

HISP Certification Course (5 days)

***HISP stands for Holistic Information Security Practitioner.

Cost: \$2,995 per person

This is the only integration course available today, which teaches the integration of ISO 27002/27001 with US Federal Regulations, pertaining to Information Security & Privacy.

Course Curriculum: Day 1–2

Course: ISO/IEC 27002:2005 (formally known as ISO 17799) Compliance

Description: The objective of this course is to provide delegates with the necessary skills to implement a corporate Information Security Management System (ISMS) framework that is compliant with the requirements of ISO 27002, UK Data Protection Act, EU Directive on Privacy, HIPAA Security, FFIEC, GLB Act, Sarbanes-Oxley Act (Security), FACT Act, PCI Data Security, California SB-1386, OSFI, PIPEDA, PIPA, Canadian Bill C-198 and meets certification requirements of ISO 27001.

Who should attend?

- Staff tasked with the implementation and management of an ISO 17799:2000 or ISO 27002:2005 Information security management system (ISMS).
- Staff tasked with ensuring compliance with UK Data Protection Act, EU Directive on Privacy, HIPAA Security, SOX Security, FFIEC, GLBA, California SB1386, FACT Act, PCI Data Security, OSFI, PIPEDA, PIPA, Canadian Bill C-168 and other regulations.
- Information Security Consultants or Third Party Auditors.
- Auditors (External and Internal).
- Information Security Officers.
- IT Managers/Directors.
- Privacy/Compliance Officers.

Benefits to Your Business

- Learn how to adopt international best practices pertaining to Information Security.
- Take the knowledge and skills imparted during this exercise and use them to improve confidentiality, integrity and availability of information systems.
- Gain competitive advantage.
- Improve customer and investor confidence.
- Show due diligence and due care.

Course Content

The course is designed for people who have a reasonable awareness of Information security management.

- History of ISO 17799 / BS 7799 / ISO 27000 series.
- Comparison of ISO 17799:2000 and ISO 27002:2005
- ISO 27001 certification requirements.
- Determination of scope.
- Identification of information assets.

- Determination of the value of information assets.
- Determination of risk.
- Determination of policy(ies) and the degree of assurance required from controls.
- Identification of control objective and controls.
- Definition of polices, standards and procedures to implement the controls.
- Production and implementation of policies, standards and procedures.
- Completion of ISMS documentation requirements.
- Establishment of Management Framework and Security Forum.
- Audit and review of ISMS.
- Case Studies.

Course Curriculum: Day 3-5

Course: US Federal Government Information Security Governance.

Description: The objective of this course is to provide delegates with the necessary skills to implement an Information Security Program at a federal, state or local government agency that is compliant with the requirements of the Clinger-Cohen Act of 1996, the Federal Information Security Management Act (FISMA) of 2002, Office of Management and Budget (OMB) Circular A-130, and the National Institute of Standards and Technology (NIST).

Who should attend?

- Chief information officers (CIOs)
- Senior Agency Information Security Officers (SAISOs).
- Chief Information Security Officers (CISOs).
- Chief Privacy Officers (CPOs)
- Information System Security Officers (ISSOs).
- Information System Security Managers (ISSMs).
- Information Security Administrators.
- IT Managers/Directors.
- Privacy/Compliance Officers.
- Information Security Consultants.
- Staff tasked with the implementation of FISMA, OMB and NIST compliance.

Benefits to Your Agency

- Learn a broad overview of information security best practices.
- Learn how to adopt FISMA, OMB and NIST Information Security Governance framework.
- Take the knowledge and skills imparted during this exercise and use them to improve confidentiality, integrity and availability of information systems.
- Gain information that can be used to build an information security program implementation and management strategies.
- Show due diligence and due care.

Course Content

The course is designed for people who have a reasonable awareness of Information Technology Controls, including.

- Clinger-Cohen Act of 1996
- FISMA (Federal Information Security Management Act)
- Office of Management and Budget (OMB) Circular A-130, (Management of Federal Information Resources).
- FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems)
- FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems)
- NIST SP800-30 (Risk Management Guide for Information Technology Systems)
- NIST SP800-37 (Guide for the Security Certification and Accreditation of Federal Information Systems)
- NIST SP800-34 (Contingency Planning Guide for Information Technology Systems)
- NIST SP800-53 (Recommended Security Controls for Federal Information Systems)
- NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems)
- NIST SP800-100 (Information Security Handbook: A Guide for Managers)
- Privacy Act/Privacy Impact Analysis
- DITSCAP/NIACAP Process (Department of Defense Technology Security Certification & Accreditation Process/National Information Assurance Certification and Accreditation Process)
- DIACAP (Department of Defense Information Assurance Certification and Accreditation Process)
- NIST SP 800-53 VS. ISO/IEC 27002:2005 MAPPING
- Case Studies:
 - C&A
 - POA&M Creation and Management
 - Information Security Program implementation
 - Leadership Styles in Information Security Implementation

Certification Exam

Attendees can chose to take the HISP Certification Exam which is now managed by the HISP Institute on the afternoon of Day 5, consisting of:

- 100 multiple-choice questions.
- Questions covering the entire HISP course curriculum.

