

2012 CIB Updates

CISSP – SSCP – ISSEP



What is Changing?

There are three (ISC)² certifications that have had changes posted in Candidate Information Bulletins (CIBs) for 2012



CISSP

- One domain name change
- Domain order re-arranged for educational material
- Rewording of some domain subheadings plus new material



SSCP

- **NO** changes to domain names
- Rewording of some domain subheadings plus new material



ISSEP

- Two domain name changes
- Rewording of some domain subheadings plus new material

CISSP – Domain Changes

The “*Application Development Security*” domain has now become the “*Software Development Security*” domain.

Old

1	ACCESS CONTROL
2	APPLICATION DEVELOPMENT SECURITY
3	BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING
4	CRYPTOGRAPHY
5	INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT
6	LEGAL, REGULATIONS, INVESTIGATIONS AND COMPLIANCE
7	OPERATIONS SECURITY
8	PHYSICAL AND ENVIROMENTAL SECURITY
9	SECURITY ARCHITECTURE & DESIGN
10	TELECOMMUNICATIONS & NETWORK SECURITY

New

1	ACCESS CONTROL
2	TELECOMMUNICATIONS & NETWORK SECURITY
3	INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT
4	SOFTWARE DEVELOPMENT SECURITY
5	CRYPTOGRAPHY
6	SECURITY ARCHITECTURE & DESIGN
7	OPERATIONS SECURITY
8	BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING
9	LEGAL, REGULATIONS, INVESTIGATIONS AND COMPLIANCE
10	PHYSICAL (ENVIRONMENTAL) SECURITY

CISSP – Domain Updates

NOTES	NEW CODE	TOPIC DESCRIPTION
1. ACCESS CONTROLS		
new	1.B.1	Threat modeling
new	1.B.2	Asset valuation
new	1.B.3	Vulnerability analysis
new	1.B.4	Access aggregation
new	1.C.1	User entitlement
new	1.C.2	Access review & audit
new	1.D	Identity and access provisioning lifecycle (e.g., provisioning, review, revocation)
2. TELECOMMUNICATIONS & NETWORK SECURITY		
reworded	2.A	Understand secure network architecture and design (e.g., IP & non-IP protocols, segmentation)
new	2.A.1	OSI and TCP/IP models
new	2.A.2	IP networking
new	2.A.3	Implications of multi-layer protocols
reworded	2.B.1	Hardware (e.g., modems, switches, routers, wireless access points)
reworded	2.B.2	Transmission media (e.g., wired, wireless, fiber)
reworded	2.B.3	Network access control devices (e.g., firewalls, proxies)
reworded	2.C	Establish secure communication channels (e.g., VPN, TLS/SSL, VLAN)
reworded	2.C.1	Voice (e.g., POTS, PBX, VoIP)
reworded	2.C.3	Remote access (e.g., screen scraper, virtual application/desktop, telecommuting)
reworded	2.C.4	Data communications
reworded	2.D	Understand network attacks (e.g., DDoS, spoofing, session highjack)

CISSP – Domain Updates (continued)

NOTES	NEW CODE	TOPIC DESCRIPTION
	3.	INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT
reworded	3.B.1	Organizational processes (e.g., acquisitions, divestitures, governance committees)
reworded	3.B.2	Security roles and responsibilities
reworded	3.E	Manage the information life cycle (e.g., classification, categorization, and ownership)
new	3.F	Manage third-party governance (e.g., on-site assessment, document exchange and review, process/policy review)
reworded	3.G.2	Risk assessment/analysis (qualitative, quantitative, hybrid)
new	3.G.5	Tangible and intangible asset valuation
reworded	3.H	Manage personnel security
reworded	3.H.1	Employment candidate screening (e.g., reference checks, education verification, background checks)
reworded	3.J	Manage the Security Function
new	3.J.1	Budget
new	3.J.2	Metrics
reworded	4.	SOFTWARE DEVELOPMENT SECURITY
reworded	4.A	Understand and apply security in the software development life cycle
reworded	4.A.1	Development Life Cycle
reworded	4.B	Understand the environment and security controls
reworded	4.B.1	Security of the software environment
reworded	4.B.3	Security issues in source code (e.g., buffer overflow, escalation of privilege, backdoor)
reworded	4.C	Assess the effectiveness of software security
reworded	4.C.1	Certification and accreditation (i.e., system authorization)

