HCISPP®

HealthCare Information Security and Privacy Practitioner

ISC2 Certification

Certification **Exam Outline**

Effective Date: September 1, 2022

ISC2™

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 seven domains:

- Healthcare Industry
- Data and Information Governance in Healthcare
- Information Technologies in Healthcare
- Regulatory and Standards Environment
- Privacy and Security in Healthcare
- Risk Management and Risk Assessment
- Third-Party and Supply Chain Risk Management

Experience Requirements

Candidates must have a minimum of two years cumulative paid work experience in one or more knowledge areas of the HCISPP Common Body of Knowledge (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 two years of experience, one 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 ISC2 will then have three years to earn the two years of required experience. You can learn more about HCISPP experience requirements and how to account for part-time work and internships at www.isc2.org/Certifications/HCISPP/experience-requirements.

Accreditation

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

Job Task Analysis (JTA)

ISC2 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 items	125
Item 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	12%
2. Data and Information Governance in Healthcare	5%
3. Information Technologies in Healthcare	14%
4. Regulatory and Standards Environment	15%
5. Privacy and Security in Healthcare	24%
6. Risk Management and Risk Assessment	17%
7. Third-Party and Supply Chain Risk Management	13%
Total:	**100%**

Domain 1: Healthcare Industry

1.1 Understand the healthcare environment components

- Types of organizations in the healthcare sector (e.g., providers, pharma, payers)
- Health insurance (e.g., claims processing, payment models, health exchanges, clearing houses)
- Coding (e.g., Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT), International Classification of Diseases (ICD) 10)
- Revenue cycle (i.e., billing, payment, reimbursement)
- Workflow management
- Regulatory environment
- Public health reporting
- Clinical research (e.g., processes)
- Healthcare records management
- Remote workforce (i.e., telecommuting)

1.2 Understand third-party and supply chain relationships

- Vendors
- Business partners
- Regulators
- Data analytics
- Managed service providers
- Cloud service providers
- Other third-party relationships
- Supply chain vendors (e.g., software, open source analysis)

1.3 Understand foundational health data management

- Information flow and ecosystem lifecycle in the healthcare environments
- Health data characterization (e.g., classification, taxonomy, analytics, protected health information (PHI) vs. personally identifiable information (PII))
- Data interoperability and exchange (e.g., Health Level 7 (HL7), International Health Exchange (IHE), Digital Imaging and Communications in Medicine (DICOM))
- Legal medical records

Domain 2:
Data and Information Governance in Healthcare

2.1 Understand and identify data and information governance frameworks

- Security governance
- Privacy governance

2.2 Identify data governance charters, roles and responsibilities

2.3 Align data and information security and privacy standards policies and procedures

- Standards
- Policies
- Procedures and processes

2.4 Understand and integrate the code of ethics in a healthcare data environment

- Organizational code of ethics
- (ISC)^{2} code of ethics

Domain 3: Information Technologies in Healthcare

3.1 Understand the impact of healthcare information technologies on privacy and security

- Increased exposure affecting confidentiality, integrity, availability and privacy (e.g., threat landscape)
- Oversight and regulatory challenges in a changing technological environment
- Requirements for data interoperability
- Information technologies

3.2 Understand data life cycle management

- Creation and classification of healthcare data
- Storage
- Data sharing/transfer
- Data use monitoring and access control
- Archiving and record retention
- Destruction

3.3 Understand third-party connectivity

- Trust models for third-party interconnections
- Technical standards (e.g., physical, logical, network connectivity)
- Connection agreements (e.g., memorandum of understanding (MOU), Interconnection Security Agreements (ISAs))

Domain 4:
Regulatory and Standards Environment

4.1 Identify regulatory requirements

- Legal issues that pertain to data security and privacy for healthcare organizations
- Data breach regulations and guidance
- Protected personal and health information (e.g., personally identifiable information (PII), personal health information (PHI))
- Jurisdiction implications
- Data subjects
- Clinical research

4.2 Recognize regulations and controls of various countries

- Treaties
- Laws and regulations (e.g., General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH), Personal Information Protection and Electronic Documents Act (PIPEDA))

4.3 Understand compliance frameworks

- Privacy frameworks (e.g., Organization for Economic Co-operation and Development (OECD) Privacy principles, Asia-Pacific Economic Cooperation (APEC), Generally Accepted Privacy Principles (GAPP))
- Security frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Common Criteria)

