



**COURSE OVERVIEW IT0018**  
**Certified Information System Security Professional (CISSP)**  
*(ISC-CISSP Exam Preparatory Training)*

**Course Title**

Certified Information System Security Professional (CISSP) – (ISC-CISSP Exam Preparatory Training)

**Course Date/Venue**

Session 1: July 14-18, 2025/Fujairah Meeting Room, Grand Millennium Al Wahda Hotel, Abu Dhabi, UAE

Session 2: October 26-30, 2023/Boardroom 1, Elite Byblos Hotel Al Barsha, Sheikh Zayed Road, Dubai, UAE

**Course Reference**

IE0909

**Course Duration/Credits**

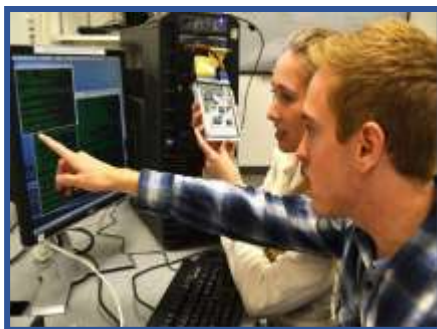
Five days/3.0 CEUs/30 PDHs



**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 certified information system security professional (CISSP). It covers the security and risk management and professional ethics; the security concepts and security governance principles; the compliance, other requirements and legal and regulatory issues that pertain to information security in a holistic context; the requirements for investigation types; develop, document, and implement security policy, standards, procedures and guidelines; the business continuity (BC) requirements; the personnel security policies and procedures; and risk management concepts and threat modeling concepts; and the methodologies and supply chain risk management (SCRM) concepts.



Further, the course will also discuss the security awareness, education and training program; the information and assets, establishing information and asset handling requirements; managing data lifecycle; the appropriate asset retention and data security controls and compliance requirements; the security architecture and engineering; researching, implementing and managing engineering processes using secure design principles; and the cryptographic solutions and security principles to site and facility.





During this interactive course participants will learn the design principles in network architectures, secure network components and secure communication channels according to design; identifying and accessing management, controlling physical and logical access to assets and managing identification and authentication; the authorization mechanisms and authentication systems; designing and validating assessment, test, and audit strategies; conducting security control testing and collecting security process data; testing output and generating report; conducting or facilitating security audits and complying with investigations; logging and monitoring activities and configuration management; the foundational security operations concepts, resource protection and incident management; operating and maintaining detective and preventative measures; the change management, recovery strategies and disaster recovery process; testing disaster recovery plans, participating in business continuity planning, managing physical security and addressing personnel safety and security concerns; and the software development security, security control and coding guidelines and standards.

### **Course Objectives**

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

- Get prepared for the next ISC-CISSP Exam and have enough knowledge and skills to pass such exam in order to get the Certified Information System Security Professional (CISSP) from the international information system security certification consortium (ISC)<sup>2</sup>
- Apply security and risk management and discuss adhere to and promote professional ethics
- Apply security concepts and evaluate security governance principles
- Determine compliance and other requirements as well as identify legal and regulatory issues that pertain to information security in a holistic context
- Recognize the requirements for investigation types and develop, document, and implement security policy, standards, procedures and guidelines
- Identify, analyze, and prioritize business continuity (BC) requirements
- Contribute and enforce personnel security policies and procedures
- Apply risk management concepts, threat modeling concepts and methodologies and supply chain risk management (SCRM) concepts
- Establish and maintain a security awareness, education and training program
- Identify and classify information and assets, establish information and asset handling requirements and manage data lifecycle
- Ensure appropriate asset retention and determine data security controls and compliance requirements
- Discuss security architecture and engineering as well as research, implement and manage engineering processes using secure design principles
- Select cryptographic solutions and apply security principles to site and facility
- Assess and implement secure design principles in network architectures, secure network components and implement secure communication channels according to design
- Identify and access management, control physical and logical access to assets, manage identification and authentication





- Implement and manage authorization mechanisms and authentication systems
- Design and validate assessment, test, and audit strategies, conduct security control testing and collect security process data
- Analyse test output and generate report, conduct or facilitate security audits and comply with investigations
- Conduct logging and monitoring activities and perform configuration management
- Apply foundational security operations concepts, resource protection and incident management
- Operate and maintain detective and preventative measures and apply change management, recovery strategies and disaster recovery process
- Test disaster recovery plans, participate in business continuity planning, manage physical security and address personnel safety and security concerns
- Carryout software development security, security control and coding guidelines and standards

### **Exclusive Smart Training Kit - H-STK®**



Participants of this course will receive the exclusive “Howard 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 security CISSP for all chief information security officers, directors of security, security system engineers, security managers, security architects, network architects, chief information officers, IT directors/managers, security analysts, security auditors and security consultants.

