

COURSE OVERVIEW DM0520
Physical Security Professional (PSP)
(ASIS-PSP Exam Preparation Training)

Course Title

Physical Security Professional (PSP):
(ASIS-PSP Exam Preparation Training)

Course Date/Venue

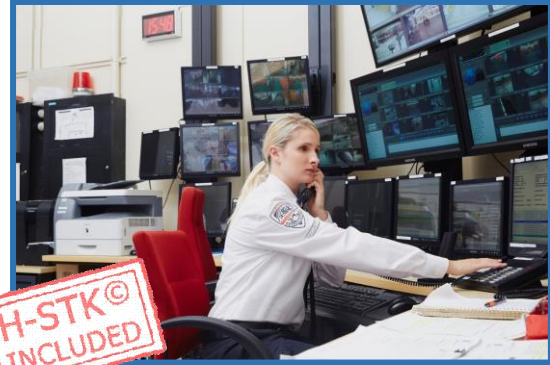
July 19-23, 2026/TBA Meeting Room, Royal
 Tulip Muscat, Muscat, Oman

Course Reference

DM0520

Course Duration/Credits

Five days/3.0 CEUs/30 PDHs



Course Description



This practical and highly-interactive course includes real-life case studies and exercises 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 physical security. It covers the physical security assessment plan; the assets to determine value, criticality and loss impact; the nature of the threats and hazards so that the risk can be determined; the assessment to identify and quantify vulnerabilities of the organization; performing risk analysis to develop countermeasures; the security program performance requirements; and the appropriate physical security countermeasures.



During this interactive course, participants will learn physical security systems and project documentation; the criteria for pre-bid meeting; the procurement plan for goods and services; and implementation of goods and services; the requirements for personnel involved in support of the security program; and monitoring and evaluating program throughout the system life cycle.

Course Objectives/Outcomes & Benefits for the Participants

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

- Get prepared for the next Physical Security Professional (PSP) exam and have enough knowledge and skills to pass such exam in order to get the certification from the American Society for Industrial Security (ASIS) International
- Develop a physical security assessment plan
- Identify assets to determine value, criticality and loss impact
- Assess the nature of the threats and hazards so that the risk can be determined
- Conduct an assessment to identify and quantify vulnerabilities of the organization
- Perform a risk analysis to develop countermeasures
- Establish security program performance requirements
- Determine appropriate physical security countermeasures
- Design physical security systems and project documentation
- Recognize criteria for pre-bid meeting
- Develop procurement plan for goods and services
- Manage implementation of goods and services
- Develop requirements for personnel involved in support of the security program
- Monitor and evaluate program throughout the system life cycle

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 physical security for those who are involved in the physical security of organizations. The course is very important for those who want to sit for ASIS-PSP examination.

Exam Eligibility & Structure

Candidates wishing to take the PSP examination must meet the following eligibility requirements:

Without higher education degree	Five (5) years of physical security experience* (or four years if you already hold an APP)
Master’s Degree or international equivalent	from an accredited institution of higher education and have three (3) years of physical security experience
Bachelor’s Degree or international equivalent	from an accredited institution of higher education and have four (4) years of physical security experience (or three years if you already hold an APP)

ASIS-PSP Certificate(s)

- (1) ASIS-PSP certificates will be issued to participants who successfully passed the ASIS-PSP exam.



- (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.

* Howard Technology * CEUs * Howard Technology * CEUs * Howard Technology * CEUs * Howard Technology *

CEUs

Howard Technology Middle East
Continuing Professional Development (HTME-CPD)

CEU Official Transcript of Records

TOR Issuance Date: 14-Nov-24
HTME No. 74851
Participant Name: Waleed Al Habeeb

Program Ref.	Program Title	Program Date	No. of Contact Hours	CEU's
DM0520	Physical Security Professional (PSP) (ASIS-PSP Exam Preparation Training)	Nov 10-14, 2024	30	3.0

Total No. of CEU's Earned as of TOR Issuance Date: **3.0**


TRUE COPY

Jaryll Castillo
Jaryll Castillo
Academic Director

Howard Technology has been approved as an Accredited Provider for the International Association for Continuing Education and Training (IACET), 2021 Cooperative Way, Suite 800, Herndon, VA 20171, USA. In obtaining this approval, Howard Technology has demonstrated that it complies with the standards and requirements of IACET. This approval is subject to annual review and renewal. Howard Technology is an IACET Accredited Provider. Provider membership status, Howard Technology is authorized to offer IACET CEUs for programs that qualify under the ANSI/IACET 1:2015 Standard.

