

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 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 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 Honeynet project – www.honeynet.org.uk and the Holistic Information Security Practitioner (HISP) Institute – www.hispi.org

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, SOFE, EDUCAUSE and HITRUST.

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 processes, policies, procedures and standards 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.

John A. DiMaria Certified Six Sigma Black Belt; HISP

John DiMaria is a management system professional and certified Holistic Information Security Practitioner (HISP) with 24 years of successful experience in Management System Development, including Information Systems, Quality Assurance, International Quality Standards, Statistical Process Control, Regulatory Affairs, Customer Service, Subcontractor Analysis and Marketing/Sales in a highly competitive environment. As the former Product Manager for BSI Management Systems America, John was the technical, scheme and marketing specialist responsible for overseeing development, education and expertise for BSI Americas regarding all information security and business continuity activities including ISO 27001, ISO 20000 and BS 25999.

He serves on committees that influence legislation and drive international harmonization such as the CSIA (Cyber Security Industry Alliance) and the BITS Shared Assessment Program. He is the President of the HISPI and has been featured in many publications such as Computer World, Quality Magazine, QSU, SC Magazine, Campus Technology and GSN Magazine concerning various topics regarding information security and business continuity.

Prior to joining BSI, DiMaria was the Managing Consultant responsible for Information Security Services for LECG a global expert services firm. He has experience working with both national and international environments.

HIGHLIGHTED EXPERIENCE

- Served as the BSI Americas Technical & Marketing specialist in the areas of ISO 27001, ISO 20000, BS 25999 and all other areas of Information Security and Business Continuity.
- Designed and delivered training to Field Development Staff on ISO/BS 7799/27001 processes and mapping an ISMS to best practice regulatory and IT Standards.

- Designed and delivered projects for building, training and servicing in all areas of TQM, Regulatory Affairs, Information systems, Risk Analysis, the International Management System Standards, Statistical Process Control, Customer Service and Marketing and Sales, showing a cost savings through process improvement

These projects included but were not limited to:

- *Complete ISMS and other Management System Implementation*
- *Management System Analysis and Improvement*
- *Process Mapping*
- *Process Flow Analysis*
- *Process Control Planning*
- *Fault Tree Analysis*
- *Technical Writing*
- *Preventive Action Planning and Implementation*
- *Use Case Modeling*
- *Six Sigma*
- *Statistical Analysis*
- *Failure Mode Effect Analysis*
- *Regulatory Analysis and Compliance (Including EMS & OSHA processes)*
- *Employee Engineering*
- *Training Development & Delivery*
- *Auditing (Internal and External)*
- *Subcontractor Evaluation*
- *Risk Assessment & Management*
- *Business Process Re-engineering*

EXPERIENCE CONT.

- Served 4 years as member of the Top Management Operations Board of Directors for a multi-site \$100M corporation. Prior 16 years managed implementation of SPC, Regulatory Affairs, process controls, information systems and international management systems standards.
- Performed over 100 internal quality system and external supplier quality audits.
- Served on an Automotive Advisory Committee to represent the Chemical Industry during the original conception of the QS 9000 international automotive standard.
- Implemented Six Sigma strategies and led a cross-functional team for a major multi-million dollar corporation in St. Louis, MO.

EDUCATION

- HISP (Holistic Information Security Practitioner); Certification
- B.B.(Black Belt) Six Sigma Certification, GE Six Sigma Academy
- Certificate, Six Sigma Leadership
- Certificate, Quality Operating Systems(QOS) FMEA; Eastern Michigan University
- Certificate. Electronic Data Interchange; EDI, INC
- Certification; Internal Auditor, Quality Management Institute
- DMACS Computerized Process Controls
- A.S. Computer Information Systems, Columbia College

PUBLICATIONS

- How to Deploy BS 25999 Version 2, April 2008
 - How to Deploy BS 25999; September 1, 2007
 - BS 7799 Audit Preparation; BSI Management Systems, March 2005
 - Benefits of BS 7799 and ISO 17799; BSI Management Systems, April 2005
 - BS 7799 Drivers and Advantages; BSI Management Systems, March 2005
-