Harness the Power of Partnership to Grow Your Business

In today’s ever-changing security landscape, there is immense pressure to stay ahead of attacks and keep knowledge and skills sharp. Certified cybersecurity professionals are scarce, compounding the challenges business, government and academia face to protect critical infrastructure and assets.

(ISC)² research shows an estimated 1.8 million cybersecurity jobs will go unfilled by 2022. But by working together as partners, we can help certify, train and develop security professionals to reverse this trend.

Align Forces with the Industry Authority

As the largest not-for-profit leader in educating and certifying cyber, information, software and infrastructure security professionals, (ISC)² is globally recognized for premier certifications and education programs. Partnering with us as an (ISC)² Training – Official Provider allows you to gain more credibility and recognition for your training programs while increasing opportunities for growth as a recognized authority in cybersecurity training.

Becoming an Official Provider demonstrates your commitment to providing the highest standards of training and meeting the knowledge and skills gap head-on.

As an Official Provider, your organization will also save time and resources developing education materials, guaranteeing your training stays current with (ISC)²’s Official Common Body of Knowledge (CBK) for all certifications. This means you have exclusive access to the official training material – directly from the creators and keepers of the CBK.
Why Become an (ISC)² Training – Official Provider?

» Offer customers access to the highest quality, most up-to-date training content to maximize their learning experiences.

» Assist security professionals and practitioners in obtaining industry-leading information security certifications.

» Save time and resources developing education materials, guaranteeing your training stays current with (ISC)²’s CBK for all certifications.

» Gain access to (ISC)²-authorized instructors, vetted by the leading information security credentialing authority.

» Differentiate yourself with (ISC)²’s globally recognized and respected brand.

» Join a global network of authorized organizations committed to delivering the highest standard in cybersecurity training in the United States, Europe, the Middle East and Asia-Pacific.

» Align your business with an elite network of more than 138,000 certified cybersecurity professionals in more than 160 countries.
Reasons to Partner with (ISC)²

(ISC)² Training – Official Providers benefit from business, technical and marketing support to drive new programs and revenue streams across the entire (ISC)² training and certification portfolio.

Go-to-Market Support
» Dedicated support through pre- and post-sales resources, preferential pricing, marketing tools and branding
» Completely up-to-date courseware for all (ISC)² certifications, helping to reduce your development costs
» Sales incentives like SPIFs to engage and motivate your team members

Certification & Training
» Ongoing education and training for your sales teams
» Dedicated partner portal with access to relevant resources and materials for your sales, marketing and partnership information
» Complete (ISC)² suite of courses to enhance the value of your existing portfolio
» (ISC)²-authorized instructors for training sessions. (ISC)² will provide an instructor, or bring your own and we will certify them.
» Certification exam vouchers to provide additional value to exam takers, available only to Official Providers

Sales & Marketing Enablement
» New revenue streams and differentiated offerings with the (ISC)² training and certification portfolio
» Lead generation through (ISC)²’s Training Finder, giving partners the ability to upload and manage their public schedules to create awareness and drive interest
» Participation in joint marketing activities and special promotions
» Sponsorship discount opportunities for (ISC)² events

“As an (ISC)² Training Preferred Official Provider and CPESubmitter, we have been able to improve security efforts for organizations around the world. In partnership with (ISC)², Learning Tree has expanded and broadened our cybersecurity offerings to include not only the popular CISSP, but all other certification courses across many disciplines in the cybersecurity space.”

— Jacqueline Visnius
Director, Product Management
Learning Tree International
Partner Participation Levels

The program includes two levels of entry to suit your commitment and business requirements. Each level includes exclusive benefits to help maximize your revenue growth potential.

Join as an Official Partner and uncover additional opportunities within the Preferred level as your business grows.

(ISC)² Training – Official Providers
Use official courseware developed by (ISC)². This ensures your training content is always relevant and up-to-date. All instructors are verified security experts who have undergone an intense training and authorization process to teach our content.

(ISC)² Training – Preferred Official Providers
Receive advanced support and resources based on an enhanced level of participation.

Contact an (ISC)² Account Executive to find out more about the Preferred Official Provider participation level.