### **Exam Eligibility & Structure**

To apply for the CISSP course certification, you need to:

- Have a minimum 5 years of cumulative paid full time work experience in two or more of the 8 domains of the (ISC)<sup>2</sup> CISSP common body of knowledge (CBK)
- One-year experience waiver can be earned with a 4-year college degree, or regional equivalent or additional credentials from the (ISC)<sup>2</sup> approved list

### **Course Fee**

**US\$ 5,500** per Delegate + **VAT**. This rate includes H-STK® (Howard 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: -

-  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.

-  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:



**Dr. Peter Lalos, PhD, MSc, BSc, is a Senior IT, Telecommunications, Control & Electronics Engineer with over 20 years of extensive experience in the areas of Information & Technology Architectures, Application Architecture, Logical Applications, Interfaces & Services, Logical & Physical Components, Portfolio Management, Application Security, Application Integration Technologies & Strategies, Solution Architecture Patterns, Web Applications & Services, Mobile & Cloud**

**Applications, Blended Learning Programs, Web Programming, E-Commerce Strategies, Advanced Database Management Systems, Web Design, HCI, 3D Animation, Multimedia Design, Gamification Techniques, Internal & External Auditing, OS Architectures and Network Security.** Further, he is also well-versed in ACAD, ASP, PHP, JSP, MS Visual Studio, VB.NET, ASP.NET, Moodle administration, Design & Development, WAMP & LAMP, Oracle JDeveloper, Oracle 11g, PL/SQL, MS SQL Server, MySQL, MS Access, HTML5, CSS, XML, XSD/ XSL, JavaScript, Ajax, Angular, jQuery, Web Services Adobe Suite, MS Office 2013, IIS Servers, MS Exchange Server & Apache Tomcat, Open Source CMS Expert (Xaraya, Joomla, Mambo) & Module Development, Open Source E-commerce Expert (oscommerce, Joomla & Virtuemart) and Module Development. Currently, he is the **IT Instructor & Subject Matter Expert** of the **University of Liverpool, UK**, wherein he instructs online courses in **Information Systems Program**.

During his career life, Dr. Peter has gained his practical and field experience through his various significant positions and dedication as the **Manager, Bid Manager, Project Manager, IT Trainer, IT Contractor, IT Professor, Lecturer/Trainer, Physics Instructor, Consultant, E-Learning Specialist, E-Learning Instructional Designer, Scientific Advisor, Laboratory Assistant, Laboratory Administrator, LMS Specialist and Moodle Expert & Administrator** for various companies and universities such as **E-Learning Software House Chemmedia Hellas Ltd, University of Greenwich, Empire State College, Roehampton University, University of East London, Athens Technology Center, University of Athens, ShellGas, Advanced Services Group (ASG), Piraeus University and Media Company.**

Dr. Peter has a **PhD** in **IT, Telecommunications, Control & Electronic** from the **University of Athens**, a **Master's degree** in **Information Technology with Web Technology** from the **University of Paisley, UK** and a **Bachelor's degree** in **Physics** from the **University of Thessaloniki, Greece**. Further, he is a **Certified Instructor/Trainer**, a **SABA Certified Administrator** and an **IBM Lotus Learning Space Certified Administrator**. He has further conducted numerous trainings, workshops, seminars, conferences, published several journals and participated as an author in various projects.



