at least one week in advance of the examination date and appropriate arrangements will be made. Due to limited parking facilities at some sites, please allow ample time to park and reach the testing area.

Admission Problems A problem table for those candidates who did not receive an admission notice or need other assistance will be available 30 minutes prior to the opening of the doors.

Examination Format and Scoring

- The CISSP® examination consists of 250 multiple choice questions with four (4) choices each.
- The CSSLP® examination consists of 175 multiple choice questions with four (4) choices each.
- The SSCP® examination contains 125 multiple choice questions with four (4) choices each.
- The ISSAP®, ISSEP®, and ISSMP® concentration examinations contain 125, 150, 125 multiple choice questions respectively with four (4) choices each.



- The Certified Authorization Professional (CAP®) examination contains 125 multiple choice questions with four (4) choices each.

There may be scenario-based items which may have more than one multiple choice question associated with it. These items will be specifically identified in the test booklet.

Each of these exams contains 25 questions which are included for research purposes only. The research questions are not identified; therefore, answer all questions to the best of your ability. Examination results will be based only on the scored questions on the examination. There are several versions of the examination. It is important that each candidate have an equal opportunity to pass the examination, no matter which version is administered. Expert certified information Security Architecture Professionals have provided input as to the difficulty level of all questions used in the examinations. That information is used to develop examination forms that have comparable difficulty levels. When there are differences in the examination difficulty, a mathematical procedure is used to make the scores equal. Because the number of questions required to pass the examination may be different for each version, the scores are converted onto a reporting scale to ensure a common standard. The passing grade required is a scale score of 700 out of a possible 1000 points on the grading scale.

Examination Results Examination results will normally be released, via e mail, within 4 to 6 weeks of the examination date. A comprehensive statistical and psychometric analysis of the score data is conducted prior to the release of scores. A minimum number of candidates must have taken the examination for the analysis to be conducted. Accordingly, depending upon the schedule of test dates for a given cycle, there may be occasions when scores are delayed beyond the 4-6 week time frame in order to complete this critical process. Results WILL NOT be released over the telephone. In order to receive your results, your primary email address must be current and any email address changes must be submitted to (ISC)² Customer Support via email customersupport@isc2.org, or may be updated online in your candidate profile.

Exam Response Information Your answer sheet MUST be completed with your name and other information as required. The answer sheet must be used to record all answers to the multiple-choice questions. Upon completion, you are to wait for the proctor to collect your examination materials. Answers marked in the test booklet will not be counted or graded, and additional time will not be allowed in order to transfer answers to the answer sheet. All marks on the answer sheet must be made with a No. 2 pencil. You must blacken the appropriate circles completely and completely erase any incorrect marks. Only your responses marked on the answer sheet will be considered. An unanswered question will be scored as incorrect. Dress is "business casual" (neat...but certainly comfortable).



Any questions?

Please direct any questions to:

(ISC)² Candidate Services

33920 US Highway 19 North

Suite 205

Palm Harbor, FL 34684

Phone: 1.866.331.ISC2 (4722) in the United States and CA

Phone: 1.727.785.0189 outside the United States and CA

Fax: 1.727.683.0785



CISSP[®]

Candidate Information Bulletin

Effective Date January 1, 2012 (Rev2)





1) ACCESS CONTROL	5
Overview	5
Key Areas of Knowledge	5
2) TELECOMMUNICATIONS AND NETWORK SECURITY	7
Overview	7
Key Areas of Knowledge	7
3) INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT	9
Overview	9
Key Areas of Knowledge	9
4) SOFTWARE DEVELOPMENT SECURITY	12
Overview	12
Key Areas of Knowledge	12
5) CRYPTOGRAPHY	13
Overview	13
Key Areas of Knowledge	13
6) SECURITY ARCHITECTURE & DESIGN	15
Overview	15
Key Areas of Knowledge	15
7) OPERATIONS SECURITY	17
Overview	17
Key Areas of Knowledge	17
8) BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING	19
Overview	19
Key Areas of Knowledge	20
9) LEGAL, REGULATIONS, INVESTIGATIONS AND COMPLIANCE	21
Overview	21
Key Areas of Knowledge	21
10) PHYSICAL (ENVIRONMENTAL) SECURITY	23



Overview	23
Key Areas of Knowledge	23
REFERENCES	25
SAMPLE EXAM QUESTIONS	30
GENERAL EXAMINATION INFORMATION.....	31
Any questions?	34



The Certified Information Systems Security Professional (CISSP) is an information assurance professional who has demonstrated a globally recognized level of competence provided by a common body of knowledge that defines the architecture, design, management, risk and controls that assure the security of business environments.

This Candidate Information Bulletin provides the following:

- Exam blueprint to a limited level of detail that outlines major topics and sub- topics within the domains,
- Suggested reference list,
- Description of the format of the items on the exam, and
- Basic registration/administration policies

Applicants must have a minimum of five years of direct full-time security professional work experience in two or more of the ten domains of the (ISC)² CISSP® CBK® or four years of direct full-time security professional work experience in two or more of the ten domains of the CISSP® CBK® with a four-year college degree. Only one year experience exemption is granted for education.

