

The **Holistic Information Security Practitioner (HISP)** Training & Certification program was created to address the current shortage of Information Security and Compliance professionals, with practical skills needed to help organizations address Information Security and Compliance requirements, by being able to Implement Compliance frameworks that are repeatable, sustainable and effective.

We are not looking to position the HISP certification to replace existing certifications such as CISSP, CISA, CISM, CFA, but rather we are looking to complement such certifications and also offer CPEs for professionals who already hold such designations.

The HISP designation means that:

- 1) The professional has a good grounding in International best practices for Information Security & Audit Governance as well as general IT Governance i.e. ISO 17799, ITIL, CobiT and COSO.
- 2) The professional takes a Holistic risk management approach to Information Security.
- 3) The professional is a hybrid Information Security professional, well balanced between technical and business skills.
- 4) The professional can function effectively in the capacity of a CISO, CCO by tackling the challenge of Information Security as a business concern that is not solved by technology alone, but by People, Process and Technology.
- 5) The professional is able to map International best practices of ISO 17799, ITIL, CobiT and COSO to current and future regulatory compliance requirements.

The HISP designation is earned by completing the following steps:

Level 1

- 1) Attend the 5-day HISP Certification Course
- 2) Pass a certification exam, administered on the final day of the Course.

Level 2

- 1) Write a Thesis
or
Use the eFortresses **Compliantz** tool on 1 or 2 live projects



The Matrix below illustrates how the HISP Curriculum encompasses domains found in CISSP, CISM and CISA:

Domains	CISSP	CISM	CISA	HISP
Access Control Systems and Methodology	Y		Y	Y
Applications and Systems Development Security	Y			Y
Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)	Y		Y	Y
Cryptography	Y			Y - Partially
IS Audit Process			Y	Y - Partially
Information Security Program Management		Y		Y
Information Security Governance		Y	Y	Y
IT Governance			Y	Y - Partially
IT Service Delivery and Support			Y	Y - Partially
Law, Investigation and Ethics	Y			Y
Operations Security	Y			Y
Physical Security	Y			Y
Protection of Information Assets			Y	Y
Response Management		Y		Y
Risk Management		Y		Y
Security Architecture and Models	Y			Y - Partially
Security Management Practices	Y	Y		Y
Systems and Infrastructure Lifecycle Management			Y	Y
Telecommunications and Network Security	Y			Y