Domain 5:
Privacy and Security in Healthcare

5.1 Understand security objectives/attributes

- Confidentiality
- Integrity
- Availability
- Privacy

5.2 Understand general security definitions and concepts

- Authorization and authentication
- Identity and access management (IAM)
- Cryptography and data encryption
- Security training and awareness
- Logging, monitoring and auditing
- Vulnerability management
- Segregation of duties
- Incident response
- Business continuity (BC) and disaster recovery (DR)
- Data backup and recovery including testing and validation
- Endpoint management (e.g. Mobile Device Management (MDM))
- Data classification controls (e.g., data loss prevention (DLP))
- Cloud provided services
- Designated security officer (e.g., facility security officer, information security officer)

5.3 Understand general privacy definitions and concepts

- Consent, restrictions, access and accountability
- Limited collection, legitimate purpose and purpose specification
- Appropriate use and disclosure limitations, third-party data exchange and trans-border concerns
- Access limitation
- Data integrity (e.g., accuracy, completeness and quality)
- Management, designation of privacy officer, supervisor re-authority, processing authorization and accountability
- Privacy training and awareness
- Transparency and openness (e.g., notice of privacy practices, privacy policy)
- Reporting (e.g., events, incidents and breaches)

5.4 Understand the relationship between privacy and security

- Dependency (i.e., security impacts to privacy)
- Integration (e.g., introduction of new technology/updates)

5.5 Understand sensitive data and handling

- Sensitivity mitigation (e.g., de-identification, anonymization)
- Categories of sensitive data (e.g., behavioral health)

Domain 6:
Risk Management and Risk Assessment

6.1 Understand enterprise risk management

- Risk management overview
- Information asset identification
- Asset valuation
- Exposure
- Likelihood
- Impact
- Threats
- Vulnerability
- Risk
- Controls (e.g., administrative, technical, physical)
- Residual Risk
- Acceptance

6.2 Understand risk frameworks

- International Organization for Standardization (ISO)
- National Institute of Standards and Technology (NIST)
- Health Information Trust Alliance (HITRUST)

6.3 Understand Risk Management Process

- Definition
- Data classification (e.g., personally identifiable information (PII), protected health information (PHI), electronic protected health information (ePHI))
- Approach (e.g., qualitative, quantitative)
- Intent
- Life cycle and continuous monitoring
- Tools, resources and techniques
- Desired outcomes
- Role of internal and external audit/assessment (e.g., privacy and information security risk assessments)

6.4 Identify control assessment procedures utilizing organization risk frameworks

6.5 Participate in risk assessment consistent with roles within the organizational environment

- Information gathering
- Risk assessment process
- Gap analysis

6.6 Understand risk response (e.g., corrective action plan)

- Mitigation
- Avoidance
- Transfer
- Acceptance
- Compensating controls
- Communications and reporting

6.6 Utilize controls to remediate risk (e.g., preventative, detective, corrective)

- Administrative
- Physical
- Technical

6.8 Participate in continuous improvement and monitoring

Domain 7:
Third-Party and Supply Chain Risk Management

7.1 Understand the definition of third-party in healthcare context

7.2 Maintain a list of third-party organizations

» Third-party relationship with the organization
» Health information use (e.g., processing, storage, transmission)

7.3 Apply management standards and practices for engaging third-parties

» Relationship management

7.4 Determine when a third-party assessment Is required

» Organizational standards
» Triggers of a third-party assessment

7.5 Support third-party assessments and audits

» Information asset protection controls
» Compliance with information asset protection controls
» Communication of results and recommended actions

7.6 Participate in third-party remediation efforts

» Risk assessment activities
» Impact assessment and risk tolerance
» Corrective action plans
» Compliance validation

7.7 Respond to notifications of security/privacy events

» Documenting and testing internal processes for incident response
» Relationship between organization and third-party Incident response
» Breach recognition, notification and initial response

7.8 Respond to third-party requests regarding privacy/security events

- Legal or contractual breach notification requirements
- Organizational information dissemination policies and standards
- Risk assessment activities
- Chain of custody principles

7.9 Promote awareness of third-party requirements

- Information flow mapping and scope
- Data sensitivity and classification
- Privacy and security requirements
- Risks associated with third-parties

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/certifications/References.

Examination Policies and Procedures

ISC2 recommends that CISSP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

Legal Info

For any questions related to ISC2's legal policies, please contact the ISC2 Legal Department at legal@isc2.org.

Any Questions?

Contact ISC2 Candidate Services in your region:

Americas

Tel: +1-866-331-ISC2 (4722)
Email: info@isc2.org

Asia-Pacific

Tel: +(852) 5803-5662
Email: isc2asia@isc2.org

Europe, Middle East and Africa

Tel: +44 (0)203-960-7800
Email: info-emea@isc2.org