Howard 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 internationally recognized organization that provides a standard for continuing education, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement for qualified courses of continuing education.

Howard Technology is accredited by



P.O. Box 26079, Abu Dhabi, United Arab Emirates | Tel.: +971 2 3091 714 | E-mail: info@haward.org | Website: www.haward.org

* Howard Technology * CEUs * Howard Technology * CEUs * Howard Technology * CEUs * Howard Technology *

Certificate Accreditations

Haward's certificates are accredited by the following international accreditation organizations: -

- 

British Accreditation Council (BAC)

Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. Haward's certificates are internationally recognized and accredited by the British Accreditation Council (BAC). 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.

- 

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.

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:



Lieutenant Colonel Nayel Sarayreh is a Senior Security Expert in Defence, Security & Military Management with over 30 years of extensive experience in Accident/Incident Investigation & Root Cause Analysis, Strategic Security Management, Security Risk Management, Security Threat Identification, Risk Analysis Evaluation & Management, Security Systems, Security Intelligence, Security Operations Management, Investigation & Security Surveying, Security Crisis Management, Security Investigations & Criminal Evidence, Incident Investigation Techniques, Incident Root Cause Analysis, Root Cause Failure Analysis, Effective Investigations, Administrative Investigations, Emergency Response & Preparedness, Disaster Management Strategies, Emergency Management Skills, Disaster Mitigation & Recovery, Emergency Communication & Response, Corporate Security Planning, Safety Protocols & Security Measures, Disaster Recovery, Crisis Management, Risk Management, Risk Analysis Evaluation & Management, Investigation & Security Surveying, Security Crisis Management, Corporate Security Planning, Advanced Security, Strategic Analysis, Systems Analysis & Design, Strategy Selection & Implementation, Security Policies & Procedures, Violence, Terrorism & Security, Counterterrorism, Civil Conflict, Anti-riot & Riot Control, Rehabilitation & Correction, Corporate Legal Advising, Law, Mediation, Arbitration, Litigation & Legal Risk, Investigation, Prosecution & Execution and Human Rights Etiquette & Protocol.

During his service, Lieutenant Colonel Nayel had been served as the **General Prosecutor, Chief of Judicial Section, Chief of Security, Commander, Deputy Commander, Police Advisor, Civil Defense Officer, Police Officer, Intelligence Officer, Crisis Communication & Emergency Response Specialist, Internal Investigator, Security Specialist, Rehabilitation & Correction Officer, Investigation Officer, Security Expert, Security Management Consultant and Senior Instructor/Trainer** from the various international organizations such as the United Nations, UNHCR, Jordan Police and Diplomatic Security Unit which is responsible of all embassies, ambassadors and residences, just to name a few.

Lieutenant Colonel Nayel has a **Bachelor's** degree in **Law**. Further, he is a **Certified Instructor/Trainer**, a **Certified Trainer/Assessor** by the **Institute of Leadership & Management (ILM)** and has delivered numerous trainings, workshops and conferences and projects worldwide.

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.

Learning Design & Customization

This course can be customized to the exact requirements of clients. Haward Technology is so proud of our huge capabilities in tailoring our courses to the training needs of our valued clients.

Accommodation

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

Training 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.

Exam Fee

US\$ 1,215 per Delegate + **VAT**.

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, 19th of July 2026

0730 – 0800	Registration & Coffee
0800 – 0815	Welcome & Introduction
0815 – 0830	PRE-TEST
0830 – 0930	Physical Security Assessment: Develop a Physical Security Assessment Plan Key Area or Critical Asset Identification • Risk Assessment Models & Considerations (e.g., Inside-out, Outside-inward, Site-specific Risk Assessment, Functional Approach) • Qualitative & Quantitative Assessment Methods • Types of Resources & Guidelines Needed for the Assessment (e.g., Stakeholders, Budget, Equipment, Policies, Standards)

