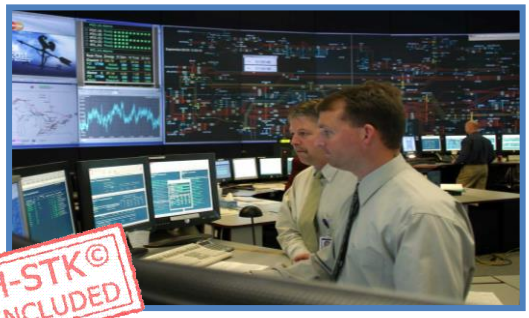
COURSE OVERVIEW IE0709-3D
Certified Cyber Security Practitioner
(ISACA Exam Preparation Training)

Course Title
Certified Cyber Security Practitioner
(ISACA Exam Preparation Training)

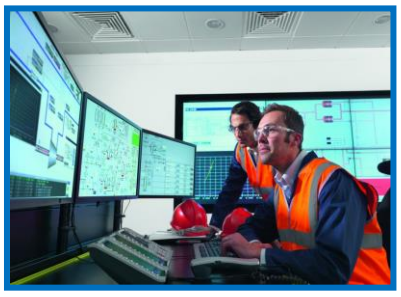


Course Date/Venue
September 15-17, 2025/Ajman Meeting Room, Grand Millennium Al Wahda Hotel, Abu Dhabi, UAE

Course Reference
IE0709-3D

Course Duration/Credits
Three days/1.8 CEUs/18 PDHs

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 cyber security. It covers the business and security environment including digital infrastructure, enterprise architecture, data and digital communication; the security environment that include network, operating systems, applications, virtualization and cloud; the operational security readiness, protection and preparedness as well as digital and data assets, ports and protocols, protection technologies, access management and configuration management; and the threat modeling, contingency planning and security procedures.

During this interactive course, participants will learn the threat detection and evaluation by monitoring vulnerability management, security logs and alerts, monitoring tools and appliances, uses cases and penetration testing; analyzing the network traffic, packet capture, data, research and correlation; the incident response and recovery, restoring incident handling, notifications, escalation and digital forensics; and mitigating containment, attack countermeasures and corrective actions as well as restoring security functions validation, incident analysis, reporting and process improvement.

Course Objectives

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

- Prepare for next ISACA exam and have enough knowledge and skills to pass such exam in order to get the ISACA certification
- Discuss business and security environment covering digital infrastructure, enterprise architecture, data and digital communication
- Recognize security environment that include network, operating systems, applications, virtualization and cloud
- Carryout operational security readiness, protection and preparedness as well as digital and data assets, ports and protocols, protection technologies, access management and configuration management
- Illustrate threat modeling, contingency planning and security procedures
- Employ threat detection and evaluation by monitoring vulnerability management, security logs and alerts, monitoring tools and appliances, uses cases and penetration testing
- Analyze network traffic, packet capture, data, research and correlation
- Apply incident response and recovery, incident handling, notifications, escalation and digital forensics
- Mitigate containment, attack countermeasures and corrective actions as well as restore security functions validation, incident analysis, reporting and process improvement

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 conveniently saved in a **Tablet PC**.*

Who Should Attend

This course provides an overview of all significant aspects and considerations of certified cyber security practitioner maintenance for a broad audience that includes asset owners from process, power and other critical infrastructures, control systems engineers, IT engineers, IT professionals, instrumentations engineers, instrumental & control staff, information and security officers and vendors, as well as security experts from government, industry associations and academia.

Course Fee

US$ 3,750 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

Training Methodology

All our Courses are including **Hands-on Practical Sessions** using equipment, State-of-the-Art Simulators, Drawings, Case Studies, Videos and Exercises. The courses include the following training methodologies as a percentage of the total tuition hours:-

30% Lectures
20% Practical Workshops & Work Presentations
30% Hands-on Practical Exercises & Case Studies
20% Simulators (Hardware & Software) & Videos

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

Exam Eligibility & Structure

Exam Candidates shall have the following minimum prerequisites:-

- Possess any one of the following Professional Certifications:-

- CISA	- ECSA
- CISM	- LPT
- CRISC	- GCIH
- CGEIT	- OSCP
- CPTO	- GPEN
- CSX Cybersecurity Fundamentals Certificate	- CySA+
- CEH	- CISSP

OR,

- Possess three years of experience in three of the five cybersecurity activity domains:

  - CISSP
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover

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 **1.8 CEUs** (Continuing Education Units) or **18 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. Mohamed Zayan, PhD, MSc, BSc, is a **Senior Communications & Telecommunications Engineer** with over **25 years** of industrial experience in the field of **Cyber Security**, **IT/Network Auditing**, **IT Security Governance**, **Networking & Communications System, Physical Security**, **Security Systems**, **Information Security Management System** (IS0/IEC 27001), **Security Systems** Installation & Maintenance, **IT Confidentiality & Security**, **IT Application Security & Compliance**, **Security Logs & Alerts**, **Digital Forensics**, **Security Functions Validation**, **IT Management**, **Information Technology System**, **Information Confidentiality**, **Data Confidentiality** Classification, System Analysis, **E-Communication** & Collaboration Skills, Instrumentation & Control System, Digital & Data Communications, Control Loop Analysis & Troubleshooting, **Wireless Technology**, **Digital & Satellite** Communication, Digital Signal Processing, VOIP, SDH, SONET, DWDM, ADM, APS, DCC, HFC, SPE, EDFA, MPLS, BER, Electronics, Networking, Frequency assignment, System Identification and Adaptive Control, ISO/IGC 27001, ISO 27002, ISO 27003, ISO 21827 and software tools such as **MAZA3**, **STK C/C++** and **UNIX**. Further, he is also well-versed in **SIL**, **SIS**, **ESD**, **DCS**, **PLC & SCADA**, Structured Cabling System (**SCS**), Compressor Control & Protection, Gas Turbine Control & Protection System, HVAC Direct Digital Control (**DDC**), Liquid & Gas Multiphase Flowmetring, **Substation Automation** Systems & Application, Process Control and Communication. He is further an **Authority** in **PLC**, **DCS**, **SCADA** and **Fieldbus** engineering and technology. He is currently the **Satellite Control Station Manager** & **Satellite Operation Engineer** of **Nilesat** wherein he is in-charge of the security system engineering for the system and subsystems and operation of the spacecraft and Satellite Control Center (SCC).

Dr. Mohamed has already proven his proficiency since the time he started his career as a **Design Engineer** with **USAID** wherein he was in-charge of designing and installing modern process computer control systems and Distributed Control Systems (**DCS**). He later on worked as a **Senior Communications Engineer** where he administered the maintenance & operation of VHF & UHF transmitters. Afterwards he moved to be in-charge of **Information Security System Engineering** and operation of a Spacecraft and Satellite Control Center (SCC). Further, he worked as an **Operations Engineer**, **Lecture and Information Technology Instructor** wherein his duties include system design, installation, testing & commissioning as well as developing and implementing the latest transmission, modulation, **instrumentation**, **control**, compression, coding, encryption & broadband techniques and applications along with **securing** the entire security system of the organization.

Among his many achievements, Dr. Mohamed was nominated as a member of the Reviewing Committee of the International Conference on Computing Communications and Control Technologies (CCCT) of the University of Texas at Austin and the International Institute of Informatics and Systemic (IIIS) in the USA. Motivated by his significant involvement and contribution in the industry, he has authored papers & publications about **security system**, communication technology, **instrumentation** & **control** engineering and neural networks that were presented in **various international conferences**. He has also lectured worldwide on various subjects such as **security management system**, **flowmetering**, **instrumentation**, **control**, microwave engineering, IT, system realization, neural networks, control systems and digital communication.

Dr. Mohamed has a **PhD** in **Electrical Engineering**, a **Master's degree** in **Digital Communication Engineering**, a **Bachelor's degree** in **Communication & Electro-physics** and attained his Postgraduate **Diploma** in **Spacecraft Control Engineering** from Matra Marconi Space (Toulouse Plant) in **France**. He is currently active as the **Board Member** of the Egyptian **Space Board & Remote Security Council**. He further **won** the 9th European Satellite Navigation Competition (ESNC) with his innovative project to implement autonomous location monitoring for satellites in orbit.

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: Monday, 15th of September 2025

0730 – 0800	*Registration & Coffee*
0800 – 0815	*Welcome & Introduction*
0815 – 0830	***PRE-TEST***
0830 – 0930	***Business & Security Environment (ID)*** *Business Environment (Digital Infrastructure ● Enterprises Architecture ● Data & Digital Communication)*
0930 – 0945	*Break*
0945 – 1100	***Business & Security Environment (ID) (cont'd)*** *Security Environment (Network ● Operating Systems ● Applications ● Virtualization & Cloud)*
1100 – 1200	***Operational Security Readiness (PR)*** *Protection (Digital & Data Assets ● Ports & Protocols ● Protection Technologies ● Identify & Access Management ● Configuration Management)*
1200 – 1215	*Break*
1215 – 1420	***Operational Security Readiness (PR) (cont'd)*** *Preparedness (Threat Modeling ● Contingency Planning ● Security Procedures)*
1420 – 1430	***Recap***
1430	*Lunch & End of Day One*

