

IAPP Privacy Certification

Program Introduction to the Certification Foundation



Overview

Each candidate who seeks an IAPP privacy certification for the very first time must complete the Certification Foundation, an elective course and mandatory exam that cover elementary concepts of privacy and data protection from a global perspective.

Certification Foundation describes the fundamental definitions and standards frameworks for privacy and data protection and takes an international view in outlining all of the different data protection models in force today. Detailed coverage of national privacy and data protection laws and regulations is provided separately under the individual certification programs (CIPP, CIPP/G, CIPP/C and CIPP/IT). These individual programs may be selected by each student based upon professional objective.

The Certification Foundation program also addresses two general practice concentrations: (1) Information security; and, (2) Online privacy. These subject matter areas have no geographic boundaries and thus are relevant to all privacy professionals irrespective of jurisdiction, practice or industry.

Existing IAPP-certified professionals (CIPP, CIPP/G, CIPP/C or CIPP/IT credential holders) are not required to complete the Certification Foundation examination; however, if they seek an additional IAPP certification over time, they must successfully complete the corresponding examination for that certification of choice.

It is important to note that Certification Foundation is not itself an IAPP credential; rather, it is the necessary first step in the path toward an IAPP credential. It consists of a course of instruction and a timed examination:

- Certification Foundation Training Workshop (five hours) is *optional* for all certification candidates, open to all certification candidates and held as a single class at select events;
- Certification Foundation Examination (two hours) is *required* of all certification candidates and is held as a single class at select events. It is the first of two requirements that candidates must satisfy in order to achieve *any* IAPP certification (the second requirement being successful completion of a single certification examination of the candidate's choosing).

Who Should Apply

- ALL first-time candidates seeking an IAPP certification for the very first time

Please note that existing IAPP-certified professionals (CIPP, CIPP/G, CIPP/C or CIPP/IT credential holders) need not apply for Certification Foundation as they are 'grandfathered' in to the course requirements by virtue of their current designation.

Course Format

The Certification Foundation course is designed to provide the basis for a multi-faceted approach to privacy and data protection and to allow for the specific application of IAPP privacy certifications (presently CIPP, CIPP/G, CIPP/C and CIPP/IT) to build upon this foundation with minimal repetition.

The Certification Foundation course components are:

- I. **Introduction to Privacy: Common Principles and Approaches**
- II. **Information Security: Protecting and Safeguarding Personal Information**
- III. **Online Privacy: Using Personal Information on Web Sites and with Other Internet-related Technologies**

All first-time candidates for IAPP certification must complete and pass the Certification Foundation Examination: a two-hour, three-part, 120-item objective test offered by the IAPP. This examination covers each of the three course components that are identified above and described in further detail on the following pages. "Successful completion" of the Foundation Exam is defined as an individual, aggregate score of 84 points (70%) or greater.

Candidates for IAPP certification may take the Foundation Examination in sequence with the certification examination of their choice or, at separate testing dates and locations according to the testing schedule published regularly by the IAPP and available for review at www.privacyassociation.org.

Course References

The following publications (with specific chapters and page numbers identified) are highly recommended for Certification Foundation course and exam preparation:

- Chapters I, II (pages 28-50 and 81-105 only), IV, V and VI of "[Information Privacy: Official Reference for the Certified Information Privacy Professional \("CIPP"\)](#)" by Peter P. Swire, CIPP and Sol Bermann, CIPP (IAPP, 2007). ISBN #978-0-9795901-0-8. Available through the IAPP Certification Reference Library.
- Chapters I, VIII and IX from "[The IAPP Information Privacy Case Book: A Global Survey of Privacy and Security Enforcement Actions with Recommendations for Reducing Risk](#)" by Margaret P. Eisenhauer, Esq., CIPP (IAPP, 2008). ISBN #978-0-9795901-2-2. Available through the IAPP Certification Reference Library.

Training workshops for students of Certification Foundation are provided by the IAPP in both live classroom settings and as DVD courseware packages. More information on scheduling and purchasing is available at www.privacyassociation.org/certification.