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Authorized</th>
<th>Preferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam Discounts</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Student Kit Discounts</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sales Incentives</td>
<td>Basic</td>
<td>Advanced</td>
</tr>
<tr>
<td>Access to Sales and Marketing Portal</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Listing on (ISC)² Website and Training Finder</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Demand Generation</td>
<td>Basic</td>
<td>Advanced</td>
</tr>
<tr>
<td>Marketing Resources</td>
<td>Basic</td>
<td>Advanced</td>
</tr>
<tr>
<td>(ISC)² SME Assistance</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>(ISC)² Channel Manager Client Assistance</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access to Official (ISC)² Courseware</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Instructor Development</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>CPE Skill Builder</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Member Benefits</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Partner Conferences</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Product Briefings</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Sponsorship Discounts</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Official Provider Requirements

1. Must commit to supporting (ISC)²’s vision and mission:
   **Our Vision** – Inspire a safe and secure cyber world
   **Our Mission** – Support and provide members and constituents with credentials, resources and leadership to address cyber, information, software and infrastructure security to deliver value to society.

2. Pay a one-time fee that may be used toward the purchase of student kits.

3. Meet a minimum annual revenue requirement, determined in collaboration with your sales team.

4. Complete the instructor authorization program that includes access to (ISC)²’s learning management system for courses, resources and up-to-date information.

5. Create a business plan with supporting goals for growth and success. Use our business-planning template to make planning, documentation and implementation seamless!
Flexible Solutions for Cybersecurity Certification and Training

Every organization has unique certification and training needs, and cookie-cutter solutions fall short of meeting them. That’s why (ISC)²’s offerings can be tailored to your budget, schedule and cybersecurity requirements. Count on our team of account executives to recommend solutions that validate expertise, keep cybersecurity skills sharp and prove credibility to partners and clients.

(ISC)² Certifications
You may know (ISC)² for our acclaimed CISSP certification, but that’s just the beginning. We offer everything you need for enterprise cybersecurity certification and training. Organizations all over the world rely on us to certify, train and educate a diverse and changing workforce. Explore the (ISC)² certifications that support your company goals.
Industry-Leading Cybersecurity Certifications for All Levels of Your Organization

Risk management demands a company culture fully entrenched in security. Anyone who touches administrative functions in your systems or sensitive data must validate their cybersecurity expertise. Leverage our portfolio of industry-leading cybersecurity certifications to cover a wide range of experience and skill levels. Consider these advantages.

Required or Preferred by the Most Security-Conscious Organizations
(ISC)² certifications are listed on most job boards for security positions. Seven of our certifications are listed on the U.S. DoD 8140.01/8570.01.

ANSI Accreditation
(ISC)² was the first information security certification body to achieve ANSI/ISO/IEC 17024 for the CISSP certification and has received the required annual re-accreditation from ANSI for all (ISC)² certifications.

Validate Knowledge and Experience
Becoming certified entails more than just passing an exam. Candidates must meet an experience requirement and be endorsed by an (ISC)² member, confirming their professional experience.

Cover Current, Global Topics
(ISC)² certifications are industry-focused and industry-driven. To ensure continued relevance, we update each certification every 3 years by conducting a job task analysis (JTA).

Continuing Professional Education
(ISC)²-certified members never stop growing. To maintain certification, they must accrue continuing professional education (CPE) credits annually.

ACE CREDIT
Connects workplace learning with colleges and universities by helping adults gain access to academic credit at colleges and universities for formal courses and examinations taken in the workplace or other settings outside traditional higher education.

The American Council on Education’s College Credit Recommendation Service (ACE CREDIT) has evaluated and recommended 2 college credit hours for completing and Official (ISC)² CBK Training Seminar for the CISSP, CCSP, CSSLP and SSCP.
(ISC)² Certification Road Map
(ISC)² certifications validate skills at every level of an organization.

**Associate of (ISC)² – Pathway to Certification**
Your employees without the required years of work experience to obtain an (ISC)² certification can become an Associate of (ISC)², proving knowledge in cybersecurity.

**CISSP – Leadership and Operations**
Recognizes information security leaders who understand cybersecurity strategy, as well as hands-on implementation. Proves knowledge and experience to design, develop and manage the overall security posture of an organization.

**SSCP – IT Administration**
Recognizes hands-on technical abilities and practical experience. Proves skills to implement, monitor and administer IT infrastructure using IT security policies and procedures — ensuring the confidentiality, integrity and availability of data.