Instructor Biographies

Taiye Lambo CISSP, CISA, HISP, BS 7799 Certified Auditor

Taiye Lambo is a Security subject matter expert in the area of Information Security Governance; with years of experience in design & implementation of Intrusion detection and prevention systems, Honey pots, Computer Forensics, Ethical Attack & Penetration Testing, Biometric Identification, Network Security Architecture, Information security governance. He founded the UK Honey net project – www.honeynet.org.uk

He has successfully executed information security projects for a number of United Kingdom government agencies and also provided information security consulting to State of Georgia agencies. In the commercial sector he has completed Consulting engagements for clients, in the Manufacturing, Financial Services and Healthcare sector.

He was the Director of Information Security for John H. Harland (now Harland Clarke), the leading provider of solutions to the Financial Services industry, including check and check related products and accessories, direct marketing solutions, and contact center solutions.

He has dual expertise as a hybrid technical and business information security consultant with a pragmatic holistic approach to the management of information security and regulatory compliance, as well as a subject matter expert on Information Security governance and compliance relating to regulatory standards such as HIPAA, Sarbanes-Oxley Act, Gramm-Leach Bliley Act (GLBA), FDIC and others. His presentations at security events include conferences organized by organized by ISSA, InfraGard, ISACA, CPM and SOFE.

Taiye is Founder & CTO of eFortresses, an Atlanta based risk management solutions company founded in 2002. In the United Kingdom, he founded a successful information security firm CyberCops Europe, gained assignments in the USA for commercial and government agencies where he continued Information security and compliance consulting and became a subject matter expert in several of the current regulations. His involvement in the USA grew with speaking engagements at leading seminars & conferences. He left CyberCops Europe, came to the USA and founded eFortresses in October 2002. He has established numerous valuable contacts nationwide and has name recognition in the information security/regulatory compliance space.

eFortresses developed the industry's first integrated security and compliance assessment product, *Compliantz* - an automated process to assess an organization's policies, processes and procedures against internationally accepted information security best practices and multiple regulatory requirements, including HIPAA Security, Sarbanes-Oxley Act (Security), GLB Act, California SB-1386, NIST 800-53, FACT Act and PCI Data Security. eFortresses also developed and holds classes nationwide in the industry's very first information security, audit and compliance certification course - Holistic Information Security Practitioner (HISP).

With a Bachelors degree in Electrical Engineering, he also earned a Masters degree in Business Information Systems from the University of East London (United Kingdom).

Karl Chambers CISSP, CISA, PMP

Major (retired) Karl Chambers is an information security governance, assurance and risk expert. He is certified as a Project Management Professional (PMP), Certified Information Systems Auditor (CISA), and a Certified Information Systems Security Professional (CISSP). On graduating from Excelsior High School in 1978, he

joined the Jamaica Defense Force (JDF) and later served for 20 years. Major Chambers was trained at the Royal Marines Commando Training Center, and the Royal Military Academy Sandhurst, in England. He graduated from the Royal Military College of Science (Cranfield Institute of Technology) Shrivenham, England with a BEng in Electronic Systems and Software Engineering. He also holds a MSc. in Management Information Systems from the University of the West Indies.

He has over nineteen years information security experience in the military, U.S. Federal Government, U.S. Banking and international hospitality sectors. Major Chambers has conducted numerous information security risk assessments and information assurance audits for large international companies and U.S. Federal Government Agencies.

Over the last five years he has conducted numerous Certifications and Accreditation projects for applications and General Support Systems, based on the NIACAP and NIST 800-37 methodologies. Since September 2004, he has provided FISMA related information assurance services to the US Department of Justice (DOJ), helping to move that agency's Federal Cyber Security Report Card grade from a D to an A-.

In 2004 and 2005 he helped the United States Agency for International Aid (USAID) obtain consecutive A+ grades on the U.S. Federal Cyber Security Report Card. One of his more notable achievements is the development of an information security risk assessment methodology, which has been adopted as a standard by a number of US Federal Government Agencies.

He has developed and taught numerous seminars on information security awareness, privacy, managing information security risks and project management.

On retirement from the JDF he joined Bank of America as an Assistant Vice President, before founding Diligent eSecurity International, where he currently serves as President and CEO.

Charles Edward Wilson CISM, ISSM, HISP, MTS

Ed Wilson is CISM, DoD Certified Information Systems Security Manager (ISSM), and a retired US Navy Cryptologic Technical Technician with over 27 years experience in INFOSEC - securing, auditing, and accrediting IT systems to include protection of sensitive corporate information in compliance with DoD regulations, ISO 9000, BS7799/ISO 17799, ISO 15408, FISMA, COSO, COBIT, GLBA, SOX, and HIPAA legislation.

Ed Wilson is a Certified Master Training Specialist, Testing Officer/Testing Supervisor, Curriculum Developer, and Technical Writer that strengthens his demonstrated excellence in leadership, technical competence, application of instructional methodology, and desire to improve educational awareness through quality instruction.

As an INFOSEC Subject Matter Expert, Ed Wilson developed 3 Information Systems Security Manager (ISSM) courses, consisting of 31 INFOSEC topics at the master level. Ed was an adjunct lecturer on INFOSEC matters for the National Security Agency (NSA) having taught twenty-six (26) National Cryptologic School courses for NSA.
