COURSE OVERVIEW IE1065

Certified Information System Security Professional

(ISC Exam Preparation Training)

Course Title

Certified Information System Security Professional *(ISC Exam Preparation Training)*

H-STK© INCLUDED

Course Reference

IE1065

Course Duration/Credits

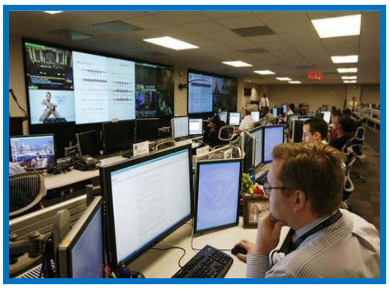
Five days/3.0 CEUs/30 PDHs

3.0 CEUs (30 PDHs) AWARD

Course Date/Venue

Session(s)	Date	Venue
1	January 15-19, 2024	Ajman Meeting Room, Grand Millennium Al Wahda Hotel, Abu Dhabi, UAE
2	April 14-18, 2024	Business Center, Concorde Hotel Doha, Doha, Qatar
3	July 07-11, 2024	Jubail Hall, Signature Al Khobar Hotel, Al Khobar, KSA
4	October 20-24, 2024	Boardroom 1, Elite Byblos Hotel Al Barsha, Sheikh Zayed Road, Dubai, UAE

Course Description



This practical and highly-interactive course includes real-life case studies where participants will be engaged in a series of interactive small groups and class workshops.

This course is designed to provide participants with a detailed and up-to-date overview of Certified Information System Security Professional. It covers the security and risk management; the concepts of confidentiality, integrity and availability; the security governance principles, compliance requirements and legal and regulatory issues that pertain to information security in a global context; the business continuity (BC) requirements and personnel security policies and procedures; and the risk management and threat modeling concepts, methodologies and risk-based management concepts to the supply chain.

Further, the course will also discuss the security awareness, education and training program; the asset security, privacy, appropriate asset retention, data security controls and information and asset handling requirements; the security architecture and engineering; the fundamental concepts of security models; and the systems security requirements, security architectures, designs and solution elements.

Participants of the course will be able to assess and mitigate vulnerabilities in web-based systems, mobile systems and embedded devices; apply cryptography, security principles to site and facility design as well as implement site and facility security controls; employ communication and network security; implement secure design principles in network architectures and identify secure network components; implement secure communication channels according to design; recognize identity and access management (IAM), control physical and logical access to assets; manage identification and authentication of people, devices, and services; integrate identity as a third-party service; implement and manage authorization mechanisms and manage the identity and access provisioning lifecycle; carryout security assessment and testing as well as design and validate assessment, test, and audit strategies and conduct security control testing; and collect security process, analyze test output, generate report and conduct or facilitate security audits.

During this interactive course, participants will learn the security operations, support investigations and the requirements for investigation types; the logging and monitoring activities, provisioning resources and foundational security operations concepts and resource protection techniques; the incident management, detective and preventative measures and patch and vulnerability management; the change management processes, recovery strategies, disaster recovery (DR) processes and disaster recovery plans (DRP); the business continuity (BC) planning and exercises, physical security and personnel safety and security concerns; the software development security, security in the software development life cycle (SDLC) and security controls in development environments; the effectiveness of software security and security impact of acquired software; and the coding guidelines and standard.

