Certified Healthcare IS Security Practitioner Certification Course (C)HISSP)

Modality: Virtual Classroom

Duration: 4 Days

About this course:

This certification course of Certified Healthcare Information Systems Security Practitioner is a training course of vendor-neutral IT operations and covers all the important regions of abilities and coursework needed to authorize the best expectations of Healthcare Practices of IT in consistence with the benchmarks in the medicinal services industry. CCHISSPs are basic in the protection and management of healthcare information and are allocated to safeguard patients' data through the management, execution, and evaluation of right IT controls for the honesty of patients' wellbeing data. Through Mile2's Assessment and Certification System (MACS), the exam of Certified Healthcare Information Systems Security Practitioner is given online.

The compensation for a Healthcare Information Systems Security Practitioner midpoints around $27,510 per annum.

Course Objectives:

- An introduction to the industry of healthcare
- Third-Party Risk Management
- Information Governance and Risk Assessment.
- Regulatory Frameworks and Environment.
- Healthcare Privacy and Security Policies.
- Information Risk Assessment
- International Controls and Regulations
- Code of Conduct/Ethics
- Compliance Frameworks
- Internal Practices Compared to New Procedures and Policies
- Risk-Based Decisions
- Risk Management Methodology
- Security and Privacy Governance
- Risk Management Activities
- Assessment of Risk Consistent with Role in Organization
- Information Risk Management Life Cycles
- Processes from within the Risk Frameworks of the Organization
- Efforts to Remediate Gaps
- Third-Party Requirements Remediation Efforts
- Explanation of Third-Parties in the Context of Healthcare
- Third-Party Management Practices and Standards
- Third-Party Connectivity
- Third-Party Audits and Assessments
- Security/Privacy Events

Audience:

This course is planned for:

- Risk Managers
- Information System Security Officers
- Information Security Managers
- Compliance & Privacy Officers
- Privacy Officers
- Information Systems Owners

Prerequisites:

Before the student attempts this course, it expected for them to have at least a year's involvement with Healthcare Information Systems

Suggested prerequisites courses:

Certified Healthcare Information Systems Security Practitioner

Course Outline:

Module 1: Intro to the Healthcare Industry

- Healthcare Environment
- Third-Party Relationships
- Health Data Management Concepts

Module 2: Regulatory Environment

- Applicable Regulations
- International Regulations and Controls
- Internal Practices Compared to New Policies and Procedures
- Compliance Frameworks
- Risk-Based Decisions
- Code of Conduct/Ethics

Module 3: Healthcare Privacy & Security Policies

- Security Objectives/Attributes
- Security Definitions/Concepts
- Privacy Principles
- Disparate Nature of Sensitive Data and Handling Implications

Module 4: Information Governance & Risk Management

- How organizations manage information risk through security and privacy governance, risk

management lifecycles, and principle risk activities
- Security and Privacy Governance
- Risk Management Methodology
- Information Risk Management Life Cycles
- Risk Management Activities

Module 5: Information Governance & Risk Assessment

- Risk Assessment
- Procedures from within Organization Risk Frameworks
- Risk Assessment Consistent with Role in Organization
- Efforts to Remediate Gaps

Module 6: Third-Party Risk Management

- Definition of Third-Parties in Healthcare Context
- Third-Party Management Standards and Practices
- Third-Party Assessments and Audits
- Security/Privacy Events
- Third-Party Connectivity
- Third-Party Requirements Remediation Efforts