HCISPP Domain Refresh

On September 1, 2019, the domains for the (ISC)² HealthCare Information Security and Privacy Practitioner (HCISPP®) credential exam were refreshed and the current HCISPP Exam Outline is available on our website.

The content of the HCISPP has been refreshed to reflect the most pertinent issues that healthcare security professionals currently face, along with the best practices for mitigating those issues. Some topics have been updated while others have been realigned. The result is an exam that most accurately reflects the deep knowledge and hands-on experience with the healthcare industry, governance, regulation and standards.

As a result of the content refresh, the domain and subdomain names have been updated to describe the topics accurately. The weights for the domains have also changed. Please see the comparison table below.

<table>
<thead>
<tr>
<th>Prior to September 1, 2019</th>
<th>Effective September 1, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain 1: Healthcare Industry</strong></td>
<td><strong>Domain 1: Healthcare Industry</strong></td>
</tr>
<tr>
<td>- Understand the healthcare environment</td>
<td>- Understand the healthcare environment components</td>
</tr>
<tr>
<td>- Understand third-party relationships</td>
<td>- Understand third-party relationships</td>
</tr>
<tr>
<td>- Understand foundational health data management concepts</td>
<td>- Understand foundational health data management concepts</td>
</tr>
<tr>
<td>Exam Weight: 10%</td>
<td>Exam Weight: 12%</td>
</tr>
<tr>
<td><strong>Domain 2: Regulatory Environment</strong></td>
<td><strong>Domain 2: Information Governance in Healthcare</strong></td>
</tr>
<tr>
<td>- Identify applicable regulations</td>
<td>- Understand information governance frameworks</td>
</tr>
</tbody>
</table>

*domain name change*
- Understand international regulations and controls
- Compare internal practices against new policies and procedures
- Understand compliance frameworks
- Understand responses for risk-based decisions
- Understand and comply with code of conduct/ethics in a healthcare information environment
- Identify governance roles and responsibilities
- Align information security and privacy policies, standards and procedures
- Understand and comply with code of conduct/ethics in a healthcare information environment

Domain 3: Privacy and Security in Healthcare
- Understand security objectives/attributes
- Understand general security definitions/concepts
- Understand general privacy principles
- Understand the relationship between privacy and security
- Understand the disparate nature of sensitive data and handling implications
- Understand security and privacy terminology specific to healthcare

Domain 3: Information Technologies in Healthcare
- Understand the impact of healthcare information technologies on privacy and security
- Understand data lifecycle management
- Understand third-party connectivity

Domain 4: Information Governance and Risk Management
- Understand security and privacy governance
- Understand basic risk management methodology
- Understand information risk management lifecycles

Domain 4: Regulatory and Standards Environment
- Identify regulatory requirements
- Recognize regulations and controls of various countries
- Understand compliance frameworks
• Participate in risk management activities

Exam Weight: 17%  
Exam Weight: 15%

**Domain 5: Information Risk Assessment**

- Understand risk assessment
- Identify control assessment procedures from within organization risk frameworks
- Participate in risk assessment consistent with role and organization
- Participate in efforts to remediate gaps

**Domain 5: Privacy and Security in Healthcare**

- Understand security objectives/attributes
- Understand general security definitions and concepts
- Understand general privacy definitions and concepts
- Understand the relationship between privacy and security
- Understand sensitive data and handling

Exam Weight: 16%  
Exam Weight: 25%

**Domain 6: Third-Party Risk Assessment**

- Understand the definition of third parties in healthcare context
- Maintain a list of third-party organizations
- Apply third-party management standards and practices for engaging third parties based upon the relationship with the organization
- Determine when third-party assessment is required
- Support third-party assessments and audits
- Respond to notifications of security/privacy events
- Support establishment of third-party connectivity

**Domain 6: Risk Management and Risk Assessment**

- Understand enterprise risk management
- Understand information risk management framework (RMF)
- Understand risk management process
- Identify control assessment procedures utilizing organization risk frameworks
- Participate in risk assessment consistent with the role in organization
- Understand risk response
- Utilize controls to remediate risk
- Participate in continuous monitoring
• Promote awareness of the third-party requirements
• Participate in remediation efforts
• Respond to third-party requests regarding privacy/security events

---

Exam Weight: 15%

Domain 7: Third-Party Risk Management

• Understand the definition of third-parties in healthcare context
• Maintain a list of third-party organizations
• Apply management standards and practices for engaging third-parties
• Determine when a third-party assessment is required
• Support third-party assessments and audits
• Participate in third-party remediation efforts
• Respond to notifications of security/privacy events
• Respond to third-party requests regarding privacy/security events
• Promote awareness of third-party requirements

Exam Weight: 20%

Exam Weight: 15%