CISSP – Domain Updates (continued)

NOTES	NEW CODE	TOPIC DESCRIPTION
	5.	CRYPTOGRAPHY
new	5.B	Understand the cryptographic life cycle (e.g., cryptographic limitations, algorithm/protocol governance)
reworded	5.G.3	Brute Force (e.g., rainbow tables, specialized/scalable architecture, GPUs, CUDA)
reworded	5.H	Use cryptography to maintain network security
reworded	5.I	Use cryptography to maintain application security
	6.	SECURITY ARCHITECTURE & DESIGN
reworded	6.E.1	Web-based (e.g., XML, SAML, OWASP)
reworded	6.E.4	Database security (e.g., inference, aggregation, data mining, warehousing)
new	6.E.5	Distributed systems (e.g., cloud computing, grid computing, peer to peer)
	7.	OPERATIONS SECURITY
reworded	7.A	Understand security operations concepts
reworded	7.B.2	Asset management (e.g., equipment life cycle, software licensing)
reworded	7.C.5	Remediation and review (e.g., root cause analysis)
reworded	7.D	Preventive measures against attacks (e.g., malicious code, zero-day exploit, denial of service)
reworded	7.F	Understand change and configuration management (e.g., versioning, baselining)
reworded	7.G	Understand system resilience and fault tolerance requirements
	8.	BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING
reworded	8.E	Exercise, assess and maintain the plan (e.g., version control, distribution)
reworded	10.F	Personnel privacy and safety (e.g., duress, travel, monitoring)

CISSP – Domain Updates (continued)

NOTES	NEW CODE	TOPIC DESCRIPTION
9. LEGAL, REGULATIONS, INVESTIGATIONS AND COMPLIANCE		
new	9.B	Understand professional ethics
new	9.B.1	(ISC)2 Code of Professional Ethics
new	9.B.2	Support organization's code of ethics
reworded	9.C.1	Policy, roles and responsibilities (e.g., rules of engagement, authorization, scope)
new	9.D.4	Hardware/embedded device analysis
reworded	9.F	Ensure security in contractual agreements and procurement processes (e.g., cloud computing, outsourcing, vendor governance)
10. PHYSICAL (ENVIRONMENTAL) SECURITY		
reworded	10.A	Understand site and facility design considerations
reworded	10.D	Support the implementation and operation of facilities security (e.g., technology, physical, and network convergence)
reworded	10.F	Personnel privacy and safety (e.g., duress, travel, monitoring)

SSCP – Domain Updates

NOTES	NEW CODE	TOPIC DESCRIPTION
1.- ACCESS CONTROLS		
Reworded	1.D	Apply Access Control Concepts (e.g., least privilege, and separation of duties)
New	1.D.1	Discretionary Access Control (DAC)
New	1.D.2	Non-discretionary Access Control
Reworded	1.E	Manage Internetwork Trust Architectures (e.g., extranet, third party connections, federated access)
New	1.F	Implement identity management
New	1.F.1	Provisioning
New	1.F.2	Maintenance
New	1.F.3	Entitlement
New	1.G	Understand basic security concepts related to cloud computing (e.g., virtualization, data control, storage, privacy, compliance)
2.- SECURITY OPERATIONS & ADMINISTRATION		
New	2.B	Perform Security Administrative Duties
New	2.B.1	Maintain adherence to security policies, baselines, standards, and procedures
New	2.B.2	Validate security controls
New	2.B.3	Data classification (e.g., control, handling, categorization)
New	2.B.4	Asset management (e.g., hardware, software, data)
New	2.B.5	Develop and maintain systems and security control documentation
Reworded	2.C	Perform Change Management Duties
Reworded	2.C.1	Assist with implementation of Configuration Management Plan
Reworded	2.C.2	Understand the impact of changes to the environment
New	2.C.3	Test patches, fixes, and updates (e.g., operating system, applications, SDLC)
New	2.D.1	Support certification and accreditation (i.e., security authorization)
Reworded	2.E	Participate in Security Awareness Education