0930 – 0945	Break
0945 – 1100	Physical Security Assessment: Identify Assets to Determine their Value, Criticality & Loss Impact Definitions & Terminology Related to Assets, Value, Loss Impact, & Criticality • The Nature & Types of Assets (Tangible & Intangible) • How to Determine Value for Various Types of Assets & Business Operations
1100 - 1230	Physical Security Assessment: Assess the Nature of the Threats & Hazards so that the Risk can be Determined The Nature, Types, Severity, & Likelihood of Threats & Hazards (e.g., Natural Disasters, Cyber, Criminal Events, Terrorism, Socio-Political, Cultural) • Operating Environment (e.g., Geography, Socioeconomic Environment, Criminal Activity, Existing Security Countermeasures, Security Risk Level)
1230 – 1245	Break
1245 - 1420	Physical Security Assessment: Assess the Nature of the Threats & Hazards so that the Risk can be Determined (cont'd) Potential Impact of External Organizations (e.g., Competitors, Organizations in Immediate Proximity) on Facility's Security Program • Other Internal & External Factors (e.g., Legal, Loss of Reputation, Economic, Supply Chain) & their Impact on the Facility's Security Program
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, 20th of July 2026

0730 – 0930	Physical Security Assessment: Conduct an Assessment to Identify & Quantify Vulnerabilities of the Organization Relevant Data & Methods for Collection (e.g., Security Survey, Interviews, Past Incident Reports, Crime Statistics, Personnel Issues, Issues Experienced by other Similar Organizations)
0930 – 0945	Break
0945 – 1100	Physical Security Assessment Plan: Conduct an Assessment to Identify & Quantify Vulnerabilities of the Organization (cont'd) Effectiveness of Current Security Technologies/Equipment, Personnel & Procedures • Interpretation of Building Plans, Drawings & Schematics • Applicable Standards/Regulations/Codes & Where to Find Them • Environmental Factors & Conditions (e.g., Facility Location, Architectural Barriers, Lighting, Entrances) that Impact Physical Security
1100 - 1230	Physical Security Assessment: Perform a Risk Analysis to Develop Countermeasures Risk Analysis Strategies & Methods • Risk Management Principles • Analysis & Interpretation of Collected Data • Threat/Hazard & Vulnerability Identification • Loss Event Profile Analyses (e.g., Consequences)
1230 – 1245	Break

1245 – 1420	<p>Physical Security Assessment: Perform a Risk Analysis to Develop Countermeasures (cont'd) <i>Appropriate Countermeasures Related to Specific Risks • Cost Benefit Analysis (e.g. Return on Investment (ROI) Analysis, Total Cost of Ownership) • Legal & Regulatory Considerations Related to Various Countermeasures/Security Applications (e.g., Video Surveillance, Privacy Issues, Personally Identifiable Information, Life Safety)</i></p>
1420 – 1430	<p>Recap <i>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</i></p>
1430	<p><i>Lunch & End of Day Two</i></p>

Day 3: Tuesday, 21st of July 2026

0730 – 0930	<p>Application, Design & Integration of Physical Security Systems: Establish Security Program Performance Requirements <i>Design Constraints (e.g. Regulations, Budget, Materials, System Compatibility) • Incorporation of Risk Analysis Results in Design • Relevant Security Terminology (e.g., Punch List, Field Test) • Relevant Security Concepts (e.g., CPTED, Defense-in-depth, the 4 Ds- deter, Detect, Delay, Deny) • Applicable Codes, Standards & Guidelines • Operational Requirements (e.g., Policies, Procedures, Staffing) • Functional Requirements (e.g., System Capabilities, Features, Fault Tolerance) • Performance Requirements (e.g., Technical Capability, Systems Design Capacities) • Success Metrics</i></p>
0930 – 0945	<p><i>Break</i></p>
0945 – 1100	<p>Application, Design & Integration of Physical Security Systems: Determine Appropriate Physical Security Countermeasures <i>Structural Security Measures (e.g., Barriers, Lighting, Locks, Blast Mitigation, Ballistic Protection) • Crime Prevention Through Environmental Design (CPTED) • Electronic Security Systems (e.g., Access Control, Video Surveillance, Intrusion Detection)</i></p>
1100 – 1230	<p>Application, Design & Integration of Physical Security Systems: Determine Appropriate Physical Security Countermeasures (cont'd) <i>Security Staffing (e.g., Officers, Technicians, Management, Administration) • Personnel, Package, & Vehicle Screening • Emergency Notification Systems (e.g., Mass Notifications, Public Address, Two-way Intercom) • Principles of Data Storage & Management (e.g., Cloud, On-premise, Redundancy, Retention, User Permissions, Personally Identifiable Information, Regulatory Requirements) • Principles of Network Infrastructure & Physical Network Security (e.g., Token Ring, LAN/WAN, VPN, DHCP vs. Static, TCP/IP) • Security Audio Communications (e.g., Radio, Telephone, Intercom, IP Audio)</i></p>
1230 – 1245	<p><i>Break</i></p>