Course Objectives

Upon the successful completion of this course, each participant will be able to:-

- Get prepared for the next ISC^2-CISSP exam and have enough knowledge and skills to pass such exam in order to get the CISSP certification
- Carryout security and risk management as well as apply concepts of confidentiality, integrity and availability
- Evaluate and apply security governance principles, determine compliance requirements and identify legal and regulatory issues that pertain to information security in a global context
- Adhere and promote professional ethics as well as develop, document and implement security policy, standards, procedures and guidelines
- Identify, analyze and prioritize business continuity (BC) requirements and contribute and enforce personnel security policies and procedures
- Apply risk management concepts, threat modeling concepts and methodologies and risk-based management concepts to the supply chain
- Establish and maintain a security awareness, education and training program
- Employ asset security, identify and classify information and assets as well as determine and maintain information and asset ownership

- Protect privacy, ensure appropriate asset retention, determine data security controls and establish information and asset handling requirements
- Recognize security architecture and engineering, implement and manage engineering processes using secure design principle and identify the fundamental concepts of security models
- Select controls based upon systems security requirements, discuss security capabilities of information systems and assess and mitigate the vulnerabilities of security architectures, designs and solution elements
- Assess and mitigate vulnerabilities in web-based systems, mobile systems and embedded devices
- Apply cryptography, security principles to site and facility design as well as implement site and facility security controls
- Employ communication and network security, implement secure design principles in network architectures and identify secure network components
- Implement secure communication channels according to design
- Discuss identity and access management (IAM), control physical and logical access to assets and manage identification and authentication of people, devices, and services
- Integrate identity as a third-party service, implement and manage authorization mechanisms and manage the identity and access provisioning lifecycle
- Carryout security assessment and testing as well as design and validate assessment, test, and audit strategies and conduct security control testing
- Collect security process, analyze test output, generate report and conduct or facilitate security audits
- Apply security operations, support investigations and identify the requirements for investigation types
- Conduct logging and monitoring activities, secure provisioning resources and apply foundational security operations concepts and resource protection techniques
- Conduct incident management, operate and maintain detective and preventative measures and implement and support patch and vulnerability management
- Participate in change management processes, implement recovery strategies and disaster recovery (DR) processes and test disaster recovery plans (DRP)
- Participate in business continuity (BC) planning and exercises, implement and manage physical security and address personnel safety and security concerns
- Implement software development security, integrate security in the software development life cycle (SDLC) and identify and apply security controls in development environments
- Assess the effectiveness of software security and security impact of acquired software as well as apply secure coding guidelines and standard

Exclusive Smart Training Kit - H-STK®

*Participants of this course will receive the exclusive "Haward Smart Training Kit" (**H-STK®**). The **H-STK®** consists of a comprehensive set of technical content which includes **electronic version** of the course materials, sample video clips of the instructor's actual lectures & practical sessions during the course conveniently saved in a **Tablet PC**.*

Who Should Attend

This course provides an overview of all significant aspects and considerations of system security for information security managers, IT and corporate security managers, corporate governance managers, risk and compliance managers and information security. It is especially relevant for those who have the responsibility to implement information security management in a business or provide consultation on the subject.

Training Methodology

This interactive training course includes the following training methodologies as a percentage of the total tuition hours:-

30%	Lectures
20%	Workshops & Work Presentations
30%	Case Studies & Practical Exercises
20%	Software, Simulators & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

Course Fee

Abu Dhabi	**US$ 5,500** per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day
Doha	**US$ 6,500** per Delegate. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.
Al Khobar	**US$ 5,500** per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.
Dubai	**US$ 5,500** per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Accommodation

Accommodation is not included in the course fees. However, any accommodation required can be arranged at the time of booking.

Course Certificate(s)

Internationally recognized certificates will be issued to all participants of the course who completed a minimum of 80% of the total tuition hours.

Certificate Accreditations

Certificates are accredited by the following international accreditation organizations: -

- The International Accreditors for Continuing Education and Training (IACET - USA)

Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units** (CEUs) in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

Haward Technology Middle East will award **3.0 CEUs** (Continuing Education Units) or **30 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant's involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant's CEU and PDH Transcript of Records upon request.

British Accreditation Council (BAC)

Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.

