STUDY GUIDE

iapp

Certified Information Privacy Professional/ United States

Effective September 2024

WELCOME

Congratulations on taking the first step toward achieving an IAPP privacy certification. This study guide contains the basic information you need to get started, including:

- Key areas of knowledge for the CIPP/US exam.
- Recommended steps to help you prepare for your exam.
- An outline of the body of knowledge for the CIPP/US program.
- An exam blueprint.
- Example questions.
- General exam information.
- An explanation of the IAPP certification program structure.

CIPP/US key areas of knowledge

The Certified Information Privacy Professional/United States certification launched in October 2004 as the first professional certification ever to be offered in information privacy. The CIPP/US credential demonstrates a strong foundation in U.S. privacy laws and regulations and understanding of the legal requirements for the responsible transfer of sensitive personal data to/from the U.S., the EU and other jurisdictions.

Subject matter areas covered include:

- The U.S. legal system: definitions, sources of law and sectoral model for privacy enforcement.
- U.S. federal laws for protection of personal data: FCRA and FACTA, HIPAA, GLBA, COPPA and DPPA.
- U.S. federal regulation of marketing practices: TSR, DNC, CAN-SPAM, TCPA and JFPA.
- U.S. state data breach notification and select state laws.
- Regulation of privacy in the U.S. workplace: FCRA, EPP, ADA and ECPA plus best practices for privacy and background screening, employee testing, workplace monitoring, employee investigation and termination of employment.

Preparation

Privacy certification is an important effort that requires advance preparation. Deciding how you will prepare for your exams is a personal choice that should include an assessment of your professional background, scope of privacy knowledge and your preferred method of learning.

In general, the IAPP recommends you plan for a minimum of 30 hours of study time in advance of your exam date. However, you might need more or fewer hours depending on your personal choices and professional experience.

You can read more about preparation suggestions and resources on our website.

The IAPP recommends you prepare in the following manner:

1. Review the body of knowledge

The body of knowledge for the CIPP/US program is a comprehensive outline of the subject matter areas covered by the CIPP/US exam. Review it carefully to help determine which areas merit additional focus in your preparation. See pages 5.

2. Review the exam blueprint

The CIPP/US exam blueprint on page 6-8 specifies the number of items from each area of the body of knowledge that will appear on the exam. Studying the blueprint can help you further target your primary study needs.

3. Study the CIPP/US textbook

"U.S. Private-sector Privacy: Law and Practice for Information Privacy Professionals" is the authoritative reference for the CIPP/US exam. The IAPP strongly recommends you take the time to carefully read and study it. Print and digital versions of the textbook are available through the IAPP store.

4. Get certification training

The IAPP offers in-person, live online and self-paced online training to help you prepare for your exams. You can find a list of scheduled trainings or purchase self-paced online training in the IAPP store.

5. Take the CIPP/US practice exam

IAPP practice exams provide insight into how you might perform on your certification exam. Practice exams consist of 90 questions in the same format as official certification exams. The questions are developed by IAPP-selected experts to match the depth and rigor of the actual exam.

6. Review other IAPP preparation resources

Additional resources are available on the IAPP website, including a searchable glossary of terms.

CIPP/US body of knowledge outline

I. Introduction to the U.S. Privacy Environment

A. Structure of U.S. Law
B. Enforcement of U.S. Privacy and Security Laws
C. Information Management from a U.S. Perspective

II. Limits on Private-sector Collection and Use of Data

A. Cross-sector FTC Privacy Protection
B. Healthcare/Medical
C. Financial
D. Education
E. Telecommunications and Marketing

III. Government and Court Access to Private-sector Information

A. Law Enforcement and Privacy
B. National Security and Privacy
C. Civil Litigation and Privacy

IV. Workplace Privacy

A. Introduction to Workplace Privacy
B. Privacy Before, During and After Employment

V. State Privacy Laws

A. Federal vs. State Authority
B. Data Privacy and Security Laws
C. Data Breach Notification Laws

CIPP/US exam format

The CIPP/US is a 2.5 hour exam composed of 90 items. Most of the items are multiple choice, including both single, stand-alone questions and others associated with case studies. There are no essay questions. Each correct answer is worth one point.

