



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

December 14-18, 2026/Glasshouse Meeting Room, Grand Millennium Al Wahda Hotel, Abu Dhabi, UAE

Course Reference

DM0520

Course Duration/Credits

Five days/3.0 CEUs/30 PDHs

Course Description



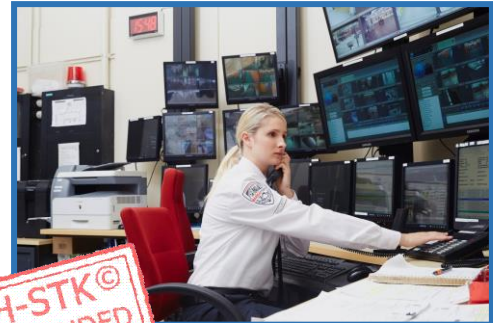
This practical and highly-interactive course includes real-life case studies and exercises where participants will be engaged in a series of interactive small groups and class workshops.



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 ASIS-PSP exam and have enough knowledge and skills to pass such exam
- Apply and gain an in-depth knowledge on physical security
- 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 years of physical security experience* (or four years if you already hold an APP)
With higher education degree: • Master’s Degree or international equivalent • Bachelor’s Degree or international equivalent	from an accredited institution of higher education and have three years of physical security experience
	from an accredited institution of higher education and have four 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.

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

TRUE COPY
Jaryl Castillo
Academic Director

Haward Technology has been approved as an Accredited Provider for Continuing Education and Training by the International Association for Continuing Education and Training (IACET). All courses offered by Haward Technology are designed to meet the standards of good practice internationally, as measured by their Accredited Provider membership status. Haward Technology is authorized to offer IACET CEU's for programs that qualify under the ANSI/IACET 1-2016 Standard.

Haward Technology's courses meet the professional certification and continuing education requirements for participants seeking Continuing Education Units (CEU's) for their professional development. The CEU is an internationally accepted unit of measurement in qualified courses of continuing education.

Haward Technology is accredited by:

BAC, IACET, ISO 9001:2015, UKAS, TCM, BOTS

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

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:



Mr. Pan Kosmidis, MSc, BSc, is a **Senior Security Consultant** with almost **25** years of experience in the areas of Programming with **Security Risk Management, Strategic Planning, Terrorism, Security Management, Security Risk Assessment, Physical Asset Protection, API 780 standards, HCIS New Security Directives & Process, Risk-Based Screening, Threat & Vulnerability Assessments, Residual Risks Calculation, Countermeasure Risk Scores Development, Advanced Intrusion Detection Systems, Perimeter & Building Barriers Design, Intellectual Property Protection, Interdependency & External Infrastructure Security, Quantitative Risk Assessments, Risk Registers Maintenance, Security Situation Reporting, Operating Access Control System, Security Operations Management, Security Investigations & Criminal Evidence, Security Risk Assessment, Supervising Security Operation Team, Industrial Security & Asset Protection, Security Threat Identification, Risk Analysis & Evaluation, Security Planning & Design, Security Policy Development, Integrated Security Systems Management, Safety & Loss Prevention, Security Engineering & Emergency Management Planning, Security Incident Management, Information Security & Confidentiality Management, Security Crisis Management, Strategic Security Management, Security Report Writing, Security Detection Systems & Operation, Security Surveying & Design, Emergency Response Planning, Emergency Management, HSE Risk Identification. Further he is also well versed in AI Fundamentals, Effective & Interactive Dashboards, Predictive Analytics Concepts, Apply AI Algorithms, AI-Driven Predictive Maintenance, Data Storytelling with AI Insights, Integrating Real-Time Data Ingestion, and Software Tools such as Python, Java, JavaScript/TypeScript, C#/.NET, PHP/Laravel, Node.js, HTML/CSS, SQL (RDBMS & NoSQL), Redis, RabbitMQ, Kafka, Event Store, Docker, CI/CD, Git and Methodologies & Architecture such as Agile (Scrum, Kanban), DDD, CQRS, Clean Architecture, Event Sourcing, SOLID, RESTful APIs and CI/CD Pipelines. Further, he is also well-versed in Business Management, Financial Marketing, Contract Negotiation, Crisis Management, Training Programme Design & Delivery, Project Management, Business & Team Leadership, Financial Analysis, Investment & Risk Management, Technical & Fundamental Analysis, Mentoring and Consultancy.**

During his career life, Mr. Kosmidis has gained his practical and field experience through his various significant positions and dedication as the **Business Development Operations Director, Enterprise Architect, IT Consultant, Educational Consultant & Instructor, Investment Analyst & Trader, University Lecturer, DevOps Engineer, Security & Crisis Management Instructor, Site Security Officer & Executive Protection, Multiple International Security Training Organisations Instructor, Emergency Response & Civil Protection, IT Specialist, Software Developer and Senior Instructor/Trainer/Lecturer** from various companies and universities.