Course Instructor(s)

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:

Dr. Pan Glou, PhD, BSc, is a **Senior IT**, **Telecommunications**, **Control & Electronics Engineer** with over **29 years** of extensive experience in the areas of **Web Programming**, **Gamification Techniques**, Internal & External Auditing, **E-Commerce Strategies**, **Advanced Database Management Systems**, **Web Design**, **HCI**, **3D Animation**, **Multimedia Design**, **OS Architectures** and **Network Security, Information** & **Technology Architectures**, **Application Architecture**, **Portfolio Management**, **Application Security**, **Application Integration Technologies** & **Strategies**, **Solution Architecture Patterns**, **Web Applications** & Services, **Logical Applications**, **Interfaces** & Services, Logical & Physical Components, **Mobile** & **Cloud Applications**, **Blended Learning Programs**. Further, he is also well-versed in SQL Server, ASP.NET Web Core Apps, Power BI, Web Services, IIS, MS Access Databases, MS Excel & Word, HTML5, CSS3, jQuery, Javascript and Syncfusion.

During his career life, Dr. Glou has gained his practical and field experience through his various significant positions and dedication as the **IT Director**, **Head IT**, **Senior Analyst, Analyst**, **Senior Data Analyst**, **Head** of **Development**, **Project Manager**, **Senior Developer**, **Database Administrator**, **Development Team Leader**, **Team Leader**, **Supervisor**, **Senior Developer**, **Technical Consultant**, **Database Administrator**, **Developer (Part time), Technical Supervisor**, **IT Manager**, **Instructor**, **Professor** and **Assistant Professor** for various companies and universities such as METAdrasi, KPI Metrics Solution, Athens Doctors Association, Athens Dentists Association, Chania Bank, Medical Office, INTERFINAN Single P.C., ODEON, Business or Sector Entertainment Industry, NERIT, Supermarket AB Vasilopoulos, VIVODI Telecommunications, CITIBANK, Eurobank Cards, OASP, Ministry of Environment and Public Works, VIKELAS J. & A., Colgate Palmolive Hellas S.A.A. and Tsaoussoglou.

Dr. Glou has a **PhD** in **Partial Query Evaluation** on **Very Large Databases** with **Error Probability** from the **National Technical University of Athens**, and a **Bachelor's degree** in **Mathematics** from the **University** of **Patras**, **Greece**. Further, he is a **Certified Instructor/Trainer** and has delivered numerous trainings, courses, workshops, seminars and conferences internationally.

Course Program

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the course for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

Day 1

0730 – 0800	*Registration & Coffee*
0800 – 0830	*Welcome & Introduction*
0830 – 0845	***PRE-TEST***
0845 – 1100	***Security & Risk Management*** *Understand & Apply Concepts of Confidentiality, Integrity & Availability ● Evaluate & Apply Security Governance Principles ● Determine Compliance Requirements ● Understand Legal & Regulatory Issues That Pertain to Information Security in a Global Context ● Understand, Adhere To & Promote Professional Ethics ● Develop, Document & Implement Security Policy, Standards, Procedures & Guidelines ● Identify, Analyze & Prioritize Business Continuity (BC) Requirements*
1100 – 1115	*Break*
1115 – 1230	***Security & Risk Management (cont'd)*** *Contribute to & Enforce Personnel Security Policies & Procedures ● Understand & Apply Risk Management Concepts ● Understand & Apply Threat Modeling Concepts & Methodologies ● Apply Risk-Based Management Concepts to the Supply Chain ● Establish & Maintain a Security Awareness, Education & Training Program*
1230 – 1330	***Asset Security*** *Identify & Classify Information & Assets ● Determine & Maintain Information & Asset Ownership ● Protect Privacy*
1330 – 1345	*Break*
1345 – 1420	***Asset Security (cont'd)*** *Ensure Appropriate Asset Retention ● Determine Data Security Controls ● Establish Information & Asset Handling Requirements*
1420 – 1430	***Recap***
1430	*Lunch & End of Day One*