CISSP professional experience includes but is not limited to:

- Work requiring special education or intellectual attainment, usually including a liberal education or college degree.
- Work requiring habitual memory of a body of knowledge shared by others doing similar work.
- Management/supervision of projects and/or employees.
- Work requiring the exercise of judgment, management decision-making, and discretion.
- Work requiring the exercise of ethical judgment (as opposed to ethical behavior).
- Professional writing and oral communication (e.g., presentation).
- Teaching, instructing, training and the mentoring of others.
- Research and development.
- The specification and selection of controls and mechanisms (i.e. identification and authentication technology- does not include the mere operation of these controls).
- Applicable job title examples are: CISO, Director, Manager, Supervisor, Analyst, Cryptographer, Cyber Architect, Information Assurance Engineer, Instructor, Professor, Lecturer, Investigator, Computer Scientist, Program Manager, Lead, etc.



1) ACCESS CONTROL

Overview

Access Control domain covers mechanisms by which a system grants or revokes the right to access data or perform an action on an information system.

Access Control systems include:

- File permissions, such as "create," "read," "edit," or "delete" on a file server.
- Program permissions, such as the right to execute a program on an application server.
- Data rights, such as the right to retrieve or update information in a database.

CISSP candidates should fully understand access control concepts, methodologies and their implementation within centralized and decentralized environments across an organization's computing environment.

Key Areas of Knowledge

A. Control access by applying the following concepts/methodologies/techniques

- A.1 Policies
- A.2 Types of controls (preventive, detective, corrective, etc.)
- A.3 Techniques (e.g., non-discretionary, discretionary and mandatory)
- A.4 Identification and Authentication
- A.5 Decentralized/distributed access control techniques
- A.6 Authorization mechanisms
- A.7 Logging and monitoring

B. Understand access control attacks

- B.1 Threat modeling
- B.2 Asset valuation
- B.3 Vulnerability analysis
- B.4 Access aggregation



C. Assess effectiveness of access controls

C.1 User entitlement

C.2 Access review & audit

D. Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)



2) TELECOMMUNICATIONS AND NETWORK SECURITY

Overview

The Telecommunications and Network Security domain encompasses the structures, techniques, transport protocols, and security measures used to provide integrity, availability, confidentiality and authentication for transmissions over private and public communication networks.

The candidate is expected to demonstrate an understanding of communications and network security as it relates to data communications in local area and wide area networks, remote access, internet/intranet/extranet configurations. Candidates should be knowledgeable with network equipment such as switches, bridges and routers, as well as networking protocols (e.g., TCP/IP, IPSec), and VPNs.

Key Areas of Knowledge

A. Understand secure network architecture and design (e.g., IP & non-IP protocols, segmentation)

- A.1 OSI and TCP/IP models
- A.2 IP networking
- A.3 Implications of multi-layer protocols

B. Securing network components

- B.1 Hardware (e.g., modems, switches, routers, wireless access points)
- B.2 Transmission media (e.g., wired, wireless, fiber)
- B.3 Network access control devices (e.g., firewalls, proxies)
- B.4 End-point security

C. Establish secure communication channels (e.g., VPN, TLS/SSL, VLAN)

- C.1 Voice (e.g., POTS, PBX, VoIP)
- C.2 Multimedia collaboration (e.g., remote meeting technology, instant messaging)
- C.3 Remote access (e.g., screen scraper, virtual application/desktop, telecommuting)



C.4 Data communications

D. Understand network attacks (e.g., DDoS, spoofing)



3) INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT

Overview

The Information Security Governance and Risk Management domain entails the identification of an organization's information assets and the development, documentation, implementation and updating of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

The candidate is expected to understand the planning, organization, roles and responsibilities of individuals in identifying and securing organization's information assets; the development and use of policies stating management's views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary and private information; third party management and service level agreements related to information security; employment agreements, employee hiring and termination practices, and risk management practices and tools to identify, rate, and reduce the risk to specific resources

Key Areas of Knowledge

A. Understand and align security function to goals, mission and objectives of the organization

B. Understand and apply security governance

- B.1 Organizational processes (e.g., acquisitions, divestitures, governance committees)
- B.2 Security roles and responsibilities
- B.3 Legislative and regulatory compliance
- B.4 Privacy requirements compliance
- B.5 Control frameworks
- B.6 Due care



B.7 Due diligence

C. Understand and apply concepts of confidentiality, integrity and availability

D. Develop and implement security policy

D.1 Security policies

D.2 Standards/baselines

D.3 Procedures

D.4 Guidelines

D.5 Documentation

E. Manage the information life cycle (e.g., classification, categorization, and ownership)

F. Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)

G. Understand and apply risk management concepts

G.1 Identify threats and vulnerabilities

G.2 Risk assessment/analysis (qualitative, quantitative, hybrid)

G.3 Risk assignment/acceptance

G.4 Countermeasure selection

G.5 Tangible and intangible asset valuation

H. Manage personnel security

H.1 Employment candidate screening (e.g., reference checks, education verification)

H.2 Employment agreements and policies

H.3 Employee termination processes

H.4 Vendor, consultant and contractor controls

I. Develop and manage security education, training and awareness

J. Manage the Security Function

J.1 Budget

J.2 Metrics



- J.3 Resources
- J.4 Develop and implement information security strategies
- J.5 Assess the completeness and effectiveness of the security program



4) SOFTWARE DEVELOPMENT SECURITY

Overview

Software Development Security domain refers to the controls that are included within systems and applications software and the steps used in their development (e.g., SDLC).