**CCSP – Cloud Security**
Recognizes IT and cybersecurity leaders who have the knowledge and competency to apply best practices to cloud security architecture, design, operations and service orchestration. Designates leaders on the forefront of cloud security.

**CAP – Authorization**
Recognizes knowledge, skills and abilities to authorize and maintain information systems within the risk management framework (RMF). Proves knowledge to formalize processes to assess risk and establish security documentation.

**CSSLP – Software Security**
Recognizes expertise and ability to incorporate security practices — authentication, authorization and auditing — into each phase of the software development lifecycle.

**HCISPP – Healthcare Security and Privacy**
Recognizes knowledge and ability to successfully implement, manage or assess security and privacy controls for healthcare and patient information. Proves a strong foundation in healthcare risk, security and privacy, and understanding of important healthcare regulations.

**CISSP Concentrations – Beyond the CISSP**
(ISC)² concentrations are elite, specialized credentials that build on the CISSP to prove subject matter mastery. They recognize evolving expertise in information security architecture, engineering and management.
Top 5 Benefits for Customer Organizations

1. Protect against threats in an increasingly complex cyber world.

2. Ensure staff stays current on emerging threats, technologies, regulations, standards and practices.

3. Support professional development and employee retention.

4. Ensure employees use a universal language, avoiding ambiguity with industry-accepted terms and practices.

5. Promote a culture of information security innovation with well-trained and well-educated staff to achieve long-term organizational viability and profitability.
CISSP Course Outline

Leadership and Operations

40 CPEs

The Official (ISC)² CISSP training provides a comprehensive review of the knowledge required to effectively design, engineer and manage the overall security posture of an organization. This training course will help students review and refresh their knowledge and identify areas they need to study for the CISSP exam. Taught by an (ISC)²-authorized instructor, the course features:

- Official (ISC)² courseware
- Flash Cards
- Post-course assessment
- Collaboration with classmates (not currently available for self-paced course)
- Real-world learning activities and scenarios

Who Should Attend

The training seminar is ideal for those working in positions such as but not limited to:

- Security Consultant
- Security Manager
- IT Director/Manager
- Security Auditor
- Security Architect
- Security Analyst
- Security Systems Engineer
- Chief Information Security Officer
- Security Director
- Network Architect

Course Agenda

- Domain 1: Security and Risk Management
- Domain 2: Asset Security
- Domain 3: Security Architecture and Engineering
- Domain 4: Communication and Network Security
- Domain 5: Identity and Access Management (IAM)
- Domain 6: Security Assessment and Testing
- Domain 7: Security Operations
- Domain 8: Software Development Security

Course Delivery Methods

- Classroom-Based
- Online Instructor-Led
- Online Self-Paced
- Private On-Site
Course Objectives

After completing this course, participants will be able to:

» Understand and apply fundamental concepts and methods related to the fields of information technology and security.

» Align overall organizational operational goals with security functions and implementations.

» Understand how to protect assets of the organization as they go through their lifecycle.

» Understand 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.

» Implement system security through the application of security design principles and application of appropriate security control mitigations for vulnerabilities present in common information system types and architectures.

» Understand the importance of cryptography and the security services it can provide in today’s digital and information age.

» Understand the impact of physical security elements on information system security and apply secure design principles to evaluate or recommend appropriate physical security protections.

» Understand the elements that comprise communication and network security coupled with a thorough description of how the communication and network systems function.

» List the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1-7.

» Identify standard terms for applying physical and logical access controls to environments related to their security practice.

» Appraise various access control models to meet business security requirements.

» Name primary methods for designing and validating test and audit strategies that support business requirements.

» Enhance and optimize an organization’s operational function and capacity by applying and utilizing appropriate security controls and countermeasures.

» Recognize risks to an organization’s operational endeavors and assess specific threats, vulnerabilities and controls.