**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**

0730 – 0800	Registration & Coffee
0800 – 0815	Welcome & Introduction
0815 – 0830	<b>PRE-TEST</b>
0830 – 0930	<b>Security &amp; Risk Management</b> Understand, Adhere to, & Promote Professional Ethics ((ISC) <sup>2</sup> Code of Professional Ethics, Organizational Code of Ethics) • Understand & Apply Security Concepts (Confidentiality, Integrity, & Availability, Authenticity & Nonrepudiation) • Evaluate & Apply Security Governance Principles (Alignment of the Security Function to Business Strategy, Goals, Mission, & Objectives, Organizational Processes (e.g., Acquisitions, Divestitures, Governance Committees), Organizational Roles & Responsibilities, Security Control Frameworks, Due Care/Due Diligence)
0930 - 0945	Break
0945 – 1100	<b>Security &amp; Risk Management (cont'd)</b> Determine Compliance & Other Requirements (Contractual, Legal, Industry Standards, & Regulatory Requirements, Privacy Requirements) • Understand Legal & Regulatory Issues that Pertain to Information Security in a Holistic Context (Cybercrimes & Data Breaches, Licensing & Intellectual Property (IP) Requirements, Import/Export Controls, Transborder Data Flow, Privacy • Understand Requirements for Investigation Types (I.E., Administrative, Criminal, Civil, Regulatory, Industry Standards) • Develop, Document, & Implement Security Policy, Standards, Procedures, & Guidelines • Identify, Analyze, & Prioritize Business Continuity (BC) Requirements (Business Impact Analysis (BIA), Develop & Document the Scope & the Plan) • Contribute to & Enforce Personnel Security Policies & Procedures (Candidate Screening & Hiring, Employment Agreements & Policies, Onboarding, Transfers, & Termination Processes, Vendor, Consultant, & Contractor Agreements & Controls, Compliance Policy Requirements, Privacy Policy Requirements)





1100 – 1230	<p><b>Security &amp; Risk Management (cont'd)</b>            Understand &amp; Apply Risk Management Concepts (Identify Threats &amp; Vulnerabilities, Risk Assessment/Analysis, Risk Response, Countermeasure Selection &amp; Implementation, Applicable Types of Controls (e.g., Preventive, Detective, Corrective), Control Assessments (Security &amp; Privacy), Monitoring &amp; Measurement, Reporting, Continuous Improvement (e.g., Risk Maturity Modeling), Risk Frameworks) • Understand &amp; Apply Threat Modeling Concepts &amp; Methodologies • Apply Supply Chain Risk Management (SCRM) Concepts (Risks Associated With Hardware, Software, &amp; Services, Third-Party Assessment And Monitoring, Minimum Security Requirements, Service Level Requirements) • Establish &amp; Maintain a Security Awareness, Education, &amp; Training Program (Methods &amp; Techniques to Present Awareness &amp; Training (e.g., Social Engineering, Phishing, Security Champions, Gamification), Periodic Content Reviews, Program effectiveness evaluation)</p>
1230 – 1245	Break
1245 - 1420	<p><b>Asset Security</b>            Identify &amp; Classify Information &amp; Assets (Data Classification, Asset Classification) • Establish Information &amp; Asset Handling Requirements • Provision Resources Securely (Information &amp; Asset Ownership, Asset Inventory (e.g., Tangible, Intangible), Asset Management)</p>
1420 - 1430	<b>Recap</b>
1430	Lunch & End of Day One

**Day 2**

0730 – 0830	<p><b>Asset Security (cont'd)</b>            Manage Data Lifecycle (Data Roles (i.e., Owners, Controllers, Custodians, Processors, Users/Subjects), Data Collection, Data Location, Data Maintenance, Data Retention, Data Remanence, Data Destruction) • Ensure Appropriate Asset Retention (e.g., End-of-Life (EOL), End-of-Support (EOS)) • Determine Data Security Controls &amp; Compliance Requirements (Data States (e.g., in use, in Transit, at Rest), Scoping &amp; Tailoring, Standards Selection, Data Protection Methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))</p>
0830 - 0930	<p><b>Security Architecture &amp; Engineering</b>            Research, Implement &amp; Manage Engineering Processes Using Secure Design Principles (Threat Modeling, Least Privilege, Defense in Depth, Secure Defaults, Fail Securely, Separation of Duties (Sod), Keep it Simple, Zero Trust, Privacy By Design, Trust but Verify, Shared Responsibility) • Understand the Fundamental Concepts of Security Models (e.g., Biba, Star Model, Bell-Lapadula) • Select Controls Based Upon Systems Security Requirements • Understand Security Capabilities of Information Systems (IS) (e.g., Memory Protection, Trusted Platform Module (TPM), Encryption/Decryption)</p>
0930 - 0945	Break