Software refers to system software (operating systems) and application programs such as agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments.

The candidate should fully understand the security and controls of the systems development process, system life cycle, application controls, change controls, data warehousing, data mining, knowledge-based systems, program interfaces, and concepts used to ensure data and application integrity, security, and availability.

Key Areas of Knowledge

A. Understand and apply security in the software development life cycle

- A.1 Development Life Cycle
- A.2 Maturity models
- A.3 Operation and maintenance
- A.4 Change management

B. Understand the environment and security controls

- B.1 Security of the software environment
- B.2 Security issues of programming languages
- B.3 Security issues in source code (e.g., buffer overflow, escalation of privilege, backdoor)
- B.4 Configuration management

C. Assess the effectiveness of software security



5) CRYPTOGRAPHY

Overview

The Cryptography domain addresses the principles, means, and methods of applying mathematical algorithms and data transformations to information to ensure its integrity, confidentiality and authenticity.

The candidate is expected to know basic concepts within cryptography; public and private key algorithms in terms of their applications and uses; algorithm construction, key distribution and management, and methods of attack; the applications, construction and use of digital signatures to provide authenticity of electronic transactions, and non-repudiation of the parties involved; and the organization and management of the Public Key Infrastructures (PKIs) and digital certificates distribution and management.

Key Areas of Knowledge

A. Understand the application and use of cryptography

- A.1 Data at rest (e.g., Hard Drive)
- A.2 Data in transit (e.g., On the wire)

B. Understand the cryptographic life cycle (e.g., cryptographic limitations, algorithm/protocol governance)

C. Understand encryption concepts

- C.1 Foundational concepts
- C.2 Symmetric cryptography
- C.3 Asymmetric cryptography
- C.4 Hybrid cryptography
- C.5 Message digests
- C.6 Hashing

D. Understand key management processes

- D.1 Creation/distribution
- D.2 Storage/destruction
- D.3 Recovery



D.4 Key escrow

E. Understand digital signatures

F. Understand non-repudiation

G. Understand methods of cryptanalytic attacks

G.1 Chosen plain-text

G.2 Social engineering for key discovery

G.3 Brute Force (e.g., rainbow tables, specialized/scalable architecture)

G.4 Cipher-text only

G.5 Known plaintext

G.6 Frequency analysis

G.7 Chosen cipher-text

G.8 Implementation attacks

H. Use cryptography to maintain network security

I. Use cryptography to maintain application security

J. Understand Public Key Infrastructure (PKI)

K. Understand certificate related issues

L. Understand information hiding alternatives (e.g., steganography, watermarking)



6) SECURITY ARCHITECTURE & DESIGN

Overview

The Security Architecture & Design domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.

Information security architecture and design covers the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that these practices and processes align with the organization's core goals and strategic direction.

The candidate is expected to understand security models in terms of confidentiality, integrity, data flow diagrams; Common Criteria (CC) protection profiles; technical platforms in terms of hardware, firmware, and software; and system security techniques in terms of preventative, detective, and corrective controls.

Key Areas of Knowledge

- A. Understand the fundamental concepts of security models (e.g., Confidentiality, Integrity, and Multi-level Models)***
- B. Understand the components of information systems security evaluation models***
 - B.1 Product evaluation models (e.g., common criteria)
 - B.2 Industry and international security implementation guidelines (e.g., PCI-DSS, ISO)
- C. Understand security capabilities of information systems (e.g., memory protection, virtualization, trusted platform module)***
- D. Understand the vulnerabilities of security architectures***
 - D.1 System (e.g., covert channels, state attacks, emanations)
 - D.2 Technology and process integration (e.g., single point of failure, service oriented architecture)



E. Understand software and system vulnerabilities and threats

- E.1 Web-based (e.g., XML, SAML, OWASP)
- E.2 Client-based (e.g., applets)
- E.3 Server-based (e.g., data flow control)
- E.4 Database security (e.g., inference, aggregation, data mining, warehousing)
- E.5 Distributed systems (e.g., cloud computing, grid computing, peer to peer)

F. Understand countermeasure principles (e.g., defense in depth)



7) OPERATIONS SECURITY

Overview

Security Operations domain is used to identify critical information and the execution of selected measures that eliminate or reduce adversary exploitation of critical information. It includes the definition of the controls over hardware, media, and the operators with access privileges to any of these resources. Auditing and monitoring are the mechanisms, tools and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

The candidate is expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms available, the potential for abuse of access, the appropriate controls, and the principles of good practice.