Mr. Kosmidis is currently taking up his **Master's** degree in **Data Analytics and Financial Technology** and he holds a **Bachelor's** degree with (Honours) in **Computer Science** and a **Bachelor's** degree in **Business Administration & Economics**. Further, he is a **Certified Instructor/Trainer** and has delivered numerous trainings, courses, workshops, conferences and seminars internationally.

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**.

Training Methodology

Our courses employ an interactive, learner-centred methodology that integrates theoretical knowledge with practical application. The training is delivered through a suitable combination of some or all of the following methods, selected according to the course content and learning objectives:

- Instructor-led presentations and facilitated discussions
- Practical workshops and participant presentations
- Hands-on exercises and real-world case studies
- Equipment demonstrations and technical drawings
- Hardware- and software-based simulations
- Gamification & Role Play in soft-skills courses only
- Virtual Reality (VR) and Augmented Reality (AR)
- Instructional videos and other relevant training resources

This blended approach encourages active participation, strengthens practical skills and supports the effective application of acquired knowledge in the workplace.

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.

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, 14th of December 2026*

0900 – 0930	<i>Registration & Coffee</i>
0930 – 0945	<i>Welcome & Introduction</i>
0945 – 1000	PRE-TEST
1000 – 1130	<i>Physical Security Assessment: Develop a Physical Security Assessment Plan</i> <i>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)</i>

1130 - 1145	Break
1145 - 1300	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
1300 - 1400	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)
1400 - 1415	Break
1415 - 1550	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
1550 - 1600	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
1600	Lunch & End of Day One

Day 2: Tuesday, 15th of December 2026

0900 - 1130	Physical Security Assessment: Conduct an Assessment to Identify & Quantify Vulnerabilities of the Organization Relevant Data & Methods for Collection (e.g., Security Survey, Interviews, Incident Reports, Crime Statistics, Personnel Issues, Benchmarking)
1130 - 1145	Break
1145 - 1300	Physical Security Assessment Plan: Conduct an Assessment to Identify & Quantify Vulnerabilities of the Organization (cont'd) Effectiveness of Current Security Technologies/Equipment, Personnel & Procedures • Evaluation 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
1300 - 1400	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)
1400 - 1415	Break

1415 - 1550	Physical Security Assessment: Perform a Risk Analysis to Develop Countermeasures (cont'd) Appropriate Countermeasures Related to Specific Risks • Cost Benefit Analysis (e.g. Return on Investment (ROI), Total Cost of Ownership) • Legal & Regulatory Considerations Related to Various Countermeasures/Security Applications (e.g., Video Surveillance, Privacy Issues, Personally Identifiable Information, Life Safety)
1550 - 1600	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
1600	Lunch & End of Day Two

Day 3: Wednesday, 16th of December 2026

0900 - 1130	Application, Design & Integration of Physical Security Systems: Establish Security Program Performance Requirements 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
1130 - 1145	Break
1145 - 1300	Application, Design & Integration of Physical Security Systems: Determine Appropriate Physical Security Countermeasures 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)
1300 - 1400	Application, Design & Integration of Physical Security Systems: Determine Appropriate Physical Security Countermeasures (cont'd) 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)
1400 - 1415	Break

1415 - 1550	Application, Design & Integration of Physical Security Systems: Determine Appropriate Physical Security Countermeasures (cont'd) Systems Monitoring & Display (e.g., 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
1550 - 1600	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
1600	Lunch & End of Day Three

Day 4: Thursday, 17th of December 2026

0900 - 1130	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)
1130 - 1145	Break
1145 - 1300	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)
1300 - 1400	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
1400 - 1415	Break
1415 - 1550	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
1550 - 1600	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
1600	Lunch & End of Day Four

Day 5: Friday, 18th of December 2026

0900 - 1130	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
1130 - 1145	Break
1145 - 1300	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)
1300 - 1400	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
1400 - 1415	Break
1415 - 1515	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
1515 - 1530	Course Conclusion Using this Course Overview, the Instructor(s) will Brief Participants about the Course Topics that were Covered During the Course
1530 - 1545	POST-TEST
1545 - 1600	Presentation of Course Certificates
1600	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