

HISP Certification Course (5 days)**Cost: \$2,995 per person**

***HISP stands for Holistic Information Security Practitioner.

This is the only integration course available today, which teaches the integration of ISO 27002/27001 with COBIT, COSO, ITIL and Multiple Regulations, pertaining to Information Security & Privacy.

Course Curriculum: Day 1 – 3**Course:** ISO 27002 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, NIST 800-53, 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 3-4

Course: COBIT auditing framework.

Description: The objective of this course is to provide delegates with the necessary skills to audit information technology systems using COBIT as a benchmarking standard.

Who should attend?

- Staff tasked with the adoption of COBIT as an IT governance framework.
- 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 COBIT as an IT governance framework.
- 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 Technology Controls.

- History of COBIT.
- Understanding COBIT Controls.
- Understanding COBIT mapping to ISO 27002.
- Understanding COBIT mapping to COSO.
- Understanding COBIT mapping to ISO 27002 and ITIL.
- COBIT case studies.

Course Curriculum: Day 5

Course: *Compliantz*® methodology

Description: The objective of this course is to provide delegates with the knowledge of how ISO 27002 requirements map to HIPAA, FFIEC, GLB Act, Sarbanes-Oxley Act, OSFI, PIPEDA, PIPA, Canadian Bill C-168 and other regulations. We will explain how to identify areas of **non-compliance** in a matter of a few **days**.

Who should attend?

- Staff tasked with achieving regulatory compliance with multiple Information security requirements.
- 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 effectively map multiple standards through a Compliance Matrix.
- 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 *Compliantz*.
- *Compliantz* methodology – proprietary mapping component.
- Description of *Compliantz* modules.
- Using automation to quickly identify non-compliance areas.
- Case studies.

Certification Exam

Attendees will be given the option to take the HISP Certification Exam, at no extra cost, 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, Honeydroids, Computer Forensics, Ethical Attack & Penetration Testing, Biometric Identification, Network Security Architecture, Information security governance. He founded the UK Honeydroid project – www.honeydroid.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).

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 manners for the National Security Agency (NSA) having taught twenty-six (26) National Cryptologic School courses for NSA.

Michael P. Johnson, CPP, CISSP, HISP, ISO 27001 Auditor, MBA, MSIA

Michael Johnson has more than twenty-five years experience in the security profession with his most recent work as an Information Security Practice Leader within the professional services organization of a large information technology services company. In this role he had senior management responsibility for a professional services organization providing a broad range of IT security policy, program and technical assessment, implementation, and response consulting services employing twenty-three IT security practitioners.

During a nineteen year career with First Security Services Corporation - a leading provider of Organizational Security Services, Mr. Johnson gained increasing responsibility for marketing, sales, management and delivery of a broad range of outsourced security services including information / computer security consulting, physical security consulting, training, investigations, technical services and uniformed security officer services. He spent five years building a large security operation in the metropolitan New York City area serving the security needs of the region's leading pharmaceutical, commercial real estate, financial services, accounting and law firms. Under his direction this organization grew to encompass one thousand two hundred employees and sales of nearly forty million dollars.

As a senior corporate executive with First Security Mr. Johnson was responsible for the development and launch of the Organizational Security concept; the cost efficient delivery of bundled risk management and security services designed to protect client companies against enterprise-wide threats to their five key assets-people, property, information, integrity, and reputation. As part of the Organizational Security initiative he was responsible for the start of First Security's Information Security Solutions Group, the creation of private labeled cyber-insurance and risk management products, and the development of a Business Counter-Espionage consulting practice. Additionally, Mr. Johnson acted as a senior business advisor to several nationally recognized public safety executives in the creation and start of public safety agency re-engineering and management consulting practice.

Mr. Johnson has worked in senior sales and business development roles with two large security services providers and served as president of a New York City based start-up security services and consulting company. He has also worked as an independent security consultant providing a broad range of advisory services to several large Fortune 500 companies in the Mid-Atlantic region.

Mr. Johnson is a member of the Information Systems Security Association (ISSA), the International

Information Systems Security Certification Consortium (ISC)2, the Computer Security Institute, the Information Systems Audit and Controls Association (ISACA), and ASIS International. He has served on numerous local, regional, and national security trade industry association committees, currently serving as a volunteer member of ASIS International President's Council on Enterprise Risk Management and the board of the HISP Institute.

He has consulted and acted as a senior advisor to several public safety agencies and the US Department of Justice. Mr. Johnson has lectured at several public safety agencies' training academies as well as colleges and universities.

He has authored or co-authored information security white papers; with two articles currently pending publication in information assurance technical trade journals.

Mr. Johnson is a former officer in the U. S. Army and holds a Bachelor of Arts in Criminal Justice from Norwich University, a Masters of Business Administration from Northeastern University, and a Masters of Science in Information Assurance from Norwich University. He is a Certified Information Systems Security Professional (CISSP), certified Holistic Information Security Practitioner (HISP), Certified Protection Professional (CPP), and has completed ISO 27001 Information Security Management Systems Lead Auditor and Implementation certification training.
