COURSE OVERVIEW HE1354

Security Risk Assessment & Management

Course Title

Security Risk Assessment & Management

Course Date/Venue

February 11-15, 2024/Hourous Meeting Room,
Holiday Inn Suites Maadi, Cairo, Egypt

Course Reference

HE1354

Course Duration/Credits

Five days/3.0 CEUs/30 PDHs

3.0 CEUs (30 PDHs) AWARD

H-STK© INCLUDED

Course Description

This practical and highly-interactive course includes various practical sessions and exercises. Theory learnt will be applied using our state-of-the-art simulators.

This course is designed to provide participants with a detailed and up-to-date overview of Security Risk Assessment & Management. It covers the types, purpose and importance of security risk assessment; the potential threats, assess vulnerabilities and risk analysis; the threat modeling and assessing and mitigating physical security risks; the cyber security and personal security and security risk management; the emergency response planning, business continuity planning and security policies and procedures; the compliance and regulation requirements; and developing a compliance program and monitoring and audit compliance.

During this interactive course, participants will learn the communication strategies, stakeholder management and developing a security risk communication plan; the risk treatment measures and risk assessment tools and techniques; gathering, analyzing and utilizing threat intelligence and developing a security awareness training program; developing risk reporting and metrics; and analyzing and interpreting risk data and improving security risk management using risk reporting and metrics.

Course Objectives

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

- Apply and gain an in-depth knowledge on security risk assessment and management
- Discuss the types, purpose and importance of security risk assessment
- Identify potential threats, assess vulnerabilities and apply risk analysis
- Illustrate threat modeling and assess and mitigate physical security risks
- Identify cyber security and personal security as well as apply security risk management
- Employ emergency response planning, business continuity planning and security policies and procedures
- Implement compliance and regulation requirements, develop a compliance program and monitor and audit compliance
- Carryout communication strategies, stakeholder management and developing a security risk communication plan
- Monitor and review risk treatment measures and apply risk assessment tools and techniques
- Gather, analyze and utilize threat intelligence as well as develop a security awareness training program
- Develop risk reporting and metrics, analyze and interpret risk data and improve security risk management using risk reporting and metrics

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 security risk assessment and management for security managers, superintendents, shift superintendents, supervisors and technical representatives including similar management levels of the other organizations and entities that interface with security functions. Senior employees, security directors, loss prevention & risk managers, consultants, facility operators and security personnel responsible for the industrial security and assets protection will also benefit from this course.