Exam blueprint

The exam blueprint indicates the minimum and maximum number of items included on the CIPP/US exam from the major areas of the body of knowledge. Questions may be asked from any of the topics listed under each area. You can use this blueprint to guide your preparation.

		Min	Max
I.	**Introduction to the U.S. Privacy Environment**	**27**	**35**
A.	Structure of U.S. Law Branches of government, sources of law, legal definitions, regulatory authorities, understanding laws	4	6
B.	Enforcement of U.S. Privacy and Security Laws Criminal vs. civil liability, general theories of legal liability	5	7
C.	Information Management from a U.S. Perspective Data inventory and classification, data flow mapping, privacy program development, managing user preferences, incident response programs, workforce training, accountability, data and records retention and disposal (FACTA), online privacy, privacy notices, vendor management, international data transfers and Schrems decisions, other key considerations for U.S.-based multinational companies (including GDPR requirements, APEC), resolving multinational compliance conflicts	18	22
II.	**Limits on Private-sector Collection and Use of Data**	**15**	**25**
A.	Cross-sector FTC Privacy Protection The FTC Act, FTC privacy enforcement actions, FTC security enforcement actions, COPPA, future of federal enforcement	5	7
B.	Healthcare/Medical HIPAA, HITECH, GINA, the 21st Century Cures Act of 2016, Confidentiality of Substance Use Disorder Patient Records Rule	4	6
C.	Financial FCRA, FACTA, GLBA, Red Flags Rules, Dodd-Frank, CFPB, online banking	4	6
D.	Education FERPA, education technology	1	3
E.	Telecommunications and Marketing	1	3

		Min	Max
III.	**Government and Court Access to Private-sector Information**	**3**	**7**
A.	Law Enforcement and Privacy Access to financial data, access to communications, CALEA	1	3
B.	National Security and Privacy FISA, USA-Patriot Act, USA Freedom Act, Cybersecurity Information Sharing Act (CISA)	1	2
C.	Civil Litigation and Privacy Compelled disclosure of media information, electronic discovery	1	2
IV.	**Workplace Privacy**	**5**	**9**
A.	Introduction to workplace privacy Workplace privacy concepts, U.S. agencies regulating workplace privacy issues, U.S. anti-discrimination laws	2	4
B.	Privacy before, during and after employment Automated employment decision tools and potential for bias, employee background screening, employee monitoring, investigation of employee misconduct, termination of employment relationship, working with third parties	3	5
V.	**State Privacy Laws**	**9**	**15**
A.	Federal vs. state authority State attorneys general, California Privacy Protection Agency (CPPA)	1	3
B.	Data privacy and security laws Applicability, data subject rights, privacy notice requirements, data security requirements, data protection agreements, data protection assessments/risk assessments, health data rules, data retention and destruction, selling and sharing of personal information, enforcement, cookie and online tracking regulations, facial recognition use restrictions, biometric information privacy regulations, AI bias laws, important comprehensive data privacy laws	6	8
C.	Data breach notification laws Elements of, key differences among states, significant developments	2	4

Example questions

1. What does data classification **mainly** enable an organization to do?
   A. Review and update its database.
   B. Evaluate data by level of sensitivity.
   C. Easily extract information from its database.
   D. Achieve compliance with rules for cross-border data flow.

2. Under the Children's Online Privacy Protection Act, which is an accepted means for an organization to validate parental consent when it intends to disclose a child's information to a third party?
   A. Email a consent form and the parent can provide consent by responding to the email.
   B. Email a consent form and the parent can provide consent by signing and mailing back the form.
   C. Email a consent form and request that the parent provide a mailing address or phone number for additional contact.
   D. Email a consent form to the parent allowing 30 days to object to the data disclosure.