» Understand the System Lifecycle (SLC) and the Software Development Lifecycle (SDLC) and how to apply security to it; identify which security control(s) are appropriate for the development environment; and assess the effectiveness of software security.
SSCP Course Outline

IT Administration

40 CPEs

The Official (ISC)² SSCP training provides a comprehensive review of the knowledge required to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability. This training course will help students review and refresh their knowledge and identify areas they need to study for the SSCP exam. Taught by an (ISC)²-authorized instructor, the course features:

» Official (ISC)² courseware
» Flash Cards
» Post-course assessment
» Collaboration with classmates not currently available for self-paced course
» Real-world learning activities and scenarios
» Labs available for Online Instructor-Led only

Course Agenda

» Domain 1: Access Controls
» Domain 2: Security Operations and Administration
» Domain 3: Risk Identification, Monitoring and Analysis
» Domain 4: Incident Response and Recovery
» Domain 5: Cryptography
» Domain 6: Network and Communications Security
» Domain 7: Systems and Application Security

Who Should Attend

The training seminar is ideal for those working in positions such as but not limited to:

» Network Security Engineer
» Systems/Network Administrator
» Security Analyst
» Systems Engineer
» Security Consultant/Specialist
» Security Administrator
» Systems/Network Analyst
» Database Administrator

Course Delivery Methods

» Classroom-Based
» Online Instructor-Led
» Online Self-Paced (Through Coursera Only)
» Private On-Site
SSCP Training Course

Course Objectives
Note: Course will be updated in November 2018

After completing this course, participants will be able to:

» Understand the different access control systems and how they should be implemented to protect the system and data using the different levels of confidentiality, integrity and availability.

» Understand the processes necessary for working with management and information owners, custodians and users so that proper data classifications are defined. This will ensure the proper handling of all hard copy and electronic information as it is applied by the security operations and administration.

» Identify, measure and control losses associated with adverse events, and review, analyze, select and evaluate safeguards for mitigating risk.

» Identify how to handle incident response and recovery using consistent, applied approaches including the use of the business continuity plan (BCP) and disaster recovery plan (DRP) concepts to mitigate damages, recover business operations, avoid critical business interruption, and apply emergency response and post-disaster recovery.

» Identify and differentiate key cryptographic concepts and how to apply them, implement secure protocols, key management concepts, key administration and validation, and Public Key Infrastructure as it applies to securing communications in the presence of third parties.

» Define and identify the networks and communications security needed to secure network structure, data transmission methods, transport formats, and the security measures used to maintain integrity, availability, authentication and confidentiality of the information being transmitted.

» Identify and define technical and non-technical attacks and how an organization can protect itself from these attacks including the concepts in endpoint device security, cloud infrastructure security, securing big data systems and securing virtual environments.
CCSP Course Outline

Cloud Security

40 CPEs

The Official (ISC)² CCSP training provides a comprehensive review of the knowledge required for understanding cloud computing and its information security risks and mitigation strategies. This training course will help students review and refresh their knowledge and identify areas they need to study for the CCSP exam. Taught by an (ISC)²-authorized instructor, the course features:

» Official (ISC)² courseware
» Flash Cards
» Post-course assessment
» Collaboration with classmates
  not currently available for self-paced course
» Real-world learning activities and scenarios

Who Should Attend

The training seminar is ideal for those working in positions such as but not limited to:

» Enterprise Architect
» Security Administrator
» Systems Engineer
» Security Architect
» Security Consultant
» Security Engineer
» Security Manager
» Systems Architect

Course Agenda

» Domain 1: Architectural Concepts & Design Requirements
» Domain 2: Cloud Data Security
» Domain 3: Cloud Platform & Infrastructure Security
» Domain 4: Cloud Application Security
» Domain 5: Operations
» Domain 6: Legal & Compliance

Course Delivery Methods

» Classroom-Based
» Online Instructor-Led
» Online Self-Paced
» Private On-Site
Course Objectives

After completing this course, participants will be able to:

» Describe the physical and virtual components of and identify the principle technologies of cloud based systems.

» Define the roles and responsibilities of customers, providers, partners, brokers and the various technical professionals that support cloud computing environments.

» Identify and explain the five characteristics required to satisfy the NIST definition of cloud computing.

» Differentiate between various as a service delivery models and frameworks that are incorporated into the cloud computing reference architecture.

» Discuss strategies for safeguarding data, classifying data, ensuring privacy, assuring compliance with regulatory agencies and working with authorities during legal investigations.

» Contrast between forensic analysis in corporate data center and cloud computing environments.

» Evaluate and implement the security controls necessary to ensure confidentiality, integrity and availability in cloud computing.