Key Areas of Knowledge

A. Understand security operations concepts

- A.1 Need-to-know/least privilege
- A.2 Separation of duties and responsibilities
- A.3 Monitor special privileges (e.g., operators, administrators)
- A.4 Job rotation
- A.5 Marking, handling, storing and destroying of sensitive information
- A.6 Record retention

B. Employ resource protection

- B.1 Media management
- B.2 Asset management (e.g., equipment life cycle, software licensing)

C. Manage incident response

- C.1 Detection
- C.2 Response
- C.3 Reporting
- C.4 Recovery



C.5 Remediation and review (e.g., root cause analysis)

D. Implement preventative measures against attacks (e.g., malicious code, zero-day exploit, denial of service)

E. Implement and support patch and vulnerability management

F. Understand change and configuration management (e.g., versioning, baselining)

G. Understand system resilience and fault tolerance requirements



8) BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING

Overview

The Business Continuity and Disaster Recovery Planning domain addresses the preservation of the business in the face of major disruptions to normal business operations. BCP and DRP involve the preparation, testing and updating of specific actions to protect critical business processes from the effect of major system and network failures.

Business Continuity Planning (BCP) helps to identify the organization's exposure to internal and external threats; synthesize hard and soft assets to provide effective prevention and recovery for the organization, and maintains competitive advantage and value system integrity. BCP counteracts interruptions to business activities and should be available to protect critical business processes from the effects of major failures or disasters. It deals with the natural and man-made events and the consequences, if not dealt with promptly and effectively.

Business Impact Analysis (BIA) determines the proportion of impact an individual business unit would sustain subsequent to a significant interruption of computing or telecommunication services. These impacts may be financial, in terms of monetary loss, or operational, in terms of inability to deliver.

Disaster Recovery Plans (DRP) contain procedures for emergency response, extended backup operation and post-disaster recovery, should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objective of the disaster recovery plan is to provide the capability to process mission-essential applications, in a degraded mode, and return to normal mode of operation within a reasonable amount of time.

The candidate is expected to know the difference between business continuity planning and disaster recovery; business continuity planning in terms of project scope and planning, business impact analysis, recovery strategies, recovery plan development, and implementation. Moreover, the candidate should understand disaster recovery in terms of recovery plan development, implementation and restoration.



Key Areas of Knowledge

A. Understand business continuity requirements

A.1 Develop and document project scope and plan

B. Conduct business impact analysis

B.1 Identify and prioritize critical business functions

B.2 Determine maximum tolerable downtime and other criteria

B.3 Assess exposure to outages (e.g., local, regional, global)

B.4 Define recovery objectives

C. Develop a recovery strategy

C.1 Implement a backup storage strategy (e.g., offsite storage, electronic vaulting, tape rotation)

C.2 Recovery site strategies

D. Understand disaster recovery process

D.1 Response

D.2 Personnel

D.3 Communications

D.4 Assessment

D.5 Restoration

D.6 Provide training

E. Exercise, assess and maintain the plan (e.g., version control, distribution)



9) LEGAL, REGULATIONS, INVESTIGATIONS AND COMPLIANCE

Overview

The Legal, Regulations, Investigations and Compliance domain addresses ethical behavior and compliance with regulatory frameworks. It includes the investigative measures and techniques that can be used to determine if a crime has been committed, and methods used to gather evidence (e.g., forensics). A computer crime is any illegal action where the data on a computer is accessed without permission. This includes unauthorized access or alteration of data, or unlawful use of computers and services. This domain also includes understanding the computer incident forensic response capability to identify the Advanced Persistent Threat (APT) that many organizations face today.

Key Areas of Knowledge

A. Understand legal issues that pertain to information security internationally

- A.1 Computer crime
- A.2 Licensing and intellectual property (e.g., copyright, trademark)
- A.3 Import/Export
- A.4 Trans-border data flow
- A.5 Privacy

B. Understand professional ethics

- B.1 (ISC)² Code of Professional Ethics
- B.2 Support organization's code of ethics

C. Understand and support investigations

- C.1 Policy, roles and responsibilities (e.g., rules of engagement, authorization, scope)
- C.2 Incident handling and response
- C.3 Evidence collection and handling (e.g., chain of custody, interviewing)
- C.4 Reporting and documenting



D. Understand forensic procedures

- D.1 Media analysis
- D.2 Network analysis
- D.3 Software analysis
- D.4 Hardware/embedded device analysis

E. Understand compliance requirements and procedures

- E.1 Regulatory environment
- E.2 Audits
- E.3 Reporting

F. Ensure security in contractual agreements and procurement processes (e.g., cloud computing, outsourcing, vendor governance)



10) PHYSICAL (ENVIRONMENTAL) SECURITY

Overview

The Physical (Environmental) Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information. These resources include people, the facility in which they work, and the data, equipment, support systems, media, and supplies they utilize.

Physical security describes measures that are designed to deny access to unauthorized personnel (including attackers) from physically accessing a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts.