SSCP – Domain Updates (continued)

NOTES	NEW CODE	TOPIC DESCRIPTION
	2.-	SECURITY OPERATIONS & ADMINISTRATION (Continued)
New	2.F.1	Understand impact of security testing
Reworded	2.G	Understand concepts of endpoint device security (e.g., virtualization, thin clients, thick clients, USB devices, mobile devices)
New	2.H	Comply with data management policies (e.g., storage media (paper or electronic), transmission, archiving, retention requirements, destruction, deduplication, data loss prevention, social network usage, information rights management (IRM))
New	2.I	Understand security concepts (e.g., confidentiality, integrity, availability, privacy)
	3.-	MONITORING AND ANALYSIS
Reworded	3.A	Maintain Effective Monitoring Systems (e.g., continuous monitoring)
Reworded	3.A.3	Review systems for unauthorized changes (e.g., file integrity checkers, honeypots, unauthorized connections)
New	3.A.5	Install and configure agents and management systems
	4.-	RISK, RESPONSE, AND RECOVERY
Reworded	4.A	Understand Risk Management Process
Reworded	4.A.1	Understand risk management concepts (e.g., impacts, threats, vulnerabilities)
Reworded	4.A.3	Support mitigation activity (e.g., safeguards, countermeasures)
New	4.A.4	Address audit findings
Reworded	4.B	Perform Security Assessment Activities
Reworded	4.B.4	Interpret results of scanning and testing
Reworded	4.C.2	Understand the concepts of forensic investigations (e.g., first responder, evidence handling, chain of custody, preservation of scene)
Reworded	4.D	Understand and support Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
Reworded	4.D.1	Understand the Components of a Business Continuity Plan (BCP)
Reworded	4.D.2	Understand and support Disaster Recovery Plan (DRP)
	5.-	CRYPTOGRAPHY
New	5.A.1	Install and maintain cryptographic systems
Reworded	5.C	Support Certificate and Key Management
New	5.C.1	Understand basic key management concepts (e.g., public key infrastructure)
Reworded	5.C.2	Administration and validation (e.g., key creation, exchange, revocation, escrow)
Reworded	5.D	Understand the use of Secure Protocols (e.g., differences in implementation, appropriate use)

SSCP – Domain Updates (continued)

NOTES	NEW CODE	TOPIC DESCRIPTION
6.- NETWORKS AND COMMUNICATIONS		
Reworded	6.A	Understand security issues related to Networks
New	6.A.2	Network topographies and relationships (e.g., token ring, star, bus, ethernet)
Reworded	6.A.3	Commonly used ports and protocols
Reworded	6.A.5	Network security concepts (e.g., address translation, defense in depth, IP addressing)
Reworded	6.B.2	Common Vulnerabilities
Reworded	6.C.2	Common Vulnerabilities
Reworded	6.D.1	Methods (e.g., application filtering, packet filtering, stateful/stateless inspection)
Reworded	6.D.2	Types (e.g., host based, network based)
Reworded	6.D.3	Common Vulnerabilities
Reworded	6.E	Understand Wireless and Cellular Technologies
Reworded	6.E.2	Technology (e.g., Bluetooth, RFID, 802.11, WiMax, GSM, 3G, NFC)
Reworded	6.E.3	Common Vulnerabilities
7.- MALICIOUS CODE & ACTIVITY		
Reworded	7.A	Identify Malicious Code (e.g., virus, worms, trojan horses, logic bombs)
Reworded	7.A.1	Understand concepts of rootkits
Reworded	7.A.2	Understand types of malware (e.g., spyware, scareware, ransomware)
Reworded	7.A.3	Understand concepts of Trapdoors & Backdoors
Reworded	7.A.4	Understand concepts of Botnets
Reworded	7.A.5	Understand concepts of Mobile Code
Reworded	7.B.2	Deploy and manage anti-malware
Reworded	7.B.4	Software Security (e.g., code signing, application review, server side input validation)
Reworded	7.C	Identify Malicious Activity (e.g., social engineering, insider threat, data theft, DDoS, spoofing, phishing, pharming, spam)
New	7.C.1	Understand malicious web activity (e.g., cross site scripting, cross site request forgery, injection, social networking attacks)
New	7.C.2	Understand the concept of zero day exploits