0945 - 1200	<p><b>Security Architecture &amp; Engineering (cont'd)</b>            Assess &amp; Mitigate the Vulnerabilities of Security Architectures, Designs, &amp; Solution Elements (Client-Based Systems, Server-Based Systems, Database Systems, Cryptographic Systems, Industrial Control Systems (ICS), Cloud-Based Systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform As A Service (PaaS)), Distributed Systems, Internet of Things (IoT), Microservices, Containerization, Serverless, Embedded Systems, High-Performance Computing (HPC) Systems, Edge Computing Systems, Virtualized Systems) • Select &amp; Determine Cryptographic Solutions (Cryptographic Life Cycle (e.g., Keys, Algorithm Selection), Cryptographic Methods (e.g., Symmetric, Asymmetric, Elliptic Curves, Quantum), Public Key Infrastructure (PKI), Key Management Practices, Digital Signatures &amp; Digital Certificates, Non-Repudiation, Integrity (e.g., Hashing)) • Understand Methods of Cryptanalytic Attacks (Brute Force, Ciphertext Only, Known Plaintext, Frequency Analysis, Chosen Ciphertext, Implementation Attacks, Side-Channel, Fault Injection, Timing, Man-In-The-Middle (MITM), Pass the Hash, Kerberos Exploitation, Ransomware) • Apply Security Principles to Site &amp; Facility Design • Design Site &amp; Facility Security Controls (Wiring Closets/Intermediate Distribution Facilities, Server Rooms/Data Centers, Media Storage Facilities, Evidence Storage, Restricted &amp; Work Area Security, Utilities &amp; Heating, Ventilation, &amp; Air Conditioning (HVAC), Environmental Issues, Fire Prevention, Detection, &amp; Suppression, Power (e.g., Redundant, Backup))</p>
1200 - 1230	<p><b>Communication &amp; Network City</b>            Assess &amp; Implement Secure Design Principles in Network Architectures (Open System Interconnection (OSI) &amp; Transmission Control Protocol/Internet Protocol (TCP/IP) Models, Internet Protocol (IP) Networking (e.g., Internet Protocol Security (IPSEC), Internet Protocol (IP) V4/6), Secure Protocols, Implications of Multilayer Protocols, Converged Protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice Over Internet Protocol (VOIP)), Micro-Segmentation (e.g., Software Defined Networks (SDN), Virtual Extensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (Sd-Wan)), Wireless Networks (e.g., Li-Fi, Wi-Fi, Zigbee, Satellite), Cellular Networks (e.g., 4G, 5G), Content Distribution Networks (CDN))</p>
1230 - 1245	Break
1245 - 1420	<p><b>Communication &amp; Network City (cont'd)</b>            Secure Network Components (Operation of Hardware (e.g., Redundant Power, Warranty, Support), Transmission Media, Network Access Control (NAC) Devices, Endpoint Security</p>
1420 - 1430	<b>Recap</b>
1430	Lunch & End of Day Two

**Day 3**

0730 - 0830	<p><b>Communication &amp; Network City (cont'd)</b>            Implement Secure Communication Channels According to Design (Voice, Multimedia Collaboration, Remote Access, Data Communications, Virtualized Networks, Third-Party Connectivity</p>
0830 - 0930	<p><b>Identity &amp; Access Management (IAM)</b>            Control Physical &amp; Logical Access to Assets (Information, Systems, Devices, Facilities &amp; Applications) • Manage Identification &amp; Authentication Of People, Devices &amp; Services (Identity Management (IDM) Implementation, Single/Multi-Factor Authentication (MFA), Accountability, Session Management, Registration, Proofing, &amp; Establishment of Identity, Federated Identity Management (FIM), Credential Management Systems, Single Sign on (SSO) &amp; Just-In-Time (JIT))</p>