The candidate is expected to know the elements involved in choosing a secure site, its design and configuration, and the methods for securing the facility against unauthorized access, theft of equipment and information, and the environmental and safety measures needed to protect people, the facility, and its resources.

Key Areas of Knowledge

- A. Understand site and facility design considerations*
- B. Support the implementation and operation of perimeter security (e.g., physical access control and monitoring, audit trails/access logs)*
- C. Support the implementation and operation of internal security (e.g., escort requirements/visitor control, keys and locks)*
- D. Support the implementation and operation of facilities security (e.g., technology convergence)*
 - D.1 Communications and server rooms
 - D.2 Restricted and work area security
 - D.3 Data center security
 - D.4 Utilities and Heating, Ventilation and Air Conditioning (HVAC) considerations
 - D.5 Water issues (e.g., leakage, flooding)
 - D.6 Fire prevention, detection and suppression
- E. Support the protection and securing of equipment*



F. Understand personnel privacy and safety (e.g., duress, travel, monitoring)



REFERENCES

This reference list is **NOT** intended to be an all-inclusive collection representing the CISSP® Core Body of Knowledge (CBK®). Its purpose is to provide candidates a starting point for their studies in domains which need supplementary learning in order to complement their associated level of work and academic experience. Candidates may also consider other references, which are not on this list but adequately cover domain content.

Note: (ISC)² does not endorse any particular text or author and does not imply that any or all references be acquired or consulted. (ISC)² does not imply nor guarantee that the study of these references will result in an examination pass.

Domain	Supplementary Reference
Access Control	Bertino, E., K. Takahashi, (2010). <i>Identity Management: Concepts, Technologies, and Systems</i>
	Chin, S-K., S.B. Older (2010). <i>Access Control, Security, and Trust: A Logical Approach</i>
	Ferraiolo, D.F., D.R. Kuhn, R. Chandramouli, (2007). <i>Role-Based Access Control (2nd Edition)</i>
	Kayem, A.V., S.G. Akl, P. Martin, (2010). <i>Adaptive Cryptographic Access Control</i>
	Konicek, J., (1997). <i>Security, ID Systems and Locks: The Book on Electronic Access Control</i>
	Links, C.L., (2008). <i>IAM Success Tips (Volumes 1-3)</i>
	Newman, R., (2009). <i>Security and Access Control Using Biometric Technologies: Application, Technology, and Management</i>
	Rankl, W., W. Effing, (2010). <i>Smart Card Handbook</i>
	Tipton, H.F., M.K. Nozaki, (2011). <i>Information Security Management Handbook (2011 CD-ROM Edition)¹</i>
	Vacca, J.R., (2010). <i>Biometric Technologies and Verification Systems</i>
Telecommunications and Network Security	Cheswick, W.R., S.M. Bellovin, A.D. Rubin, (2003). <i>Firewalls and Internet Security: Repelling the Wily Hacker (2nd Edition)</i>
	Daniel V. Hoffman, D.V., (2008). <i>Implementing NAP and NAC Security Technologies: The Complete Guide to Network Access Control</i>
	Davis, C., (2001). <i>IPSec: Securing VPNs</i>
	Hogg, S., E. Vyncke, (2008). <i>IPv6 Security</i>
	Kadrich, M., (2007). <i>Endpoint Security</i>

¹ This reference can be used for multiple domains.



Telecommunications and Network Security (cont')	Luotonen, A., (1997). <i>Web Proxy Servers</i>
	Porter, T., J. Kanclirz, B. Baskin, (2006). <i>Practical VoIP Security</i>
	Prowell, S., R.Kraus, M. Borkin, (2010). <i>Seven Deadliest Network Attacks</i>
	Stevens, W.R., G.R. Wright, (2001). <i>TCP/IP Illustrated (3 Volume Set)</i>
	Wetteroth, D., (2001). <i>OSI Reference Model for Telecommunications</i>
Information Security Governance and Risk Management	(ISC) ² , <i>Code of Ethics</i> (https://www.isc2.org/ethics/default.aspx)
	Bacik, S., (2008). <i>Building an Effective Information Security Policy Architecture</i>
	Brotby, K., (2010). <i>Information Security Governance</i>
	Calder, A., S. Watkins, (2008). <i>IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002</i>
	Hayden, L., (2010). <i>IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data</i>
	Herold, R., (2010). <i>Managing an Information Security and Privacy Awareness and Training Program, (2nd Edition)</i>
	Jaquith, A., (2007). <i>Security Metrics: Replacing Fear, Uncertainty, and Doubt</i>
	Landoll, D.J., (2005). <i>The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments</i>
	Thomas L. Norman, T.L., (2009). <i>Risk Analysis and Security Countermeasure Selection</i>
Software Development Security	Tipton, H.F., (2009). <i>Official (ISC)2 Guide to the CISSP CBK, (2nd Edition)²</i>
	Whitman, M.E., H.J. Mattord, (2010). <i>Management of Information Security (3rd Edition)</i>
	Allen, J.A., S.J. Barnum, R.J. Ellison, G. McGraw, N.R. Mead, (2008). <i>Software Security Engineering: A Guide for Project Managers</i>
	Chess, B., J. West, (2007). <i>Secure Programming with Static Analysis</i>
	Clarke, J., (2009). <i>SQL Injection Attacks and Defense</i>
	Dowd, M., J. McDonald, J. Schuh, (2006). <i>The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities</i>
	Dwivedi, H., (2010). <i>Mobile Application Security</i>
	Howard, M., D. LeBlanc, J. Viega, (2009). <i>24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them</i>
	Howard, M., S. Lipner, (2006). <i>The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software</i>
	Ligh, M., S. Adair, B. Hartstein, M. Richard, (2010). <i>Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code</i>
Stuttard, D., M. Pinto, (2007). <i>The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws</i>	