Day 2

0730 – 0930	***Security Architecture & Engineering*** *Implement & Manage Engineering Processes Using Secure Design Principles ● Understand the Fundamental Concepts of Security Models ● Select Controls Based Upon Systems Security Requirements*
0930 – 0945	*Break*
0945 – 1130	***Security Architecture & Engineering (cont'd)*** *Understand Security Capabilities of Information Systems (E.G., Memory Protection, Trusted Platform Module (TPM), Encryption/Decryption) ● Assess & Mitigate the Vulnerabilities of Security Architectures, Designs & Solution Elements ● Assess & Mitigate Vulnerabilities in Web-Based Systems*
1130 - 1300	***Security Architecture & Engineering (cont'd)*** *Assess & Mitigate Vulnerabilities in Mobile Systems ● Assess & Mitigate Vulnerabilities in Embedded Devices ● Apply Cryptography*
1300 – 1315	*Break*

1315 - 1420	***Security Architecture & Engineering (cont'd)*** *Apply Security Principles to Site & Facility Design ● Implement Site & Facility Security Controls*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Two*

Day 3

0730 – 0930	***Communication & Network Security*** *Implement Secure Design Principles in Network Architectures ● Secure Network Components*
0930 – 0945	*Break*
0945 – 1130	***Communication & Network Security (cont'd)*** *Implement Secure Communication Channels According to Design*
1130 – 1300	***Identity & Access Management (IAM)*** *Control Physical & Logical Access to Assets ● Manage Identification & Authentication of People, Devices & Services ● Integrate Identity as a Third-Party Service*
1300 - 1315	*Break*
1315 - 1420	***Identity & Access Management (IAM) (cont'd)*** *Implement & Manage Authorization Mechanisms ● Manage the Identity & Access Provisioning Lifecycle*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Three*

Day 4

0730 – 0930	***Security Assessment & Testing*** *Design & Validate Assessment, Test, & Audit Strategies ● Conduct Security Control Testing ● Collect Security Process Data (e.g., Technical & Administrative)*
0930 – 0945	*Break*
0945 – 1130	***Security Assessment & Testing (cont'd)*** *Analyze Test Output & Generate Report ● Conduct or Facilitate Security Audits*
1130 – 1300	***Security Operations*** *Understand & Support Investigations ● Understand Requirements for Investigation Types ● Conduct Logging & Monitoring Activities ● Securely Provisioning Resources*
1300 – 1315	*Break*
1315 - 1420	***Security Operations (cont'd)*** *Understand & Apply Foundational Security Operations Concepts ● Apply Resource Protection Techniques ● Conduct Incident Management ● Operate & Maintain Detective & Preventative Measures*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Four*

Day 5

0730 – 0930	***Security Operations (cont'd)*** *Implement & Support Patch & Vulnerability Management ● Understand & Participate in Change Management Processes ● Implement Recovery Strategies ● Implement Disaster Recovery (DR) Processes*
0930 – 0945	*Break*

0945 – 1100	***Security Operations (cont'd)*** *Test Disaster Recovery Plans (DRP) ● Participate in Business Continuity (BC) Planning & Exercises ● Implement & Manage Physical Security ● Address Personnel Safety & Security Concerns*
1100 – 1200	***Software Development Security*** *Understand & Integrate Security in The Software Development Life Cycle (SDLC) ● Identify & Apply Security Controls in Development Environments*
1200 – 1215	*Break*
1215 – 1345	***Software Development Security (cont'd)*** *Assess the Effectiveness of Software Security ● Assess Security Impact of Acquired Software ● Define & Apply Secure Coding Guidelines & Standards*
1345 – 1400	***Course Conclusion***
1400 – 1415	***POST TEST***
1415 – 1430	*Presentation of Course Certificates*
1430	*Lunch & End of Course*

Practical Sessions

This practical and highly-interactive course includes real-life case studies and exercises:-

Course Coordinator

Kamel Ghanem, Tel: +971 2 30 91 714, Email: kamel@haward.org