0930 - 0945	Break
0945 - 1100	<b>Identity &amp; Access Management (IAM) (cont'd)</b> Federated Identity With a Third-Party Service (On-Premise, Cloud & Hybrid) • Implement & Manage Authorization Mechanisms (Role Based Access Control (RBAC), Rule Based Access Control, Mandatory Access Control (MAC), Discretionary Access Control (DAC), Attribute Based Access Control (ABAC) & Risk Based Access Control)
1100 - 1200	<b>Identity &amp; Access Management (IAM) (cont'd)</b> Manage the Identity & Access Provisioning Lifecycle (Account Access Review (e.g., User, System, Service), Provisioning & Deprovisioning (e.g., On /Off Boarding & Transfers), Role Definition (e.g., People Assigned To New Roles) & Privilege Escalation (e.g., Managed Service Accounts, Use of Sudo, Minimizing Its Use) • Implement Authentication Systems (OpenID Connect (OIDC)/Open Authorization (Oauth), Security Assertion Markup Language (SAML), Kerberos, Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+))
1200 - 1230	<b>Security Assessment &amp; Testing</b> Design & Validate Assessment, Test, & Audit Strategies (Internal, External & Third-Party) • Conduct Security Control Testing (Vulnerability Assessment, Penetration Testing, Log Reviews, Synthetic Transactions, Code Review & Testing, Misuse Case Testing, Test Coverage Analysis, Interface Testing, Breach Attack Simulations & Compliance Checks)
1230 - 1245	Break
1245 - 1420	<b>Security Assessment &amp; Testing (cont'd)</b> Collect Security Process Data (e.g., Technical & Administrative)( Account Management, Management Review & Approval, Key Performance & Risk Indicators, Backup Verification Data, Training & Awareness & Disaster Recovery (DR) & Business Continuity (BC)) • Analyse Test Output & Generate Report(Remediation, Exception Handling & Ethical Disclosure)
1420 - 1430	<b>Recap</b>
1430	Lunch & End of Day Four

**Day 4**

0730 - 0830	<b>Security Assessment &amp; Testing (cont'd)</b> Conduct or Facilitate Security Audits (Internal, External & Third-Party)
0830 - 0930	<b>Security Operations</b> Understand & Comply with Investigations (Evidence Collection & Handling, Reporting & Documentation, Investigative Techniques, Digital Forensics Tools, Tactics, & Procedures & Artifacts (e.g., Computer, Network, Mobile Device)) • Conduct Logging & Monitoring Activities (Intrusion Detection & Prevention, Security Information & Event Management (SIEM), Continuous Monitoring, Egress Monitoring, Log Management, Threat Intelligence (e.g., Threat Feeds, Threat Hunting) & User & Entity Behaviour Analytics (UEBA)) • Perform Configuration Management (CM) (e.g., Provisioning, Baselining, Automation) • Apply Foundational Security Operations Concepts (Need-To-Know/Least Privilege, Separation of Duties (SoD) & Responsibilities, Privileged Account Management, Job Rotation & Service Level Agreements (SLAs)) • Apply Resource Protection (Media Management & Media Protection Techniques)
0930 - 0945	Break



0945 – 1230	<p><b>Security Operations (cont'd)</b>            Conduct Incident Management (Detection, Response, Mitigation, Reporting, Recovery, Remediation &amp; Lessons Learned) • Operate &amp; Maintain Detective &amp; Preventative Measures (Firewalls (e.g., Next Generation, Web Application, Network), Intrusion Detection Systems (IDS) &amp; Intrusion Prevention Systems (IPS), Whitelisting/Blacklisting, Third-Party Provided Security Services, Sandboxing, Honeypots/Honeynets, Anti-Malware &amp; Machine Learning &amp; Artificial Intelligence (AI) Based Tools) • Implement &amp; Support Patch &amp; Vulnerability Management • Understand &amp; Participate in Change Management • Implement Recovery Strategies (Backup Storage Strategies, Recovery Site Strategies, Multiple Processing Sites &amp; System Resilience, High Availability (HA), Quality of Service (QOS), &amp; Fault Tolerance)</p>
1230 – 1245	Break
1245 - 1420	<p><b>Security Operations (cont'd)</b>            Implement Disaster Recovery (DR) Processes (Response, Personnel, Communications, Assessment, Restoration, Training &amp; Awareness &amp; Lessons Learned • Test Disaster Recovery Plans (DRP)(Read-Through/Tabletop, Walkthrough, Simulation, Parallel &amp; Full Interruption) • Participate in Business Continuity (BC) Planning &amp; Exercises • Implement &amp; Manage Physical Security (Perimeter Security Controls &amp; Internal Security Controls) • Address Personnel Safety &amp; Security Concerns (Travel, Security Training &amp; Awareness, Emergency Management &amp; Duress)</p>
1420 - 1430	<b>Recap</b>
1430	Lunch & End of Day Four