ISSEP – Domain Changes

- A. The “***Certification and Accreditation (C&A)***” domain has now become the “***Certification and Accreditation (C&A)/Risk Management Framework (RMF)***” domain.
- B. The “***U.S. Government Information Assurance (IA) Governance (e.g., laws regulations, policies, guidelines, standards)***” domain has now become the “***U.S. Government Information Assurance Related Policies and Issuances***” domain.

OLD ISSEP Domains (Effective: March 13, 2010)		NEW ISSEP Domains (Effective: March 2012 – Notice: July 1, 2011)	
Domain 1	System Security Engineering	Domain 1	Systems Security Engineering
Domain 2	Certification and Accreditation (C&A)	Domain 2	Certification and Accreditation (C&A) / Risk Management Framework (RMF)
Domain 3	Technical Management	Domain 3	Technical Management
Domain 4	U.S. Government Information Assurance (IA) Governance (e.g., laws, regulations, policies, guidelines, standards)	Domain 4	U.S. Government Information Assurance Related Policies and Issuances

ISSEP – Domain Updates

NOTES	NEW CODE	TOPIC DESCRIPTION
	1.	Systems Security Engineering
Reworded	1.A.1	Understand security and systems engineering methodologies (e.g., Institute of Electrical and Electronics Engineers , (IEEE) 1220, INCOSE Systems Engineering Handbook)
Reworded	1.A.2	Understand process models (e.g., lifecycle models, Systems Security Engineering Capability Maturity Model (ISO/IEC 21827), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15288)
Reworded	1.B.3	Identify data types and determine additional legal / regulatory requirements
Reworded	1.C.1	Develop system security context (e.g., support system, application)
Reworded	1.C.4	Review design constraints
Reworded	1.C.5	Assess information protection effectiveness
Reworded	1.F.1	Support security implementation, integration and test
Reworded	2.	Certification and Accreditation (C&A) / Risk Management Framework (RMF)
Reworded	2.A	Understand the U.S. Government C&A/RMF process to be applied (e.g., National Information Assurance Certification and Accreditation Process (NIACAP), DoD Information Assurance Certification and Accreditation Process (DIACAP), National Institute of Standards and Technology Special Publication(NIST SP) 800-37 rev 1)
Reworded	2.A.1	Understand the purpose of C&A/RMF
Reworded	2.A.2	Identify and understand criteria used to determine applicability of U.S. Government C&A/RMF processes
Reworded	2.B	Understand the roles and responsibilities of stakeholders identified within the C&A/RMF process

ISSEP – Domain Updates (continued)

NOTES	NEW CODE	TOPIC DESCRIPTION
Reworded	2.	Certification and Accreditation (C&A) / Risk Management Framework (RMF) (continued)
Note -		Section C (<i>Understand Risk Management</i>) from the previous version has been removed and the old Section D is now Section C in the 2012 CIB
Reworded	2.C	Integrate the C&A/RMF processes with systems security engineering
Reworded	2.C.1	Understand the attributes and significance of well-defined, integrated processes (e.g., administrative security policies/procedures and its relationship to C&A/RMF)
Reworded	2.C.7	Identify and correlate C&A/RMF phases and tasks with systems engineering phases and tasks
Reworded	2.C.9	Support C&A/RMF activities as appropriate based on C&A/RMF tailoring (e.g., register system with the appropriate information assurance program, communicate results of risk analysis to certifier and accreditor, prepare and present C&A/RMF documentation to accreditor, submit reports to centralized database)
	3.	Technical Management
Note -		No changes in Domain 3 from the previous version
Reworded	4.	U.S. Government Information Assurance Related Policies and Issuances
Reworded	4.A	Understand national laws and policies
Reworded	4.B	Understand civil agency policies and guidelines
Reworded	4.C	Understand DoD policies and guidelines
Reworded	4.D	Understand applicable international standards