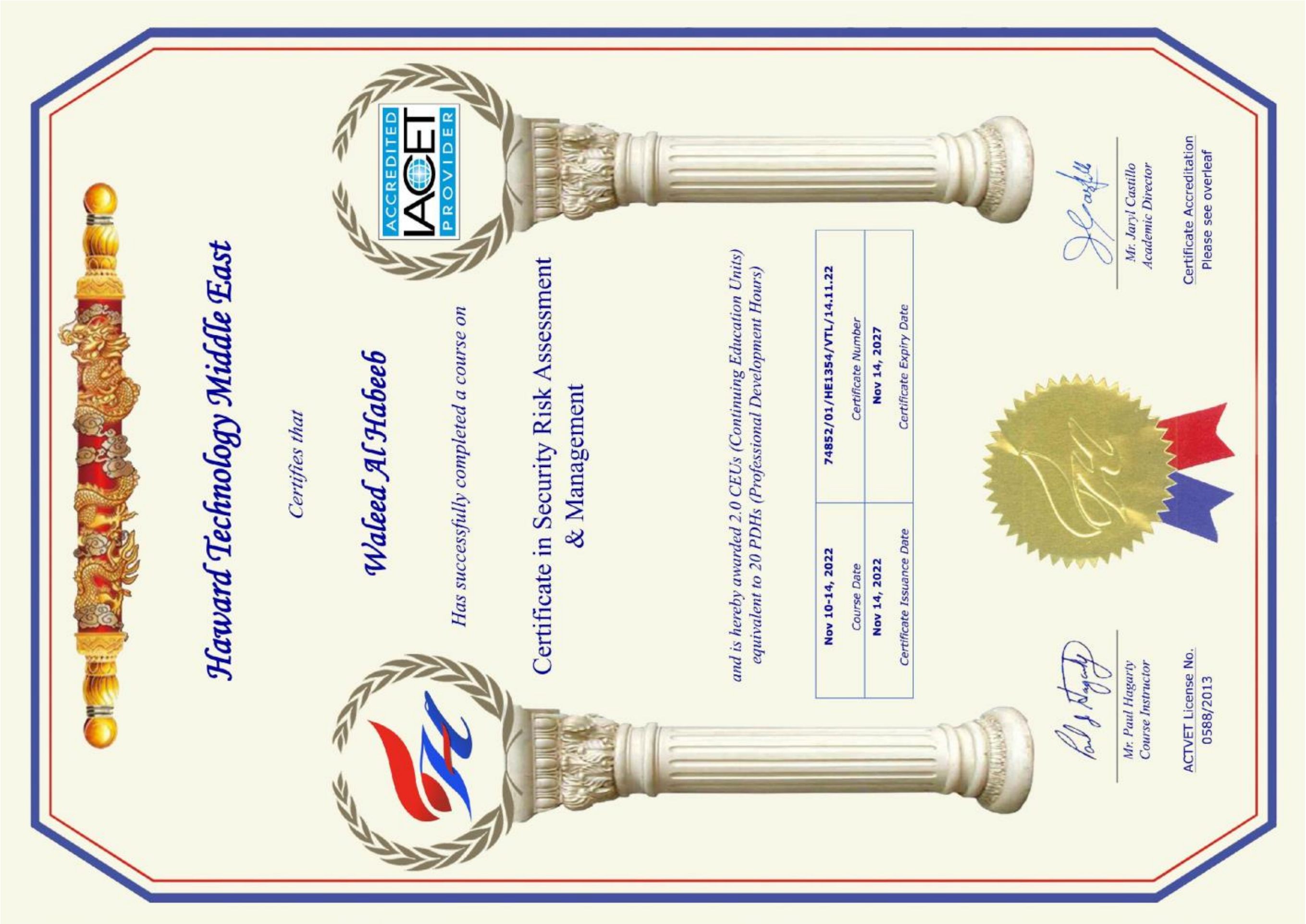
Course Certificate(s)

(1) Internationally recognized Competency Certificates and Plastic Wallet Cards will be issued to participants who completed a minimum of 80% of the total tuition hours and successfully passed the exam at the end of the course. Certificates are valid for 5 years.

Recertification is FOC for a Lifetime.

Sample of Certificates

The following are samples of the certificates that will be awarded to course participants:-



ACCREDITED IACET PROVIDER

Haward Technology Middle East

Certifies that

Waleed Al Habeeb

Has successfully completed a course on

Certificate in Security Risk Assessment & Management

and is hereby awarded 2.0 CEUs (Continuing Education Units) equivalent to 20 PDHs (Professional Development Hours)

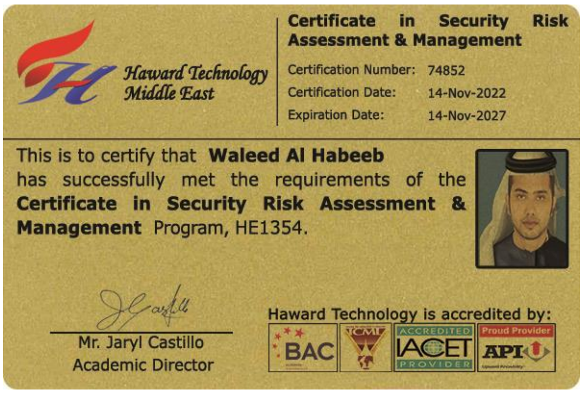
Nov 10-14, 2022 *Course Date*	**74852/01/HE1354/VTL/14.11.22** *Certificate Number*
Nov 14, 2022 *Certificate Issuance Date*	**Nov 14, 2027** *Certificate Expiry Date*

