HCISPP®

HealthCare Information Security and Privacy Practitioner

Certification **Exam Outline**

Effective Date: November 2013

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD.

About HCISPP

The HealthCare Information Security and Privacy Practitioner (HCISPP) is the ideal certification for those with the core knowledge and experience needed to implement, manage, or assess the appropriate security and privacy controls of a healthcare organization. HCISPP provides confirmation of a practitioner's knowledge of best practices and techniques to protect organizations and sensitive data against emerging threats and breaches.

The broad spectrum of topics included in the HCISPP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of information security. Successful candidates are competent in the following six domains:

- Healthcare Industry
- Regulatory Environment
- Privacy and Security in Healthcare
- Information Governance and Risk Management
- Information Risk Assessment
- Third Party Risk Management

Experience Requirements

Candidates must have a minimum of 2 years cumulative paid full-time work experience in 1 or more knowledge areas of the HCISPP CBK that includes security, compliance, and privacy. Legal experience may be substituted for compliance and information management experience may be substituted for privacy. Of the 2 years of experience, 1 of those years must be in the healthcare industry.

A candidate that doesn't have the required experience to become a HCISPP may become an Associate of (ISC)² by successfully passing the HCISPP examination. The Associate of (ISC)² will then have 3 years to earn the 2 years required experience.

Accreditation

HCISPP is in compliance with the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

(ISC)² has an obligation to its membership to maintain the relevancy of the HCISPP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the HCISPP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing healthcare information security and privacy practitioners.

HCISPP Examination Information

Length of exam	3 hours
Number of questions	125
Question format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

HCISPP Examination Weights

Domains	Weight
1. Healthcare Industry	10%
2. Regulatory Environment	16%
3. Privacy and Security in Healthcare	26%
4. Information Governance and Risk Management	17%
5. Information Risk Assessment	16%
6. Third Party Risk Management	15%
Total:	**100%**

Domain 1: Healthcare Industry

1.1 Understand the Healthcare Environment

- Types of Organizations in the Healthcare Sector (e.g., providers, pharma, payers, business associates)
- Health Information Technology (e.g., computers, medical devices, networks, health information exchanges, Electronic Health Record [EHR], Personal Health Record [PHR])
- Health Insurance (e.g., claims processing, payment models)
- Coding (e.g., SNOMED CT, ICD-9/10)
- Billing, Payment, and Reimbursement
- Workflow Management
- Regulatory Environment (e.g., security, privacy, oversight)
- Public Health Reporting
- Clinical Research (e.g., processes)
- Healthcare Records Management

1.2 Understand Third-Party Relationships

- Vendors
- Business Partners
- Data Sharing
- Regulators

1.3 Understand Foundational Health Data Management Concepts

- Information Flow and Life Cycle in the Healthcare Environments
- Health Data Characterization (e.g., classification, taxonomy, analytics)
- Data Interoperability and Exchange (e.g., HL7, HIE, DICOM)
- Legal Medical Records

Domain 2: Regulatory Environment

2.1 Identify Applicable Regulations

- Legal Issues that Pertain to Information Security and Privacy for Healthcare Organizations
- Data Breach Regulations
- Personally Identifiable Information
- Information Flow Mapping
- Jurisdiction Implications
- Data Subjects
- Data Owners/Controllers/Custodians/Processors

2.2 Understand International Regulations and Controls

- Treaties (e.g., Safe Harbor)
- Regulations
- Industry Specific Laws
- Legislative (e.g., EU Data Privacy Directive, HIPAA/HITECH)

2.3 Compare Internal Practices Against New Policies and Procedures

- Policies (information security and privacy)
- Standards (information security and privacy)
- Procedures (information security and privacy)

2.4 Understand Compliance Frameworks (e.g., ISO, NIST, Common Criteria, IG Toolkit, Generally Accepted Privacy Principles [GAPP])

2.5 Understand Responses for Risk-Based Decision

- Compensating Controls
- Control Variance Documentation
- Residual Risk Tolerance

2.6 Understand and Comply with Code of Conduct/Ethics in a Healthcare Information Environment

- Organizational Code of Ethics
- (ISC)² Code of Ethics

Domain 3:
Privacy and Security in Healthcare

3.1 Understand Security Objectives/Attributes

- Confidentiality
- Integrity
- Availability

3.2 Understand General Security Definitions/Concepts

- Access Control
- Data Encryption
- Training and Awareness
- Logging and Monitoring
- Vulnerability Management
- Systems Recovery
- Segregation of Duties
- Least Privilege (Need to Know)
- Business Continuity
- Data Retention and Destruction