3. All of the following are considered acceptable lines of questioning by U.S. employers to applicants in the pre-employment process except:
   A. Questions about the applicant's duration of stay on the job or any anticipated absences.
   B. Questions regarding any medical conditions or disabilities that would inhibit the performance of the job function.
   C. Questions on whether an applicant has applied for or received worker's compensation.
   D. Questions about the applicant's height or weight as this relates to a specific job function.

See page 10 for answers.

General exam information

The IAPP offers testing via computer-based delivery at more than 6,000 testing locations worldwide, or you can take your certification exam from home with online proctoring. Remote proctoring is currently available for in-language exams but requires enough knowledge of English to communicate with exam proctors.

You can find detailed information about how to register for exams, as well as exam-day instructions, in the IAPP Certification Information Candidate Handbook on our website.

Questions?

The IAPP understands that privacy certification is an important professional development effort requiring commitment and preparation. We thank you for choosing to pursue certification, and we welcome your questions and comments.

Please don't hesitate to contact us at certification@iapp.org.

Example questions: Answers

1. What does data classification **mainly** enable an enterprise to do?
   A. Review and update its database.
   B. Evaluate data by level of sensitivity.
   C. Easily extract information from its database.
   D. Achieve compliance with rules for cross-border data flow.

2. Under the Children's Online Privacy Protection Act, which is an accepted means for an enterprise to validate parental consent when it intends to disclose a child's information to a third party?
   A. Email a consent form and the parent can provide consent by responding to the email.
   B. Email a consent form and the parent can provide consent by signing and mailing back the form.
   C. Email a consent form and request that the parent provide a mailing address or phone number for additional contact.
   D. Email a consent form to the parent allowing 30 days to object to the data disclosure.

3. All of the following are considered acceptable lines of questioning by U.S. employers to applicants in the pre-employment process except:
   A. Questions about the applicant's duration of stay on the job or any anticipated absences.
   B. Questions regarding any medical conditions or disabilities that would inhibit the performance of the job function.
   C. Questions on whether an applicant has applied for or received worker's compensation.
   D. Questions about the applicant's height or weight as this relates to a specific job function.

The IAPP certification program structure

The IAPP currently offers three certifications: the Artificial Intelligence Governance Professional, the Certified Information Privacy Professional, the Certified Information Privacy Manager and the Certified Information Privacy Technologist.

AIGP certification demonstrates comprehension of AI systems and the ability to deploy AI in a manner that abates risk and ensures safety and trust. It confirms an understanding of AI ecosystems, identification and mitigation of bias, and the capability to effectively communicate best practices for responsible AI management.

CIPP certification demonstrates a mastery of data privacy laws and regulations and how to apply them: jurisdictional laws, regulations and enforcement models, plus legal requirements for handling and transferring data. Within the CIPP, there are four concentrations:

Asian privacy (CIPP/A).
Canadian privacy (CIPP/C).
European data protection (CIPP/E).
U.S. private-sector privacy (CIPP/US).

CIPM certification demonstrates understanding of implementing privacy regulatory requirements in day-to-day operations. It confirms the ability to create a company vision, structure a data protection team, develop and implement system frameworks, communicate to stakeholders and measure performance.

CIPT certification demonstrates a deep understanding of privacy's role in technology, including building privacy-friendly products, service and systems; deploying emerging technologies while respecting consumer privacy; establishing privacy practices for data security and control.

There are no concentrations within the CIPM or CIPT — they cross all jurisdictions and industries.

Requirements for IAPP certification

1. You must pay a two-year certification maintenance fee of USD250. If you are not an IAPP member, we recommend purchasing the certification maintenance fee at the time of your exam purchase so it will activate automatically upon passing the exam.

   OR

   You can become a member of the IAPP with access to numerous benefits, like discounts, networking opportunities, members-only resources and more, for just USD295 annually, which includes your maintenance fee.

2. You must meet the annual continuing privacy education requirements of 20 credits in order to keep your certification active.

More information about IAPP membership, including levels, benefits and rates, is available on the IAPP website.