Mr. Paul Hagarty
Course Instructor

Mr. Jaryl Castillo
Academic Director

ACTVET License No.
0588/2013

Certificate Accreditation
Please see overleaf



Haward Technology Middle East

Certificate in Security Risk Assessment & Management

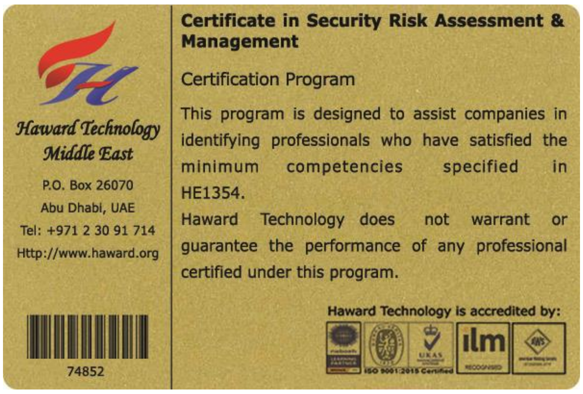
Certification Number:	74852
Certification Date:	14-Nov-2022
Expiration Date:	14-Nov-2027

This is to certify that **Waleed Al Habeeb** has successfully met the requirements of the **Certificate in Security Risk Assessment & Management** Program, HE1354.

Mr. Jaryl Castillo
Academic Director

Haward Technology is accredited by:

BAC
ICML
ACCREDITED IACET PROVIDER
Proud Provider API



Haward Technology Middle East

P.O. Box 26070
Abu Dhabi, UAE
Tel: +971 2 30 91 714
Http://www.haward.org

74852

Certificate in Security Risk Assessment & Management

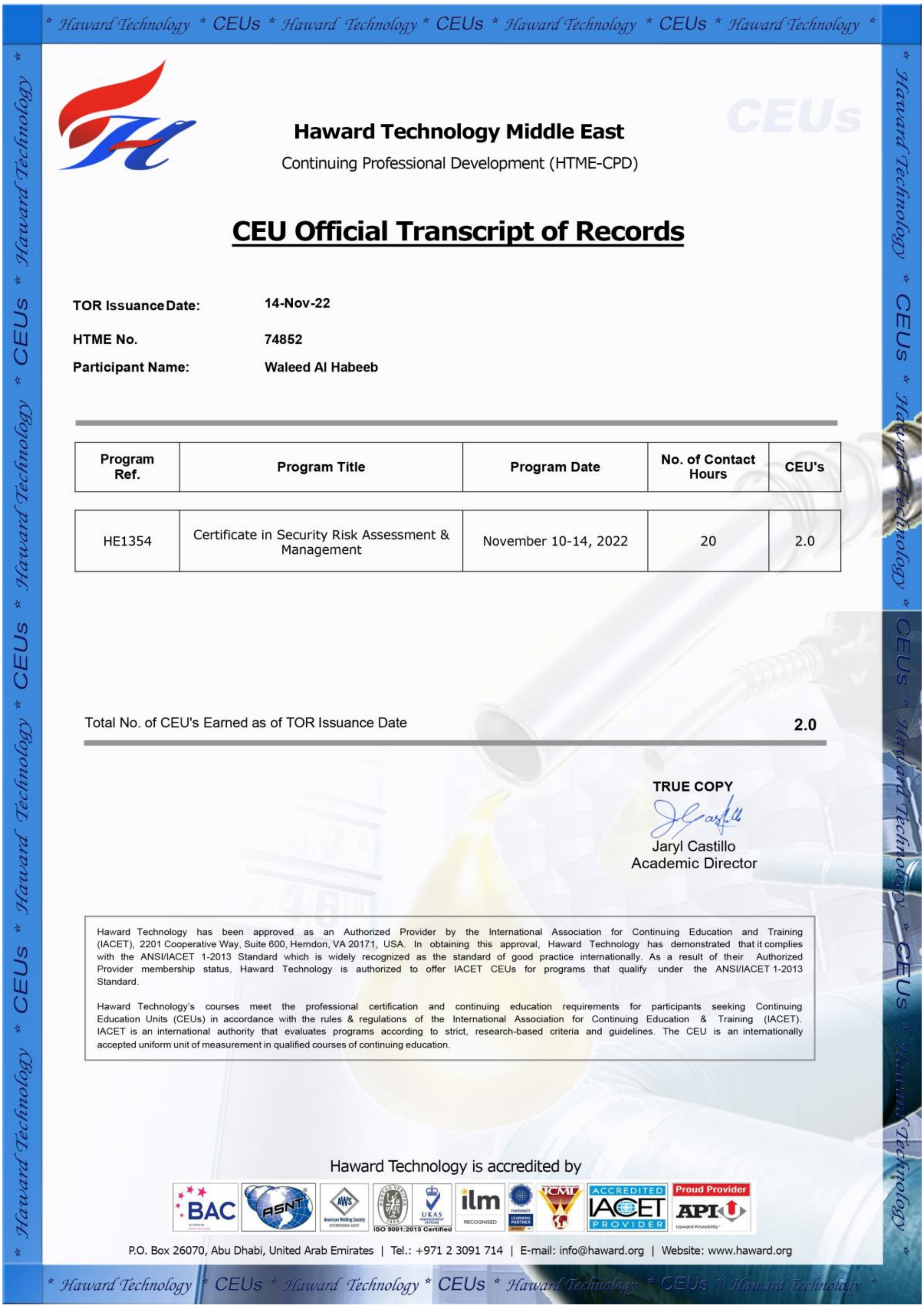
Certification Program

This program is designed to assist companies in identifying professionals who have satisfied the minimum competencies specified in HE1354.

Haward Technology does not warrant or guarantee the performance of any professional certified under this program.

Haward Technology is accredited by:

(2) Official Transcript of Records will be provided to the successful delegates with the equivalent number of ANSI/IACET accredited Continuing Education Units (CEUs) earned during the course



* Haward Technology * CEUs * Haward Technology * CEUs * Haward Technology * CEUs * Haward Technology *
CEUs

Haward Technology Middle East

Continuing Professional Development (HTME-CPD)

CEU Official Transcript of Records

TOR Issuance Date: **14-Nov-22**

HTME No. **74852**

Participant Name: **Waleed Al Habeeb**

Program Ref.	Program Title	Program Date	No. of Contact Hours	CEU's
HE1354	Certificate in Security Risk Assessment & Management	November 10-14, 2022	20	2.0

Total No. of CEU's Earned as of TOR Issuance Date **2.0**

TRUE COPY

Jaryl Castillo
Academic Director

Haward Technology has been approved as an Authorized Provider by the International Association for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this approval, Haward Technology has demonstrated that it complies with the ANSI/IACET 1-2013 Standard which is widely recognized as the standard of good practice internationally. As a result of their Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for programs that qualify under the ANSI/IACET 1-2013 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 Association 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 is accredited by

P.O. Box 26070, Abu Dhabi, United Arab Emirates | Tel.: +971 2 3091 714 | E-mail: info@haward.org | Website: www.haward.org

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 Fee

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 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:

General Ahmed Mady is a **Senior Security Consultant** and an **Expert** in **Intelligence**, **Strategic Planning**, **Terrorism**, **Security Management**, **Security Risk Assessment**, **Operating Access Control System**, **Security Operations Management** and **HSE Management** with over **40 years** of practical experience. He has consistently exemplified great skills in **Strategic Security** Management, **Security Risk** Management, **Security Threat** Identification, **Risk Analysis Evaluation** & Management, **Security Systems**, **Security Inteligence**, **Security Operations** Management, **Investigation & Security Surveying**, **Security Crisis** Management, **Corporate Security Planning**, **Strategic Analysis**, Strategy Selection & Implementation, **Security Policies & Procedures**, **Logistics Management**, **Systems Analysis & Design**, **Organization Procedure Evaluation & Auditing**, **Contracting & Systems Construction** and Maximo Managing Work & Foundation. Curently, he is the **Chief Information Directorate** of the **Ministry of Civil Aviation**.