² This reference can be used for multiple domains.



Candidate Information Bulletin

Effective Date 1 January 2012

Cryptography	Boudriga, N., (2009). <i>Security of Mobile Communications</i>
	Cole, E., (2003). <i>Hiding in Plain Sight: Steganography and the Art of Covert Communication</i>
	D. Hankerson, A.J. Menezes, S. Vanstone, (2010). <i>Guide to Elliptic Curve Cryptography</i>
	Daemen, J., V. Rijmen, (2002). <i>The Design of Rijndael: AES - The Advanced Encryption Standard</i>
	Garfinkel, S., (1994). <i>PGP: Pretty Good Privacy</i>
	Karamanian, A., S. Tennesi, (2011). <i>PKI Uncovered: Certificate-Based Security Solutions for Next-Generation Networks</i>
	Menezes, A.J., P. van Oorschot, S. Vanstone, (1996). <i>Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)</i>
	Schneier, B., (1996). <i>Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd Edition)</i>
	Tennoe, L.M., M.T. Henssonow, S.F. Surhone, (2010). <i>Tokenization (Data Security)</i>
	W. Stallings, (2010). <i>Cryptography and Network Security: Principles and Practice (5th Edition)</i>
Security Architecture and Design	Anderson, R.J., (2008). <i>Security Engineering: A Guide to Building Dependable Distributed Systems³</i>
	Challener, C., K. Yoder, R. Catherman, D. Safford, L.V. Doorn, (2008). <i>A Practical Guide to Trusted Computing</i>
	Gillis, T., (2010). <i>Securing the Borderless Network: Security for the Web 2.0 World</i>
	Higaki, W.H., Y. Higaki, (2010). <i>Successful Common Criteria Evaluations: A Practical Guide for Vendors</i>
	Kanneganti, R., P.R. Chodavarapu, (2008). <i>SOA Security</i>
	Kenan, K., (2005). <i>Cryptography in the Database: The Last Line of Defense</i>
	Petkovic, M., W. Jonker, (2010). <i>Security, Privacy, and Trust in Modern Data Management</i>
	Santos, O., (2007). <i>End-to-End Network Security: Defense-in-Depth</i>
	Shimonski, R., W. Schmied, V. Chang, T.W. Shinder, (2003). <i>Building DMZs For Enterprise Networks</i>
	Swiderski, F., W. Snyder, (2004). <i>Threat Modeling</i>

³ This reference can be used for multiple domains.



Candidate Information Bulletin

Effective Date 1 January 2012

Security Operations	Aiello, R., (2010). <i>Configuration Management Best Practices: Practical Methods that Work in the Real World</i>
	Bejtlich, R., (2005). <i>Extrusion Detection: Security Monitoring for Internal Intrusions</i>
	Bosworth, S., M. E. Kabay, E. Whyne, (2009). <i>Computer Security Handbook (2 Volume Set)</i>
	Cole, E., S. Ring, (2006). <i>Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft</i>
	Foreman, P. (2009). <i>Vulnerability Management</i>
	Fry, C., M. Nystrom, (2009). <i>Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks</i>
	Hadnagy, C., (2010). <i>Social Engineering: The Art of Human Hacking</i>
	Koren, I., C.M. Krishna, (2007). <i>Fault-Tolerant Systems</i>
	Rajnovic, D., (2010). <i>Computer Incident Response and Product Security</i>
	Trost, R., (2009). <i>Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century</i>
Business Continuity and Disaster Recovery Planning	Bowman, R.H., (2008). <i>Business Continuity Planning for Data Centers and Systems: A Strategic Implementation Guide</i>
	Buffington, J., (2010). <i>Data Protection for Virtual Data Centers</i>
	Clark, T., (2005). <i>Storage Virtualization: Technologies for Simplifying Data Storage and Management</i>
	Hiles, A., P. Barnes, (2001). <i>The Definitive Handbook of Business Continuity Management</i>
	Little, D.B., D.A. Chapa, (2003). <i>Implementing Backup and Recovery: The Readiness Guide for the Enterprise</i>
	National Fire Protection Association, (2007). <i>NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity</i>
	Preston, C., (2007). <i>Backup & Recovery: Inexpensive Backup Solutions for Open Systems</i>
	Schmidt, K., (2010). <i>High Availability and Disaster Recovery: Concepts, Design, Implementation</i>
	Snedaker, S., (2007). <i>Business Continuity and Disaster Recovery Planning for IT Professionals</i>
	Toigo, J.W., (2002). <i>Disaster Recovery Planning: Preparing for the Unthinkable (3rd Edition)</i>
Legal, Regulations, Investigations and Compliance	Barrett, D., G. Kipper, (2010). <i>Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments</i>
	Casey, E., (2011). <i>Digital Evidence and Computer Crime, Forensic Science, Computers, and the Internet (3rd Edition)</i>
	Ermann, M.D., M.S. Shauf, (2002). <i>Computers, Ethics, and Society, (3rd Edition)</i>