» Identify and explain the six phases of the data lifecycle.

» Explain strategies for protecting data at rest and data in motion.

» Describe the role of encryption in protecting data and specific strategies for key management.

» Compare a variety of cloud-based business continuity / disaster recovery strategies and select an appropriate solution to specific business requirements.

» Contrast security aspects of software development lifecycle (SDLC) in standard data center and cloud computing environments.

» Describe how federated identity and access management solutions mitigate risks in cloud computing systems.

» Conduct gap analysis between baseline and industry-standard best practices.

» Develop service level agreements (SLAs) for cloud computing environments.

» Conduct risk assessments of existing and proposed cloud-based environments.

» State the professional and ethical standards of (ISC)² and the Certified Cloud Security Professional.
CAP Course Outline

Authorization

40 CPEs

The Official (ISC)² CAP training provides a comprehensive review of the knowledge required for authorizing and maintaining information systems within the NIST Risk Management Framework. This training course will help students review and refresh their knowledge and identify areas they need to study for the CAP exam. Taught by an (ISC)²-authorized instructor, training features:

» Official (ISC)² courseware
» Flash Cards
» Collaboration with classmates
» Real-world learning activities and scenarios

Who Should Attend

The training seminar is ideal for IT, information security and information assurance practitioners and contractors who use the RMF in:

» The U.S. federal government, such as the U.S. Department of State or the Department of Defense (DoD)

» The military

» Civilian roles, such as federal contractors

» Local governments

» Private sector organizations

Course Agenda

» Domain 1: Risk Management Framework (RMF)
» Domain 2: Categorization of Information Systems
» Domain 3: Selection of Security Controls
» Domain 4: Security Control Implementation
» Domain 5: Security Control Assessment
» Domain 6: Information System Authorization
» Domain 7: Monitoring of Security Controls

Course Delivery Methods

- Classroom-Based
- Online Instructor-Led
- Private On-Site
Course Objectives

Note: Course will be updated in October 2018

After completing this course, participants will be able to:

» Describe the historical legal and business considerations that required the development of the Risk Management Framework (RMF), including related mandates.

» Identify key terminology and associated definitions.

» Describe the RMF components, including the starting point inputs (architectural description and organization inputs).

» Describe the core roles defined by the RMF, including primary responsibilities and supporting roles for each RMF step.

» Describe the core federal statutes, OMB directives, information processing standards (FIPS) and Special Publications (SP), and Department of Defense and Intelligence Community instructions that form the legal mandates and supporting guidance required to implement the RMF.

» Identify and understand the related processes integrated with the RMF.

» Identify key references related to RMF Step 1 – Categorize Information Systems.

» Identify key references related to RMF Step 2 – Select Security Controls.

» Identify key references related to RMF Step 3 – Implement Security Controls.

» Identify key references related to RMF Step 4 – Assess Security Controls.

» Identify key references related to RMF Step 5 – Authorize Information System.

» Identify key references related to RMF Step 6 – Monitor Security Controls.
CSSLP Course Outline

Software Security

40 CPEs

The Official (ISC)² CSSLP training provides a comprehensive review of the knowledge required to incorporate security practices – authentication, authorization and auditing – into each phase of the Software Development Lifecycle (SDLC), from software design and implementation to testing and deployment. This training course will help students review and refresh their knowledge and identify areas they need to study for the CSSLP exam. Taught by an (ISC)²-authorized instructor, training features:

» Official (ISC)² courseware
» Flash Cards
» Collaboration with classmates
» Real-world learning activities and scenarios
» Labs available for Online Instructor-Led only

Who Should Attend

The training seminar is ideal for those working in positions such as but not limited to:

» Software Architect
» Software Engineer
» Software Developer
» Application Security Specialist
» Software Program Manager
» Quality Assurance Tester
» Penetration Tester
» Software Procurement Analyst
» Project Manager
» Security Manager
» IT Director/Manager

Course Agenda

» Domain 1: Secure Software Concepts
» Domain 2: Secure Software Requirements
» Domain 3: Secure Software Design
» Domain 4: Secure Software Implementation/Programming
» Domain 5: Secure Software Testing
» Domain 6: Secure Lifecycle Management
» Domain 7: Software Deployment, Operations and Maintenance
» Domain 8: Supply Chain and Software Acquisition

Course Delivery Methods

» Classroom-Based
» Online Instructor-Led
» Private On-Site
Course Objectives

After completing this course, participants will be able to:

» Identify the software methodologies needed to develop software that is secure and resilient to attacks.