**Day 5**

0730 – 0930	<p><b>Software Development Security</b>            Understand &amp; Integrate Security in the Software Development Life Cycle (SDLC)( Development Methodologies (e.g., Agile, Waterfall, Devops, Devsecops), Maturity Models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM), Operation &amp; Maintenance, Change Management &amp; Integrated Product Team (Ipt)•</p>
0930 – 0945	Break
0945 – 1100	<p><b>Software Development Security (cont'd)</b>            Identify &amp; Apply Security Controls in Software Development Ecosystems (Programming Languages, Libraries, Tool Sets, Integrated Development Environment (Ide), Runtime, Continuous Integration &amp; Continuous Delivery (Ci/Cd), Security Orchestration, Automation, &amp; Response (Soar), Software Configuration Management (SCM), Code Repositories &amp; Application Security Testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST)</p>
1100 - 1230	<p><b>Software Development Security (cont'd)</b>            Assess the Effectiveness of Software Security (Auditing &amp; Logging of Changes &amp; Risk Analysis &amp; Mitigation) • Assess Security Impact of Acquired Software (Commercial-Off-The-Shelf (COTS), Open Source, Third-Party &amp; Managed Services (e.g., Software as a Service (SAAS), Infrastructure as a Service (IAAS), Platform as a Service (PAAS))</p>



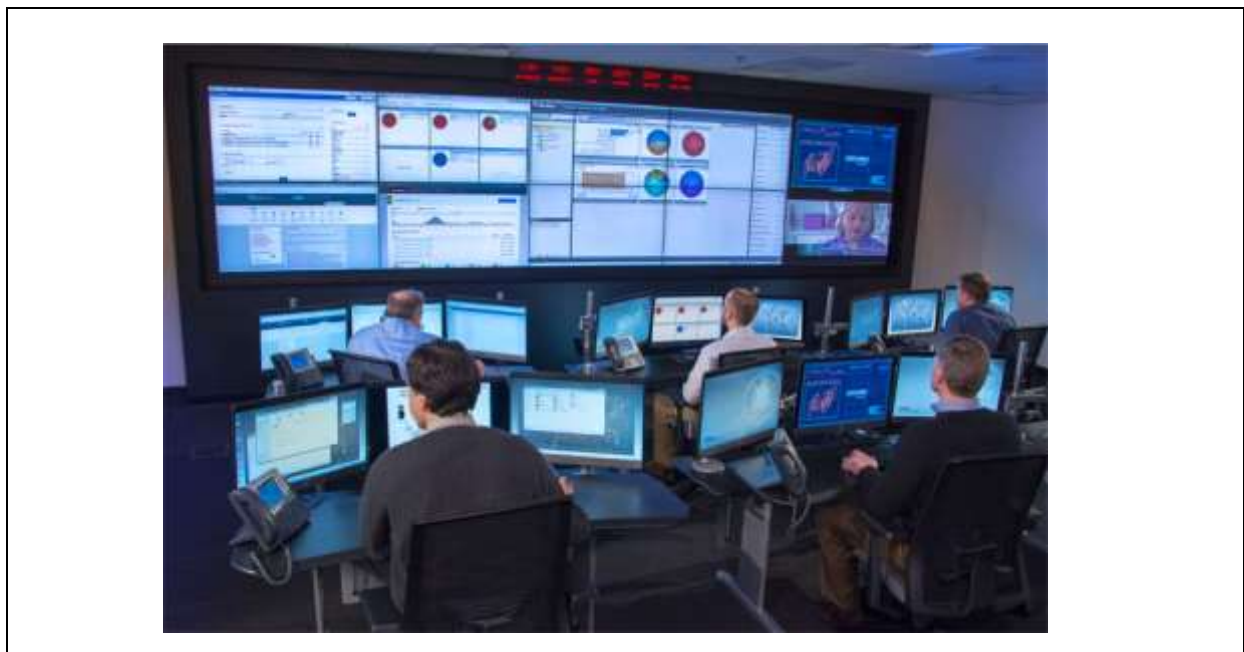
1230 – 1245	Break
1245 – 1345	<b>Software Development Security (cont'd)</b> <i>Define &amp; Apply Secure Coding Guidelines &amp; Standards (Security Weaknesses &amp; Vulnerabilities at the Source-Code Level, Security of Application Programming Interfaces (APIS), Secure Coding Practices &amp; Software-Defined Security)</i>
1345 - 1400	<b>Course Conclusion</b>
1400 – 1415	<b>POST-TEST</b>
1415 – 1430	<i>Presentation of Course Certificates</i>
1430	<i>Lunch &amp; End of Course</i>

**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 Howard’s Portal. Each participant will be given a username and password to log in Howard’s Portal for the MOCK exam during the 7 days following the course completion. Each participant has only one trial for the MOCK exam within this 7-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](mailto:mari1@haward.org)