Candidate Information Bulletin

Effective Date 1 January 2012

Legal, Regulations, Investigations and Compliance (cont'd)	Garner, B.A., (2009). <i>Black's Law Dictionary (9th edition)</i>
	Kuner, C., (2007). <i>European Data Protection Law: Corporate Regulation and Compliance</i>
	Mather, T., S. Kumaraswamy, S. Latif, (2009). <i>Cloud Security and Privacy</i>
	Moeller, R.R., (2010). <i>IT Audit, Control, and Security (2 Edition)</i>
	Nissenbaum, H., (2009). <i>Privacy in Context: Technology, Policy, and the Integrity of Social Life</i>
	Proise, C., K. Mandia, (2003). <i>Incident Response and Computer Forensics (2nd Edition)</i>
	Van Lindberg, V., (2008). <i>Intellectual Property and Open Source: A Practical Guide to Protecting Code</i>
Physical (Environmental) Security	Alger, D., (2005). <i>Build the Best Data Center Facility for Your Business</i>
	Arata, A., (2005). <i>Perimeter Security</i>
	Damjanovski, V., (2005). <i>CCTV, Networking and Digital Technology, (2nd Edition)</i>
	Fennelly, L., (2003). <i>Effective Physical Security, (3rd Edition)</i>
	Garcia, M.L., (2005). <i>Vulnerability Assessment of Physical Protection Systems</i>
	Khairallah, M., (2005). <i>Physical Security Systems Handbook: The Design and Implementation of Electronic Security Systems</i>
	Nilsson, F., (2008). <i>Intelligent Network Video: Understanding Modern Video Surveillance Systems</i>
	Schulz, G., (2009). <i>The Green and Virtual Data Center</i>
Snevely, R. (2002). <i>Enterprise Data Center Design and Methodology</i>	



SAMPLE EXAM QUESTIONS

1. Which one of the following is the MOST important security consideration when selecting a new computer facility?

- (A) Local law enforcement response times
- (B) Adjacent to competitors' facilities
- (C) Aircraft flight paths
- (D) Utility infrastructure

Answer - D

2. Which one of the following describes a SYN flood attack?

- (A) Rapid transmission of Internet Relay Chat (IRC) messages
- (B) Creating a high number of half-open connections
- (C) Disabling the Domain Name Service (DNS) server
- (D) Excessive list linking of users and files

Answer - B

3. The typical function of Secure Sockets Layer (SSL) in securing Wireless Application Protocol (WAP) is to protect transmissions

- (A) between the WAP gateway and the wireless device.
- (B) between the web server and WAP gateway.
- (C) from the web server to the wireless device.
- (D) between the wireless device and the base station.

Answer - B



GENERAL EXAMINATION INFORMATION

General Information The doors to all examination rooms will open at 8:00a.m. Examination instructions will begin promptly at 8:30a.m. All examinations will begin at approximately 9:00a.m.

The maximum duration of the CISSP® exam is 6 hours. The maximum duration of all other exams except the CSSLP® is 3 hours. The CSSLP® candidates are allowed a maximum of 4 hours to complete the exam.

Please note there will be no lunch break during the testing period. However, you are permitted to bring a snack with you. You may, at your option, take a break and eat your snack at the back of the examination room. No additional time will be allotted for breaks.

Examination Admittance Please arrive at 8:00a.m. when the doors are opened. Please bring your admission letter to the examination site. In order to be admitted, photo identification is also required. You will not be admitted without proper identification. The only acceptable forms of identification are a driver's license, government-issued identification card, or passport. No other written forms of identification will be accepted.

Examination Security Failure to follow oral and written instructions will result in your application being voided and application fee being forfeited. Conduct that results in a violation of security or disrupts the administration of the examination could result in the confiscation of your test and your dismissal from the examination. In addition, your examination will be considered void and will not be scored. Examples of misconduct include, but are not limited to, the following: writing on anything other than designated examination materials, writing after time is called, looking at another candidate's examination materials, talking with other candidates at any time during the examination period, failing to turn in all examination materials before leaving the testing room.

You must not discuss or share reference materials or any other examination information with any candidate during the entire examination period. You are particularly cautioned not to do so after you have completed the exam and checked out of the test room, as other candidates in the area might be taking a break and still not have completed the examination. You may not attend the examination only to review or audit test materials. You may not copy any portion of the examination for any reason. No examination materials may leave the test room under any circumstances and all examination materials must be turned in and accounted for before leaving the testing room. No unauthorized persons will be admitted into the testing area.