» Incorporate security requirements in the development of software to produce software that is reliable, resilient and recoverable.

» Understand how to ensure that software security requirements are included in the design of the software, gain knowledge of secure design principles and processes, and gain exposure to different architectures and technologies for securing software.

» Understand the importance of programming concepts that can effectively protect software from vulnerabilities. Learners will touch on topics such as software coding vulnerabilities, defensive coding techniques and processes, code analysis and protection, and environmental security considerations that should be factored into software.

» Address issues pertaining to proper testing of software for security, including the overall strategies and plans. Learners will gain an understanding of the different types of functional and security testing that should be performed, the criteria for testing, concepts related to impact assessment and corrective actions, and the test data lifecycle.

» Understand the requirements for software acceptance, paying specific attention to compliance, quality, functionality and assurance. Participants will learn about pre- and post-release validation requirements as well as pre-deployment criteria.

» Understand the deployment, operations, maintenance and disposal of software from a secure perspective. This is achieved by identifying processes during installation and deployment, operations and maintenance, and disposal that can affect the ability of the software to remain reliable, resilient and recoverable in its prescribed manner.

» Understand how to perform effective assessments on an organization’s cyber-supply chain, and describe how security applies to the supply chain and software acquisition process. Learners will understand the importance of supplier sourcing and being able to validate vendor integrity, from third-party vendors to complete outsourcing. Finally, learners will understand how to manage risk through the adoption of standards and best practices for proper development and testing across the entire lifecycle of products.
HCISPP Course Outline

Healthcare Security and Privacy

24 CPEs

The Official (ISC)² HCISPP training provides a comprehensive review of the knowledge required to implement, manage or assess the appropriate security and privacy controls of a healthcare organization. This training course will help students review and refresh their knowledge and identify areas they need to study for the HCISPP exam. Taught by an (ISC)²-authorized instructor, it features:

» Official (ISC)² courseware
» Flash Cards
» Collaboration with classmates
» Real-world learning activities and scenarios

Course Agenda

» Domain 1: Healthcare Industry
» Domain 2: Regulatory Environment
» Domain 3: Privacy and Security in Healthcare
» Domain 4: Information Governance and Risk Management
» Domain 5: Information Risk Assessment
» Domain 6: Third Party Risk Management

Who Should Attend

The training seminar is ideal for those working in positions such as but not limited to:

» Compliance Officer
» Information Security Manager
» Privacy Officer
» Compliance Auditor
» Risk Analyst
» Medical Records Supervisor
» Information Technology Manager
» Privacy and Security Consultant
» Health Information Manager
» Practice Manager

Course Delivery Methods

» Classroom-Based
» Online Instructor-Led
» Private On-Site
Course Objectives

After completing this course, participants will be able to:

» Conceptualize the diversity in the healthcare industry. To achieve this, learners will gain knowledge of the diverse types of healthcare organizations, types of technologies, how information and data flows and is managed, how data is exchanged, and the levels of protection required for that data.

» Identify and describe the relevant legal and regulatory requirements regarding healthcare information. These requirements are necessary to ensure that the organization's policies and procedures are in compliance and that all trans-border data exchange procedures are followed.

» Describe security and privacy concept principles as they relate to the Healthcare industry. Learners will be able to understand the relationship of security and privacy, and how to manage and handle all information requiring data protection in the healthcare industry.

» Identify how organizations manage information risk, and what security and privacy governance means for that information. Learners will be introduced to basic risk management methods and lifecycles, and the activities that support these concepts.

» Describe risk assessment, and the risk assessment practices and procedures for an organization.

» Identify concepts for managing third-party relationships. Learners will gain knowledge regarding concepts pertaining to their use of information, any additional security and privacy assurances, third-party assessments, third-party security and privacy events, and recognize the mitigation process of third-party risks.
Interested in harnessing the power of partnership to grow your business?

For more information on becoming an (ISC)² Training – Official Provider, please contact our team at otp@isc2.org or 1.866.331.4722 ext. 3.