Day 2: Tuesday, 16th of September 2025

0730 – 0930	***Threat Detection & Evaluation (DE)*** *Monitoring (Vulnerability Management ● Security Logs & Alerts ● Monitoring Tools & Appliances)*
0930 – 0945	*Break*
0945 – 1100	***Threat Detection & Evaluation (DE) (cont'd)*** *Monitoring (Use Cases ● Penetration Testing)*
1100 – 1200	***Threat Detection & Evaluation (DE) (cont'd)*** *Analysis (Network Traffic Analysis ● Packet Capture & Analysis)*
1200 – 1215	*Break*
1215 – 1420	***Threat Detection & Evaluation (DE) (cont'd)*** *Analysis (Data Analysis ● Research & Correlation)*
1420 – 1430	***Recap***
1430	*Lunch & End of Day Two*

Day 3: Wednesday, 17th of September 2025

0730 – 0930	***Incident Response & Recovery (RS & RC)*** *Incident Handling (Notification & Escalation ● Digital Forensics)*
0930 – 0945	*Break*
0945 – 1100	***Incident Response & Recovery (RS & RC) (cont'd)*** *Mitigation (Containment ● Attack Countermeasures ● Corrective Actions)*
1100 – 1230	***Incident Response & Recovery (RS & RC) (cont'd)*** *Restoration (Security Functions Validation ● Incident Analysis & Reporting)*
1230 – 1245	*Break*

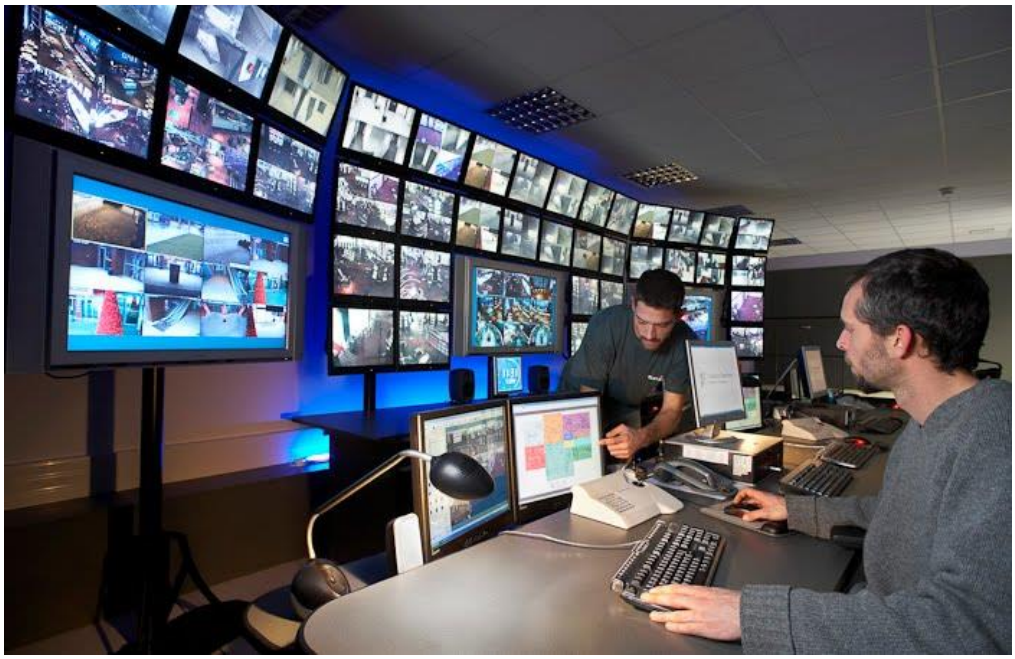
1245 – 1345	***Incident Response & Recovery (RS & RC) (cont'd)*** *Restoration (Lessons Learned & Process Improvement)*
1345 – 1400	***Course Conclusion***
1400 – 1415	***POST-TEST***
1415 – 1430	*Presentation of Course Certificates*
1430	*Lunch & End of Course*

MOCK Exam

Upon the completion of the course, participants have to sit for a MOCK Examination similar to the exam of the Certification Body through Haward's Portal. Each participant will be given a username and password to log in Haward's Portal for the MOCK Exam during the 30 days following the course completion. Each participant has only one trial for the MOCK exam within this 30-day examination window. Hence, you have to prepare yourself very well before starting your MOCK exam as this exam is a simulation to the one of the Certification Body.

Practical Sessions

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



Course Coordinator

Mari Nakintu, Tel: +971 2 30 91 714, Email: mari1@haward.org