3.3 Understand General Privacy Principles (e.g., OECD Privacy Principles, GAPP, PIPEDA, UK Data Protection Act 1998)

- Consent/Choice
- Limited Collection/Legitimate Purpose/Purpose Specification
- Disclosure Limitation/Transfer to Third Parties/ Trans-Border Concerns
- Access Limitation
- Security
- Accuracy, Completeness, Quality
- Management, Designation of Privacy Officer, Supervisor Re-authority, Processing Authorization, Accountability
- Transparency, Openness
- Proportionality, Use and Retention, Use Limitation
- Access, Individual Participation
- Notice, Purpose Specification
- Additional Measures for Breach Notification

3.4 Understand the Relationship Between Privacy and Security

- Dependency
- Integration

3.5 Understand the Disparate Nature of Sensitive Data and Handling Implications

- Personal and Health Information protected by Law
- Sensitivity mitigation (e.g., de-identification, anonymization)
- Categories of sensitive data (e.g., mental health)

3.6 Understand Security and Privacy Terminology Specific to Healthcare

Domain 4:
Information Governance and Risk Management

4.1 Understand Security and Privacy Governance

- Information governance
- Governance structures

4.2 Understand Basic Risk Management Methodology

- Approach (e.g., qualitative, quantitative)
- Information Asset Identification
- Asset Valuation
- Exposure
- Likelihood
- Impact
- Threats
- Vulnerability
- Risk
- Controls
- Residual Risk
- Acceptance

4.3 Understand Information Risk Management Life Cycles (e.g., NIST, CMS, ISO)

4.4 Participate in Risk Management Activities

- Remediation Action Plans
- Risk Treatment (e.g., mitigation/remediation, transfer, acceptance, avoidance)
- Communications
- Exception Handling
- Reporting and Metrics

Domain 5:
Information Risk Assessment

5.1 Understand Risk Assessment

- Definition
- Intent
- Lifecycle/Continuous Monitoring
- Tools/Resources/Techniques
- Desired Outcomes
- Role of Internal and External Audit/Assessment

5.2 Identify Control Assessment Procedures From Within Organization Risk Frameworks

5.3 Participate in Risk Assessment Consistent With Role in Organization

- Information Gathering
- Risk Assessment Estimated Timeline
- Gap Analysis
- Corrective Action Plan
- Mitigation Actions

5.4 Participate in Efforts to Remediate Gaps

- Types of Controls
- Controls Related to Time

Domain 6:
Third Party Risk Assessment

6.1 Understand the Definition of Third Parties in Healthcare Context

6.2 Maintain a List of Third-Party Organizations

- Health Information Use (e.g., processing, storage, transmission)
- Third-Party Role/Relationship with the Organization

6.3 Apply Third-Party Management Standards and Practices for Engaging Third Parties Based Upon the Relationship with the Organization

- Relationship Management
- Comprehend Compliance Requirements

6.4 Determine When Third-Party Assessment Is Required

- Organizational Standards
- Triggers of Third-Party Assessment

6.5 Support Third-Party Assessments and Audits

- Information Asset Protection Controls
- Compliance with Information Asset Protection Controls
- Communication of Findings

6.6 Respond to Notifications of Security/Privacy Events

- Internal Processes for Incident Response
- Relationship between Organization and Third-Party Incident Response
- Breach Recognition, Notification, and Initial Response

6.7 Support Establishment of Third-Party Connectivity

- Trust Models for Third-Party Interconnections
- Technical Standards (e.g., physical, logical, network connectivity)
- Connection Agreements

6.8 Promote Awareness of the Third-Party Requirements (internally and externally)

- Information Flow Mapping and Scope
- Data Sensitivity and Classification
- Privacy Requirements
- Security Requirements
- Risks Associated with Third Parties

6.9 Participate in Remediation Efforts

- Risk Management Activities
- Risk Treatment Identification
- Corrective Action Plans
- Compliance Activities Documentation

6.10 Respond to Third-Party Requests Regarding Privacy/Security Events

- Organizational Breach Notification Rules
- Organizational Information Dissemination Policies and Standards
- Risk Assessment Activities
- Chain of Custody Principles

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/hcispp-cbk-references.

Examination Policies and Procedures

(ISC)² recommends that HCISPP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/exam-policies-procedures.

Legal Info

For any questions related to (ISC)²'s legal policies, please contact the (ISC)² Legal Department at legal@isc2.org.

Any Questions?

(ISC)² Candidate Services
311 Park Place Blvd, Suite 400
Clearwater, FL 33759

(ISC)² Americas
Tel: +1.727.785.0189
Email: info@isc2.org

(ISC)² Asia Pacific
Tel: +(852) 28506951
Email: isc2asia@isc2.org

(ISC)² EMEA
Tel: +44 (0)203 300 1625
Email: info-emea@isc2.org