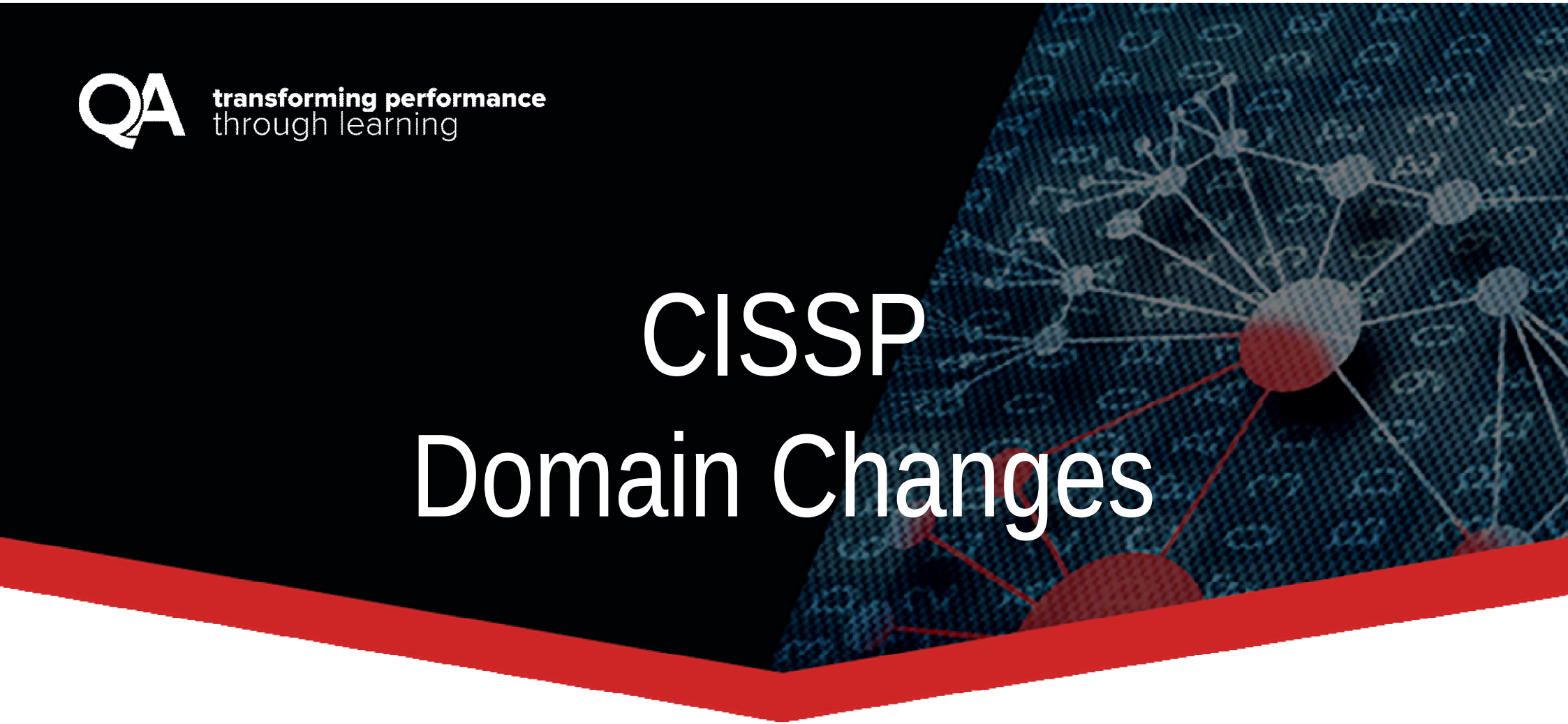


CISSP 8 Domains: Effective Date of Change: April 15th 2015

Domain Changes

CISSP 10 Domains:

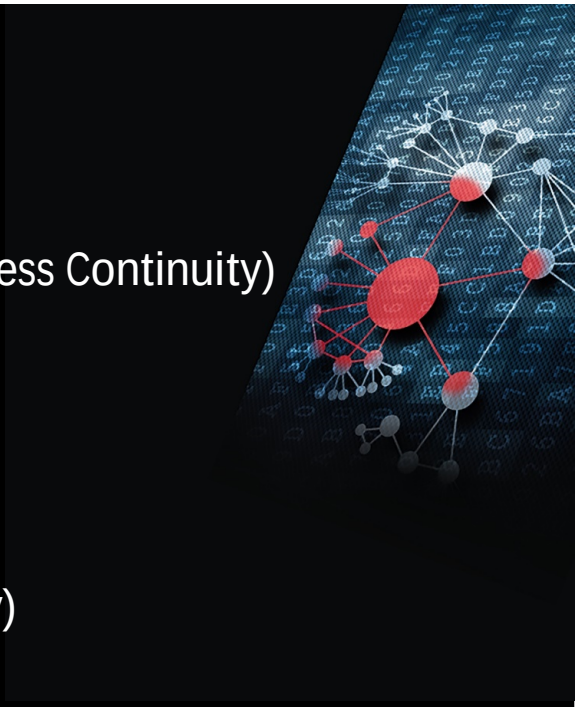
1. Access Control
2. Telecommunications and Network Security
3. Information Security Governance and Risk Mgmt.
4. Software Development Security
5. Cryptography
6. Security Architecture and Design
7. Operations Security
8. Business Continuity and Disaster Recovery Planning
9. Legal, Regulations, Investigations, and Compliance
10. Physical (Environmental) Security

CISSP 8 Domains:

(Effective April 15, 2015)

1. Security and Risk Management
2. Asset Security
3. Security Engineering
4. Communications and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

CISSP 8 Domains: *(Effective April 15, 2015)*



1. Security and Risk Management (Security, Risk, Compliance, Law, Regulations, Business Continuity)
2. Asset Security (Protecting Security of Assets)
3. Security Engineering (Engineering and Management of Security)
4. Communications and Network Security (Designing and Protecting Network Security)
5. Identity and Access Management (Controlling Access and Managing Identity)
6. Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
7. Security Operations (Foundational Concepts, Investigations, Incident Management, Disaster Recovery)
8. Software Development Security (Understanding, Applying, and Enforcing Software Security)

1. Security and Risk Management

The Security and Risk Management domain provides you with the framework and policies, concepts, principles, structures, and standards used to establish criteria for the protection of information assets and to assess the effectiveness of that protection. It includes issues of governance, organizational behaviour, and security awareness.

1. Security and Risk Management

- Understand and apply concepts of confidentiality, integrity and availability
- Apply security governance principles
- Compliance
- Understand legal and regulatory issues that pertain to information security in a global context
- Understand professional ethics
- Develop and implement documented security policy, standards, procedures, and guidelines

1. Security and Risk Management

- Understand business continuity requirements
- Contribute to personnel security policies
- Understand and apply risk management concepts
- Understand and apply threat modelling
- Integrate security risk considerations into acquisition strategy and practice
- Establish and manage information security education, training, and awareness

2. Asset Security

The Asset Security domain provides you with the concepts, principles, structures, and standards used to monitor and secure assets and those controls used to enforce various levels of confidentiality, integrity, and availability.

2. Asset Security

- Classify information and supporting assets
- Determine and maintain ownership
- Protect privacy
- Ensure appropriate retention
- Determine data security controls
- Establish handling requirements

3. Security Engineering

The Security Engineering domain provides you with 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.

3. Security Engineering

- Implement and manage engineering processes using secure design principles
- Understand the fundamental concepts of security models
- Select controls and countermeasures based upon systems security evaluation models
- Understand security capabilities of information systems
- Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

3. Security Engineering

- Assess and mitigate the vulnerabilities in web-based systems
- Assess and mitigate vulnerabilities in mobile systems
- Assess and mitigate vulnerabilities in embedded devices and cyber-physical systems
- Apply cryptography
- Apply secure principles to site and facility design
- Design and implement physical security

4. Communication & Network Security

The Communications and Network Security domain provides you with an understanding of network security related to structures, methods, formats, and measures for the transmission of information.

