

U.S. Corporate Privacy Certification

Program Introduction



The IAPP is proud to offer the privacy profession's foremost credential, the **Certified Information Privacy Professional ("CIPP")**.

The CIPP is the first professional certification ever to be offered in information privacy. It assesses understanding of corporate compliance with major U.S. privacy laws and regulations plus a selection of European data protection requirements. The program establishes educational and testing standards for privacy and data protection and is the first program of its kind to formally recognize the privacy professional with a distinguished certificate of achievement.

The CIPP was developed by the IAPP in coordination with privacy leaders from Hewlett-Packard Company, Microsoft Corporation, the Ponemon Institute, Hunton & Williams, Nationwide Insurance Company, The Procter & Gamble Company, General Electric Company, Intuit, Inc., Privacy and Information Management Services P.C. and Corporate Privacy Group. The program is made possible through founding grants from Hewlett-Packard Company and Microsoft Corporation and is offered exclusively by the IAPP.

The CIPP made its official debut on October 24, 2004 at the IAPP Privacy Academy in New Orleans, Louisiana.

Who Should Apply

- Chief Privacy Officers ("CPOs") who serve U.S.-based corporate organizations or global multinationals and who seek independent validation of their privacy knowledge and skill set with a standardized credential
- U.S. corporate privacy managers chartered with elevating a variety of staff members to a consistent level of privacy education
- Intermediate-level privacy professionals and entry-level candidates who are transitioning from non-privacy roles inside U.S. corporate organizations or who are entirely new to the privacy profession
- Information management professionals in the U.S. financial services, healthcare, or telecommunications industries who seek to broaden their expertise into a general information privacy scope
- Information security professionals (CISO, CISSP)
- Information auditing and IT governance professionals (CISA, CISM)

Certification Requirements

In order to become CIPP-certified, candidates must complete and pass both the IAPP Certification Foundation Examination and the CIPP Examination (offered separately) for a grand total of three hours of testing. These examinations are offered exclusively by the IAPP. They are administered on-site at select conferences and testing events that are held throughout the United States and around the world each year.

- **First-time candidates for IAPP privacy certification** (e.g. individuals who do not presently hold any IAPP certification) must activate an IAPP membership at any level in advance of their test and then pass both the Certification Foundation Examination, a two-hour, three-part, 120-item, objective test and the CIPP Examination, a one-hour, two-part, 60-item, objective test.
- **Existing IAPP-certified professionals** (e.g. individuals who presently hold a CIPP/G, CIPP/C or CIPP/IT designation) are “grandfathered” into the Foundation testing requirement but must still meet the CIPP testing requirement by passing the CIPP Examination, a one-hour, one-part, 60-item, objective test.

“Successful completion” of CIPP is defined as an aggregate score of 70% or greater on each exam (as applicable under each scenario above). This means at least 84 out of 120 total points for Certification Foundation exam and at least 42 out of 60 total points for CIPP exam. Partial completion of either exam will result in no credential being awarded until such time that all requirements are met. The exams may be taken in sequence at the same sitting or separately at different testing events.

Upon successful completion of both of the above referenced examinations, the CIPP certification becomes active on the date of the most recent examination and remains in force annually provided that:

- (1) Once certified, the CIPP credential holder keeps the IAPP membership status current and in good standing each year; and,
- (2) Once certified, the CIPP credential holder also satisfies a minimum of 10 credit hours of continuing privacy education each year.

Continuing privacy education (“CPE”) is defined as any program, event, forum, book, presentation, speaking engagement or teaching engagement that relates in whole to information privacy, security, auditing, risk management or legal compliance whether provided by the IAPP or another sanctioning body. Specific guidelines on CPE-eligible programs and application processes are available for review under the “Continuing Education” section of the IAPP Web site at www.privacyassociation.org.

Course Format

The CIPP Common Body of Knowledge (“CBK”) is described on the following pages in outline form. The course consists of two sections:

- I. **U.S. Corporate Privacy Law and Compliance**
- II. **U.S. Corporate Privacy Practices**

Both course sections address concepts for corporate compliance with privacy and data protection laws and regulations across jurisdictions in the United States with some visibility into the data protection laws and standards now in force across the European Union specifically with regard to trans-border flows of personal data.

Course References

Training for CIPP certification is optional and available through the IAPP Certification Foundation Training Workshop and the CIPP Training Workshop for a grand total of seven hours of instruction. Each of these courses is available for purchase online (as a CD-ROM courseware package) as well as on-site (as live classroom sessions at select IAPP conferences and partner events).

