

HISP Certification Course (5 days)

***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 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.