4. Communication & Network Security

- Apply secure design principles to network architecture
- Secure network components
- Design and establish secure communication channels
- Prevent or mitigate network attacks

5. Identity & Access Management

The Identity and Access Management domain provides the basis for the understanding how access management works, why it is a key security discipline, and how each individual component to be discussed in this chapter relates to the overall access management universe. The most fundamental and significant concept to master is a precise definition of the term “access control”.

5. Identity & Access Management

- Control physical and logical access to assets
- Manage identification and authentication of people and devices
- Integrate identity as a service
- Integrate third-party identity services
- Implement and manage authorization mechanisms
- Prevent or mitigate access control attacks
- Manage the identity and access provisioning lifecycle

6. Security Assessment & Testing

The Security Assessment and Testing domain provides you with the knowledge to assist in managing the risks involved in developing, producing, operating, and sustaining systems and capabilities.

6. Security Assessment & Testing

- Design and validate assessment and test strategies
- Conduct security control testing
- Collect security process data
- Analyse and report test outputs
- Understand the vulnerabilities of security architectures

7. Security Operations

The Security Operations domain covers operations security and security operations. Operations security is primarily concerned with the protection and control of information processing assets in centralized and distributed environments. Security operations is primarily concerned with the daily tasks required to keep security services operating reliably and efficiently.

7. Security Operations

- Understand and support investigations
- Understand requirements for investigation types
- Conduct logging and monitoring activities
- Secure the provisioning of resources
- Understand and apply foundational security operations concepts
- Employ resource protection techniques
- Conduct incident management
- Operate and maintain preventative measures

7. Security Operations

- Implement and support patch and vulnerability management
- Participate in and understand change management processes
- Implement recovery strategies
- Implement disaster recovery processes
- Test disaster recover plans
- Participate in business continuity planning and exercises
- Implement and manage physical security
- Participate in addressing personnel safety concerns

8. Software Security Development

The Software Security Development domain provides you with the abilities required to ensure that the focus of the enterprise security architecture includes application development, since many information security incidents involve software vulnerabilities in one form or another.

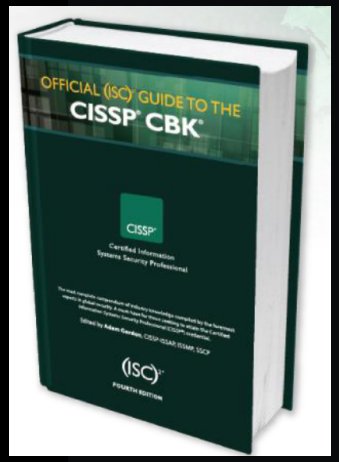
8. Software Security Development

- Understand and apply security in the software development lifecycle
- Enforce security controls in development environments
- Assess the effectiveness of software security
- Assess security impact of acquired software

Exam Outline

- Provides a comprehensive overview of the domains and key areas of knowledge
- Examination qualification requirements
- Includes a suggested reference list
- Download >> www.isc2.org/exam-outline

Official Text Book



- Aligns with the refreshed 8 domains
- Real work examples
- Glossary with over 400 terms
- End of domain review questions
- Only textbook endorsed by (ISC)²
- Available in hard cover, iTunes, and Kindle

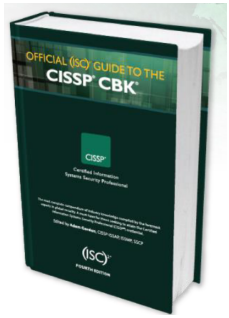
Official Text Book Provided to QA CISSP Course Students*

>> www.isc2.org/official-isc2-textbooks

*During 8 Domain Course Refresh Period

transforming performance
through learning

CISSP
Domain Changes



qa.com/cybersecurity

Effective Date of Change: April 15th 2015