IAPP Privacy Certification

Outline for the Certification Foundation Course and Examination



I. Introduction to Privacy: Common Principles and Approaches

A. Common Descriptions of Privacy

- a. Definitions
- b. Global perspectives
 - i. Countries with national data protection laws in force
 - ii. Countries with emerging privacy or data protection laws
- c. A brief history: social and statutory origins of privacy protection

B. The Concept of Personal Information

- a. Elements of privacy
 - i. Individuals and information about individuals
 - 1. Data subjects (E.U. definition)
 - 2. Personal data (E.U. definition)
 - 3. Sensitive personal information ("SPI")
 - ii. Data processing
 - 1. Data controller (E.U. definition)
 - 2. Data processor (E.U. definition)
 - iii. Oversight
 - 1. National data protection authorities ("DPA")

C. Risks and Other Driving Factors

- a. Privacy as a factor in business risk management
 - i. Common business information processes
 - 1. Internal systems
 - 2. Third party relationships

D. Modern Principles of Privacy

- a. The historical evolution of privacy principles
 - i. United States
 - 1. U.S. fair information practices

- a. U.S. Department of Health Education and Welfare (“HEW”) Report of 1974
- ii. Europe
 - 1. The Council of Europe (“COE”), “Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data of 1981” (“COE Convention”)
 - a. Data protection principles
 - 2. The European Union (“EU”) Data Protection Directive (95/46/EC)
- iii. Asia
 - 1. The Asia Pacific Economic Cooperation (“APEC”) privacy framework of 2005
- iv. Other frameworks
 - 1. The Organization of Economic Cooperation and Development (“OECD”) “Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data” (1980)
- v. Other countries
 - 1. With national data protection laws established
 - 2. With European “adequacy” achieved

E. The Collective View of Privacy Principles

- i. Policy and notice
- ii. Choice and consent
 - 1. Opt-in, opt-out
- iii. Data subject access
- iv. Information security
- v. Quality
- vi. Information lifecycle principles
 - 1. Collection
 - 2. Use and retention
 - 3. Disclosure
 - 4. Management and administration
 - 5. Monitoring and enforcement

F. Privacy and Data Protection Regulation

- a. A global view of rights, obligations and enforcement environments
 - i. Common components
 - 1. Obligations to the data subject
 - 2. Rights of the data subject
 - 3. Administration and enforcement
 - 4. Legal requirements
 - a. Privacy laws
 - b. Labor laws
 - c. Sector-based or contextual laws
- b. National data protection regimes
 - i. United States
 - 1. Federal
 - 2. State
 - 3. Safe harbor agreement
 - a. Onward transfer
 - b. Security
 - c. Data integrity
 - ii. Europe
 - 1. The European Union (“EU”) Data Protection Directive (95/46/EC)
 - a. Applicability
 - b. Core principles

- c. Data processing
 - i. Special categories of data
 - ii. Security safeguards
- d. Data integrity
- e. Model contracts
- 2. The European Union ("EU") Electronic Communications Directive (2002/58/EC)
- 3. The Article 29 Working Party
- iii. Canada
 - 1. The Privacy Act of 1983
 - 2. The Personal Information Protection and Electronic Documents Act of 2000 ("PIPEDA")
- iv. Asia
 - 1. Law Concerning the Protection of Personal Information (Japan, 2003)
 - a. Transfers of personal information
 - 2. Other national data protection laws
- v. South and Central America
 - 1. Argentina
 - 2. Chile
 - 3. Paraguay

G. Elements of Effective Privacy Management

- a. Understanding personal information use within the organization
 - i. Goals and considerations
- b. Managing privacy risk and compliance
 - i. Privacy policy development
 - ii. Program governance
 - iii. Risk management and compliance
 - iv. Incident management
- c. Controlling use of personal information
 - i. Procedures and controls
 - ii. Information security
 - iii. Managing third parties
 - iv. Training and awareness

II. **Information Security: Protecting and Safeguarding Personal Information**

A. Introduction to Information Security

- a. Privacy and information security in context
 - i. Information types
- b. Information security defined
 - i. Confidentiality, integrity and availability
- c. Information security needs and principles
 - i. Segregation of duties
 - ii. Need-to-know access
- d. Information security standards
 - i. ISO 27001 applied to personal information protection
 - ii. ISO 17799 / 27002 applied to personal information protection
 - 1. Security clauses
- e. Risks and other driving factors
 - i. Threat agents
 - ii. Natural causes

- f. Information security threats and vulnerabilities
 - i. Malware
 - ii. Phishing
 - iii. Cross-site scripting (“XSS”)
 - iv. SQL injection attacks
 - v. Risks related to unauthorized disclosure and use

B. Compliance Requirements

- a. Safeguarding personal information
 - i. United States
 - 1. The U.S. Gramm-Leach-Bliley Act (“GLBA” Safeguards Rule)
 - 2. The U.S. Health Insurance Portability and Accountability Act (“HIPAA”) Security Rule
 - 3. The U.S. Fair and Accurate Credit Transactions Act (“FACTA”)
 - 4. U.S. safe harbor certification
 - ii. Australia
 - 1. The Privacy Act: Sections 4, 4.1 and 4.2
 - iii. Europe
 - 1. The E.U. Data Protection Directive (95/46/EC): Articles 16 and 17
 - 2. The United Kingdom Data Protection Act of 1998: the seventh principle

