Holistic Information Security Practitioner Institute

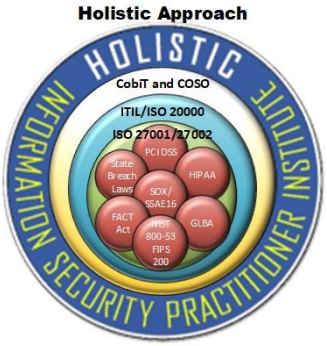
The HISP Institute:

The Holistic Information Security Practitioner (HISP) Institute (HISPI) is an independent training, education and certification 501(c)(3) Nonprofit organization promoting a holistic approach to Cybersecurity, consisting of volunteers that are true information security practitioners, such as Chief Information Officers, Chief Risk Officers, Chief Information Security Officers (CISOs), Information Security Officers (ISOs), Information Security Managers, Directors of Information Security, Security Analysts, Security Engineers and Technology Risk Managers from major corporations and organizations.

- **HISPI** focuses on international standards, best practices and comprehensive frameworks for developing robust and effective information security programs.
- The HISP certification complements existing recognized security certifications such as CISSP, CISA, CISM, CGEIT, CRISC or CMMC.

The HISP certification approach prides itself on ensuring that an educational foundation, provided by information security training, is the cornerstone of the HISP certification and the HISP Institute.

The Holistic Approach:



HISPI promotes a holistic approach to information security program management.

The issue of information security and regulatory compliance affects organizations of all sizes and sectors, with an identical problem, their inherent vulnerability and high cost of compliance. Unfortunately, in most cases, the regulations and laws set forth offer little guidance of any specific security measures or standards, leaving the decision up to the organization instead. This causes confusion, misinterpretation and drives up costs.

Many organizations struggle and treat each of these compliance areas as a silo. By taking this approach, the opportunity for a security breach is enhanced.

An integrated approach can help form the basis for a secure information security program and design and deploy a comprehensive risk governance platform for both compliance and assurance.

The HISP framework utilizes the IOCM philosophy based on a unique approach that stands alone in the security, risk management and compliance industry. IOCM is a structure for solving business and compliance problems. The structure includes a powerful methodology, analytical methods and tools, improvement techniques, trained capable People, repeatable mature Processes and optimized Technology. This approach reduces the cost of meeting legal, regulatory and contractual requirements pertaining to information security, across various sectors through the Implement Once Comply Many (IOCM) philosophy.

Phase 1: Training and Certification

HISPI created this program to help you launch a successful career in Cyber Security and take you from being an ordinary employee into an extraordinary leader.

This phase of the program lasts for 30 to 90 days at a cost of $200 per person.

To complete this program, the following steps must be completed:

- Complete entry-level on-demand HISP certification course
- Take and pass entry-level on-demand HISP certification examination

Phase 2: Mentoring, Internship, Apprenticeship and Job Placement

HISPI created this program for you to receive support for employment and continued success on your career path and journey.

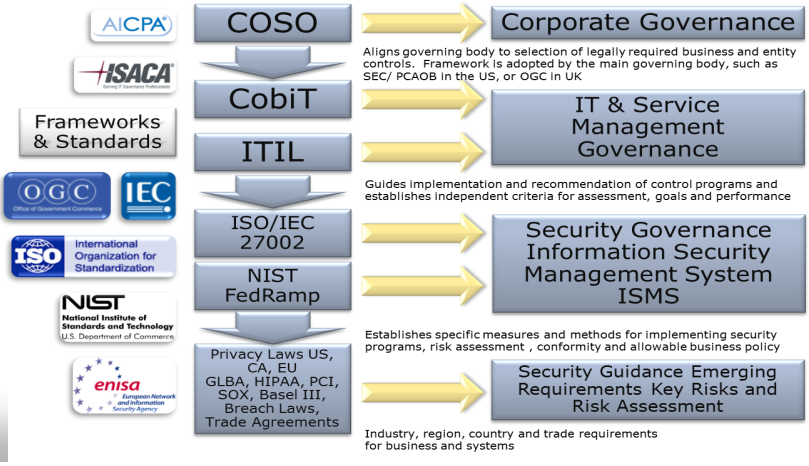
This phase of the program lasts for 180 to 270 days at a cost of $5,000 per person.