During his service, he had been tasked as the **Chief Engineering Analyst**, **On-Scene Commander** (**OSC**) **& Incident Commander** (**IC**) in the **Air Force** and was responsible for a team of engineers supporting all engineering studies, modifications, aging studies and maintenance analysis. Being a **Board Member** of the **Aviation Information Technology Center**, he holds control of the overall strategies and procedures for the ministry, contracting for major IT projects, supervising all IS activities in the aviation sector and ensuring quality and success of delivery. He had likewise served as the **Commander** of the **Air Force** and had worked closely with the **Logistics Computer Center** wherein he gave out direction on **Operational & Tactical Logistics Planning** and **Strategic Military Logistics** to numerous high ranking officials, and at the same time **commanding flying Air Force maintenance squadron logistics field activities**. General Ahmed retired in the service as a **Major General**.

Earlier in his career, General Ahmed had occupied several challenging roles with several large Logistics companies as their **General Manager**, **Maintenance Engineer**, **Systems Analyst**, **Training Branch Chief**, **Systems & Communication Engineer**, **Computer Programmer** and **Logistic Instructor**. Further, he has travelled all over Europe, Asia and the Americas joining numerous conferences and workshops with the **Ministry of Foreign Affairs** and international companies such as **IBM**, **System Science Corporation** (**SSC**) and **International Air Transport Association** (**IATA**).

General Ahmed has a **Bachelor** degree in **Mechanical Engineering**. Further, he has gained **Diplomas** on **Civil Aviation Engineering**, **Islamic Studies** and **Information Systems & Technology**. Moreover, he is a **Certified Assessor** by **City & Guilds Level 4 Certificate** in **Leading the Internal Quality Assurance of Assessment Processes & Practice** and **Level 3 Certificate in Assessing Vocational Achievement** under the **TAQA Qualification** (**Training**, **Assessment & Quality Assurance**), a **Certified Internal Verifier Level 2 & 3 NVQ Processing Operations: Hydrocarbons** by **the British City & Guilds**, a **Certified Internal Verifier/Trainer/Assessor by the British Institute of Leadership & Management** (**ILM**) and a **Certified Instructor/Trainer**

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.

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: Sunday, 11th of February 2024

0730 – 0800	*Registration & Coffee*
0800 – 0815	*Welcome & Introduction*
0815 – 0830	***PRE-TEST***
0830 – 0930	***Introduction to Security Risk Assessment*** *Definition of Security Risk Assessment • Types of Security Risks • Purpose of Security Risk Assessment • Importance of Security Risk Assessment*
0930 – 0945	*Break*
0945 – 1100	***Threats & Vulnerabilities*** *Types of Threats • Common Vulnerabilities • Identification of Potential Threats • Assessment of Vulnerabilities*
1100 – 1230	***Risk Analysis*** *Risk Analysis Process • Risk Assessment Methodologies • Quantitative and Qualitative Risk Analysis • Risk Matrix and Scoring*
1230 – 1245	*Break*
1245 – 1420	***Threat Modeling*** *Definition of Threat Modeling • Types of Threat Modeling • Steps Involved in Threat Modeling • Examples of Threat Modeling Techniques*
1420 – 1430	***Recap*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow*
1430	*Lunch & End of Day One*