Please be further advised that all examination content is strictly confidential. You may only communicate about the test, or questions on the test, using the appropriate comment forms provided by the examination staff at the test site. At no other time, before, during or after the examination, may you communicate orally, electronically or in writing with any person or entity about the content of the examination or individual examination questions.

Reference Material Candidates writing on anything other than examination materials distributed by the proctors will be in violation of the security policies above. Reference materials are not allowed in the testing room. Candidates are asked to bring as few personal and other items as possible to the testing area.

Hard copies of language translation dictionaries are permitted for the examination, should you choose to bring one to assist you with language conversions. Electronic dictionaries will not be permitted under any circumstances. The Examination Supervisor will fully inspect your dictionary at check-in. Your dictionary may not contain any writing or extraneous materials of any kind. If the dictionary contains writing or other materials or papers, it will not be permitted in the examination room. Additionally, you are not permitted to write in your dictionary at any time during the examination, and it will be inspected a second time prior to dismissal from the examination. Finally, (ISC)² takes no responsibility for the content of such dictionaries or interpretations of the contents by a candidate.

Examination Protocol While the site climate is controlled to the extent possible, be prepared for either warm or cool temperatures at the testing center. Cellular phones and beepers are prohibited in the testing area. The use of headphones inside the testing area is prohibited. Electrical outlets will not be available for any reason. Earplugs for sound suppression are allowed. No smoking or use of tobacco products will be allowed inside the testing area. Food and drinks are only allowed in the snack area located at the rear of the examination room. You must vacate the testing area after you have completed the examination. If you require special assistance, you must contact (ISC)² Candidate Services (see address at the bottom of this document) at least one week in advance of the examination date and appropriate arrangements will be made. Due to limited parking facilities at some sites, please allow ample time to park and reach the testing area.

Admission Problems A problem table for those candidates who did not receive an admission notice or need other assistance will be available 30 minutes prior to the opening of the doors.

Examination Format and Scoring

- The CISSP® examination consists of 250 multiple choice questions with four (4) choices each.
- The CSSLP® examination consists of 175 multiple choice questions with four (4) choices each.



- The SSCP® examination contains 125 multiple choice questions with four (4) choices each.
- The ISSAP®, ISSEP®, and ISSMP® concentration examinations contain 125, 150, 125 multiple choice questions respectively with four (4) choices each.
- The Certified Authorization Professional (CAP®) examination contains 125 multiple choice questions with four (4) choices each. Also, administered in computers.

There may be scenario-based items which may have more than one multiple choice question associated with it. These items will be specifically identified in the test booklet.

Each of these exams contains 25 questions which are included for research purposes only. The research questions are not identified; therefore, answer all questions to the best of your ability. There is no penalty for guessing, so candidates should not leave any item unanswered. Examination results will be based only on the scored questions on the examination. There are several versions of the examination. It is important that each candidate have an equal opportunity to pass the examination, no matter which version is administered. Subject Matter Experts (SMEs) have provided input as to the difficulty level of all questions used in the examinations. That information is used to develop examination forms that have comparable difficulty levels. When there are differences in the examination difficulty, a mathematical procedure called equating is used to make the difficulty level of each test form equal. Because the number of questions required to pass the examination may be different for each version, the scores are converted onto a reporting scale to ensure a common standard. The passing grade required is a scale score of 700 out of a possible 1000 points on the grading scale.

Examination Results Examination results will normally be released, via e mail, within 4 to 6 weeks of the examination date. A comprehensive statistical and psychometric analysis of the score data is conducted prior to the release of scores. A minimum number of candidates must have taken the examination for the analysis to be conducted. Accordingly, depending upon the schedule of test dates for a given cycle, there may be occasions when scores are delayed beyond the 4-6 week time frame in order to complete this critical process. If the test is administered via computers, candidates' pass/fail status is provided at the end of the testing on the site. Results WILL NOT be released over the telephone. In order to receive your results, your primary email address must be current and any email address changes must be submitted to (ISC) ² Customer Support via email customersupport@isc2.org, or may be updated online in your candidate profile.

Exam Response Information Your answer sheet MUST be completed with your name and other information as required. The answer sheet must be used to record all answers to the multiple-choice questions. Upon completion, you are to wait for the proctor to collect your examination materials. Answers marked in the test booklet will not be counted or graded, and



additional time will not be allowed in order to transfer answers to the answer sheet. All marks on the answer sheet must be made with a No. 2 pencil. You must blacken the appropriate circles completely and completely erase any incorrect marks. Only your responses marked on the answer sheet will be considered. An unanswered question will be scored as incorrect. Dress is "business casual" (neat...but certainly comfortable).

Any questions?

Please direct any questions to:

(ISC)² Candidate Services

33920 US Highway 19 North

Suite 205

Palm Harbor, FL 34684

Phone: 1.866.331.ISC2 (4722) in the United States and CA

Phone: 1.727.785.0189 outside the United States and CA

Fax: 1.727.683.0785