1245 – 1420	Application, Design & Integration of Physical Security Systems: Determine Appropriate Physical Security Countermeasures (cont'd) Systems Monitoring & Display (Control Centers/Consoles, Central Monitoring Station) • Primary & Backup Power Sources (e.g., Grid, Battery, UPS, Generators, Alternative/Renewable) • Signal & Data Transmission Methods (e.g., Copper, Fiber, Wireless) • Visitor & Vendor Management Policies
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, 22nd of July 2026

0730 – 0930	Application, Design & Integration of Physical Security Systems: Design Physical Security Systems & Project Documentation Design Phases (e.g., Pre-Design, Schematic Development, Construction Documentation) • Design Elements (e.g., Calculations, Drawings, Specifications, Review, Technical Data) • Construction Specification Standards (e.g., Constructions Specifications Institute, Owner's Equipment Standards, American Institute of Architects (AIA) MasterSpec)
0930 – 0945	Break
0945 – 1100	Application, Design & Integration of Physical Security Systems: Design Physical Security Systems & Project Documentation (cont'd) Systems Integration • Project Management Concepts • Scheduling (e.g., Gantt Charts, PERT Charts, Milestones, Objectives) • Cost Estimation & Cost-Benefit Analysis of Design Options (e.g., Value Engineering)
1100 - 1230	Implementation of Physical Security Measures: Outline Criteria for Pre-Bid Meeting Bid Process (e.g., Site Visits, RFI, Substitution Requests, Pre-bid Meeting • Bid Package Types (e.g., RFP, RFQ, IFB, Sole Source) • Bid Package Components (e.g., Project Timelines, Costs, Personnel, Documentation, Scope of Work) • Criteria for Evaluation of Bids (e.g., Cost, Experience, Scheduling, Certification, Resources) • Technical Compliance Criteria • Ethics in Contracting
1230 – 1245	Break
1245 – 1420	Implementation of Physical Security Measures: Develop Procurement Plan for Goods & Services Vendor Evaluation & Selection (e.g., Interviews, Due Diligence, Reference Checks) • Project Management Functions & Processes • Procurement Process
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, 23rd of July 2026

0730 – 0900	Implementation of Physical Security Measures: Manage Implementation of Goods & Services Installation & Inspection Techniques • Systems Integrations • Commissioning • Installation Problem Resolution (e.g., Punch Lists) • Systems Configuration Management (e.g., As-built Drawings) • Final Acceptance Testing Criteria (e.g., System Acceptance Testing, Factory Acceptance Testing) • End-User Training Requirements
0900 – 0915	Break
0915 – 1100	Implementation of Physical Security Measures: Develop Requirements for Personnel Involved in Support of the Security Program Roles, Responsibilities & Limitations of Security Personnel (Including Proprietary (In-House) & Contract Security Staff) • Human Resource Management (e.g., Establishing KPIs, Performance Review, Improvement Processes, Recruiting, Onboarding, Progressive Discipline)
1100 – 1200	Implementation of Physical Security Measures: Develop Requirements for Personnel Involved in Support of the Security Program (cont'd) Security Personnel Professional Development (e.g., Training, Certification) • General, Post & Special Orders • Security Personnel Uniforms & Equipment • Security Awareness Training & Education for Non-Security Personnel
1200 – 1215	Break
1215 - 1345	Implementation of Physical Security Measures: Monitor & Evaluate Program throughout the System Life Cycle Maintenance of Systems & Hardware (e.g., Preventative, Corrective, Upgrades, Calibration, Service Agreements) • Warranty Types (e.g., Manufacturer, Installation, Replacement Parts, Extended) • Ongoing System Training (e.g., System Upgrades, Manufacturer's Certification) • System Evaluation & Replacement Process
1345 – 1400	Course Conclusion Using this Course Overview, the Instructor(s) will Brief Participants about the Course Topics that were Covered During the Course
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 60 days following the course completion. Each participant has only one trial for the MOCK exam within this 60-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