Day 2: Monday, 12th of February 2024

0730 – 0930	***Physical Security*** *Definition of Physical Security • Types of Physical Security Threats • Assessing Physical Security Risks • Mitigating Physical Security Risks*
0930 – 0945	*Break*
0945 – 1100	***Cybersecurity*** *Definition of Cybersecurity • Types of Cyber Threats • Assessing Cybersecurity Risks • Mitigating Cybersecurity Risks*
1100 – 1230	***Personnel Security*** *Definition of Personal Security • Types of Personnel Security Threats • Assessing Personal Security Risks • Mitigating Personnel Security Risks*

1230 – 1245	*Break*
1245 – 1420	***Security Risk Management*** *Definition of Security Risk Management • Elements of Security Risk Management • Risk Management Strategies • Developing a Security Risk Management Plan*
1420 – 1430	***Recap*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow*
1430	*Lunch & End of Day Two*

Day 3: Tuesday, 13th of February 2024

0730 – 0930	***Emergency Response Planning*** *Definition of Emergency Response Planning • Elements of Emergency Response Planning • Emergency Response Procedures • Developing an Emergency Response Plan*
0930 – 0945	*Break*
0945 – 1100	***Business Continuity Planning*** *Definition of Business Continuity Planning • Elements of Business Continuity Planning • Developing a Business Continuity Plan • Testing and Updating the Business Continuity Plan*
1100 – 1230	***Security Policies & Procedures*** *Definition of Security Policies & Procedures • Elements of Security Policies & Procedures • Developing Security Policies and Procedures • Implementing and Enforcing Security Policies and Procedures*
1230 – 1245	*Break*
1245 – 1420	***Compliance & Regulations*** *Compliance and Regulation Requirements • Developing a Compliance Program • Monitoring and Auditing Compliance*
1420 – 1430	***Recap*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow*
1430	*Lunch & End of Day Three*

Day 4: Wednesday, 14th of February 2024

0730 – 0930	***Security Risk Communication*** *Definition of Security Risk Communication • Communication Strategies • Stakeholder Management • Developing a Security Risk Communication Plan*
0930 – 0945	*Break*
0945 – 1100	***Risk Treatment*** *Definition of Risk Treatment • Risk Treatment Options • Implementing Risk Treatment Measures • Monitoring and Reviewing Risk Treatment Measures*
1100 – 1230	***Risk Assessment Tools & Techniques*** *Pros and Cons of Different Tools and Techniques • Selecting the Right Tool for the Job • Conducting a Risk Assessment Using Selected Tools and Techniques*

1230 – 1245	Break
1245 – 1420	***Threat Intelligence*** *Definition of Threat Intelligence • Gathering Threat Intelligence • Analyzing threat Intelligence • Utilizing Threat Intelligence*
1420 – 1430	***Recap*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Topics that were Discussed Today and Advise Them of the Topics to be Discussed Tomorrow*
1430	*Lunch & End of Day Four*

Day 5: Thursday, 15th of February 2024

0730 – 0930	***Security Awareness & Training*** *Definition of Security Awareness and Training • Elements of Security Awareness and Training*
0930 – 0945	*Break*
0945 – 1100	***Security Awareness & Training (cont'd)*** *Developing a Security Awareness Training Program • Implementing and Evaluating Security Awareness and Training Programs*
1100 – 1230	***Risk Reporting & Metrics*** *Definition of Risk Reporting and Metrics • Developing Risk Reporting and Metrics • Analyzing and Interpreting Risk Data • Using Risk Reporting and Metrics to Improve Security Risk Management*
1230 – 1245	*Break*
1245 – 1300	***Case Studies in Security Risk Assessment & Management*** *Review of Case Studies in Security Risk Assessment and Management • Analysis of Risk Management Strategies Used in Case Studies • Lessons Learned from Case Studies*
1300 – 1315	***Course Conclusion*** *Using this Course Overview, the Instructor(s) will Brief Participants about the Course Topics that were Covered During the Course*
1315 – 1415	***COMPETENCY EXAM***
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