

CERTIFICATION EXAMINATION BLUEPRINT



U.S. Private-sector Privacy Certification

Examination Blueprint for the Certified Information Privacy Professional/United States (CIPP/US™)



The examination blueprint indicates the minimum and maximum number of question items that are included on the CIPP/US examination from the major areas of the Body of Knowledge. Questions may be asked from any of the listed topics under each area. You can use this blueprint to guide your preparation for the CIPP/US examination.

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 21 st 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



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