Quarterly payment plan or sponsorship may be possible.

To complete this program, requires the following steps:

- Schedule bi-weekly or monthly mentoring sessions
- Complete and present 90-day career path and roadmap
- Complete 90 day research based unpaid internship virtual part time (10 hours/week)
- Join 90 to 180 days paid apprenticeship program (30 day probation) virtual part time (10 hours/week)
- Achieve "Associate" Status
- Successful Job Placement

HISP Framework Approach



Certification Tracks:

Training track

- Attend the 5-day HISP Certification Course - public, private onsite or OnDemand web-based.
- Pass a certification exam, administered on the final day of a Course or online.

OR

Pre-requisite track

- Pass a certification exam hosted by HISPI.
- Provide evidence to HISPI that you currently possess one or more of the following certifications: CISSP, CISA, CISM, CGEIT, CRISC or OCMT and that you are in good standing with their Certifying bodies:

For additional information regarding the HISP training and certification programs, including latest course outlines, public class calendar and examination schedules,

Who Should Certify?

- Anyone tasked with the implementation and management of an ISO 27001/27002 Information Security Management System (ISMS).
- Anyone tasked with ensuring compliance with UK Data Protection Act, EU Directive on Privacy, Basel II, HIPAA Security, SOX Security, GLBA, California SB-1386, FACT Act, PCI Data Security, NIST 800-53 and other regulations.
- Information Security Consultants or Third Party Auditors.
- Auditors (External and Internal).
- Information Security Officers.
- Any security executive looking for continuous career progression and increased value by demonstrating an understanding of the full range of contemporary security issues facing their organization.

HISP Comparison Matrix

Domains	CISSP	CISM	CISA	CCSK	CMMC	HISP
Access Control	✓		✓	✓	✓	✓
Application Development Security	✓			Partial		✓
Business Continuity and Disaster Recovery Planning	✓		✓	✓	Partial	✓
Cryptography	✓			Partial	Partial	Partial
Information Security Audit Process			✓	Partial	Partial	Partial
Information Security Program Management		✓			Partial	✓
Information Security Governance		✓	✓	Partial		✓
Information Technology Governance			✓	✓		Partial
Information Technology Service Delivery and Support			✓			Partial
Legal, Regulations, Investigations and Compliance	✓			✓	Partial	✓
Operations Security	✓				✓	✓
Physical and Environmental Security	✓			✓	✓	✓
Protection of Information Assets			✓	✓	✓	✓
Response Management		✓		✓	✓	✓
Risk Management		✓		✓	✓	✓
Security Architecture and Design	✓			✓	Partial	Partial
Security Management Practices	✓	✓			✓	✓
System and Infrastructure Lifecycle Management			✓	✓	✓	✓
Telecommunications and Network Security	✓			Partial	✓	✓

CPE Requirements:

Once HISP certification is achieved it must be maintained by obtaining CPEs as follows:

A total of 90 (30 per year) CPEs by the end of a three-year certification cycle and pay the Annual Membership Fee of US$50 during each year of the three-year certification cycle before the annual anniversary date.

Group 1: Direct Domain-Related Activities Group 1 credits are given for completion of activities which relate directly to the information security profession and related frameworks (ISO 27000, ISO 20000, COBIT, ITIL, COSO, NIST & Security Regulations) 60 of the 90 credits must come from this group.

Group 2: Professional Skills Activities Completion of activities which enhance one's overall professional skills, education, knowledge or competency. Including professional development programs, such as speaking engagements, management courses and conference sessions on related fields (e.g. forensics, anti money laundering). While these may not apply directly to the HISP field we must support a rounded education in the field of information security.

HISPI Membership:

Associate membership to the HISP Institute is open to anyone. Simply visit www.hispi.org and sign up.

Full membership fees are US$50 (included in certification examination fees). Full membership provides complete access to all available reference material on the HISPI website.

For more information about the HISP Institute or Certification, visit:
www.hispi.org
or call toll free
888-247-4858