C. Information Security Management

- a. Common information security controls
 - i. Access control types
 - 1. Preventative
 - 2. Detective
 - 3. Corrective
 - ii. Access control placement
 - 1. Network
 - 2. Operating system
 - 3. Application layer
 - 4. Mobile computing / telecommuting
 - iii. Cryptography
 - 1. General concepts of shared and public key cryptography
 - a. Public key infrastructure (“PKI”)
 - b. Encryption
 - i. Data at rest
 - ii. Data in motion
 - iii. Application versus field encryption
 - iv. Disk and file encryption
 - iv. Identity and access management (“IAM”)
 - 1. Authentication
 - 2. Authorization
- b. Implementing information security controls
 - i. Security policy
 - ii. Governance
 - 1. Internal to organization
 - 2. External parties
 - iii. Asset management
 - 1. Inventory of assets
 - 2. Information classification
 - iv. Human resources security
 - 1. Pre-employment
 - 2. Change of employment

- v. Physical and environmental security
 - 1. Securing facilities
 - 2. Equipment safety
- vi. Communications and operations management
 - 1. Management of third party service delivery
 - 2. System monitoring
 - 3. Back up media
 - 4. Transfer of information
 - 5. Digital signatures
 - a. Digital signature standard (“DSS”)
 - 6. Non-repudiation
- vii. Incident management
 - 1. Reporting events and weaknesses
 - 2. Business continuity
 - 3. Security in system files
 - 4. Development and support processes
- c. The information security program
 - i. Management responsibility and review
 - ii. Internal audits
 - iii. Program development and improvement

D. Common Information Security Techniques

- a. Audit trails, logging and monitoring
- b. Logical controls at each layer of the system architecture
 - i. Networks
 - 1. Firewalls
 - 2. Segmentation
 - 3. Virtual private networks (“VPN”)
 - 4. Intrusion detection systems (“IDS”)
 - 5. Intrusion prevention systems (“IPS”)
 - ii. Operating systems
 - 1. Access management
 - 2. IDS and IPS
 - iii. Middleware
 - 1. Databases
 - 2. Enterprise resource planning (“ERP”) systems
 - iv. Communications and transactions
 - 1. Transport layer security (“TLS”)
 - 2. Secure Sockets Layer (“SSL”)
 - 3. Payment Card Industry (“PCI”) Data Security Standard (“DSS”)
 - a. Cardholder data types
 - b. Applicability of PCI DSS
 - v. Portable devices and media
 - 1. Laptops and personal digital assistants (“PDAs”)
 - 2. Thumb-drives and flash drives

III. **Online Privacy: Using Personal Information on Web Sites and with Other Internet-related Technologies**

A. Introduction to Online Technologies

- a. Web protocols
 - i. Universal Resource Identifier (“URI”)

- ii. Internet Protocol (“IP”)
- iii. Hypertext Transfer Protocol (“HTTP”)
- iv. Hypertext Transfer Protocol-Secure (“HTTPS”)
- v. Internet proxies and caches

B. Privacy Considerations for Sensitive Information Online

- a. Online privacy threats
- b. Privacy notices and methods for communication
 - i. Web site privacy statement
 - 1. Location at / link from all points of data collection
 - 2. Machine-readable policies
 - a. Platform for Privacy Preferences Project (“P3P”) of the World Wide Web Consortium (“W3C”)
 - b. Compact policy
- c. Choice and consent
 - i. Data collection
 - ii. Secondary uses of data
 - iii. Mandatory versus optional information
- d. Data subject access and redress
- e. Web site security
 - i. End user authentication
- f. Active versus passive data collection
 - i. Web forms
- g. Online identification mechanisms
 - i. Cookie files
 - 1. First party versus third party
 - 2. Session-based versus persistent
 - 3. Common use cases
 - 4. Industry best practices
 - ii. Web beacons
- h. Web analytics
 - i. Web server logs
- i. Privacy and electronic mail
 - i. Spam and unsolicited commercial email
- j. Children’s online privacy
 - i. Age and consent considerations
- k. Online advertising
 - i. Search engine marketing
 - 1. Search term legacy data
- l. Online assurance
 - i. Trust seal and dispute resolution programs: TRUSTe, BBB Online
 - ii. Self-regulatory frameworks: the Network Advertising Initiative (“NAI”) Principles
 - iii. Other programs: EuroPrise