Additional CIPP reference materials include:

- Chapters I, II, III and VI from [“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. Now available at U.S.\$65 per copy plus shipping.
- All chapters 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 soon at U.S.\$65 per copy plus shipping.

U.S. Corporate Privacy Certification

Outline of the Common Body of Knowledge (“CBK”) for the Certified Information Privacy Professional (“CIPP”)



I. U.S. Privacy and Security Laws: Regulatory Requirements and Enforcement

A. Introduction to the U.S. Legal System

- a. Branches of government
- b. Legal definitions
 - i. Contract law
 - ii. Jurisdiction
 - iii. Person
 - iv. Preemption
 - v. Private right of action
- c. Regulatory authorities
 - i. Federal Trade Commission (“FTC”)
 - ii. Federal Communications Commission (“FCC”)
 - iii. Department of Commerce (“DoC”)
 - iv. Department of Health and Human Services (“HHS”)
 - v. Banking regulators
 - 1. Federal Reserve Board
 - 2. Comptroller of the Currency
 - vi. State attorneys general
- d. Sources of law
 - i. Constitutions
 - ii. Legislation
 - iii. Regulations and rules
 - iv. Case law
 - v. Common law
- e. Understanding laws
 - i. Scope and Application
 - ii. Analyzing a law
 - iii. Determining jurisdiction
 - iv. Preemption

B. Specific U.S. Privacy and Security Laws

- f. Federal laws
 - i. Personal data protection laws
 - 1. The Fair Credit Reporting Act of 1970 (“FCRA”) and the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”)
 - 2. The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
 - a. HIPAA privacy rule
 - b. HIPAA security rule
 - 3. The Financial Services Modernization Act of 1999 (“Gramm-Leach-Bliley” or “GLBA”)
 - a. GLBA privacy rule
 - b. GLBA safeguards rule
 - 4. The Children’s Online Privacy Protection Act of 2000 (“COPPA”)
 - ii. Laws regulating marketing activities
 - 1. Telemarketing sales rules (“TSR”) and the Telephone Consumer Protection Act of 1991 (“TCPA”)
 - a. The Do-not-call registry (“DNC”)
 - 2. Combating the Assault of Non-solicited Pornography and Marketing Act of 2003 (“CAN-SPAM”)
 - 3. The Junk Fax Prevention Act of 2003 (“JFPA”)
 - iii. Laws that compel disclosure of personal information
- g. State laws
 - i. Marketing laws
 - ii. Security laws including secure disposal and SSN regulation
 - iii. Security breach notification laws
 - 1. California SB-1386
 - 2. Key differences among states today
 - iv. California SB-1

II. **U.S. Corporate Compliance: Practical Aspects of Privacy and Security**

A. Privacy in the U.S. Workplace

- a. Workplace privacy concepts
- b. U.S. / E.U. contrasts for workplace data processing
- c. U.S. agencies regulating workplace privacy issues
 - i. Federal Trade Commission (“FTC”)
 - ii. Department of Labor
 - iii. Equal Employment Opportunity Commission (“EEOC”)
 - iv. National Labor Relations Board (“NLRB”)
 - v. Occupational Safety and Health Administration (“OSHA”)
 - vi. Securities and Exchange Commission (“SEC”)
- d. U.S. Anti-discrimination laws
 - i. The Civil Rights Act of 1964 and the Americans with Disabilities Act (“ADA”)
- e. Employee background screening
 - i. FCRA requirements
 - ii. Polygraph testing
 - iii. Drug and alcohol testing
 - iv. Genetic testing
- f. Workforce and workplace monitoring
 - i. Telephone
 - ii. Video
 - iii. Electronic mail

- iv. Computer usage
 - g. Investigation of employee misconduct
 - i. Data handling in misconduct investigations
 - ii. Use of third parties in investigations
 - iii. Documenting performance problems
 - iv. Balancing rights of multiple individuals in a single situation
 - h. Termination of the employment relationship
 - i. Transition management, records retention and references
- B. Enforcement of U.S. Privacy and Security Laws
 - a. General theories of legal liability
 - i. Contract
 - ii. Tort
 - iii. Civil enforcement
 - b. Criminal versus civil liability
 - c. Negligence
 - d. Unfair and deceptive trade practices (“UDTP”)
 - e. Enforcement action basics
 - f. Settlement and agreement terms
- C. Data Management and Standard Practices: The U.S. Legal Perspective
 - h. Data classification
 - i. Privacy program development
 - j. Incident response programs
 - k. Vendor management
 - l. International data transfers
 - i. Key considerations for U.S.-based global multinational companies
 - m. Resolving multinational compliance conflicts
 - i. E.U. data protection versus e-Discovery