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. For example, over half of the questions on the CIPP/US examination come from domains I and II.

I. Introduction to the U.S. Privacy Environment	**28**	**34**
A. Structure of U.S. Law Branches of government, sources of law, legal definitions, regulatory authorities, understanding laws	6	9
B. Enforcement of U.S. Privacy and Security Laws Criminal vs. civil liability, general theories of legal liability	3	5
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 retention and disposal (FACTA), online privacy, privacy notices, vendor management, international data transfers, 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	**20**	**24**
A. Cross-sector FTC Privacy Protection The FTC Act, FTC privacy enforcement actions, FTC security enforcement actions, COPPA, future of federal enforcement	2	4
B. Healthcare HIPAA, HITECH, GINA, The 21st Century Cures Act of 2016, Confidentiality of Substance Use Disorder Patient Records Rule	5	7
C. Financial FCRA, FACT Act, GLBA, Red Flags Rules, Dodd-Frank, CFPB, online banking	5	7
D. Education FERPA, education technology	0	2

	E. Telecommunications and Marketing	5	7
III.	**Government and Court Access to Private-sector Information**	**6**	**8**
	A. Law Enforcement and Privacy Access to financial data, access to communications, CALEA	3	5
	B. National Security and Privacy FISA, USA-Patriot Act, USA Freedom Act, Cybersecurity Information Sharing Act (CISA)	1	3
	C. Civil Litigation and Privacy Compelled disclosure of media information, electronic discovery	0	2
IV.	**Workplace Privacy**	**8**	**12**
	A. Overview of workplace privacy Workplace privacy concepts, U.S. agencies regulating workplace privacy issues, U.S. anti-discrimination laws	3	5
	B. Privacy before, during and after employment Employee background screening, employee monitoring, investigation of employee misconduct, termination of employment relationship, working with third parties	5	7
V.	**State Privacy Laws**	**5**	**7**
	A. Federal vs. state authority	0	2
	B. Marketing laws	0	2
	C. Financial data	0	2
	D. Data security laws	0	2
	E. Data breach notification laws Elements of, key differences among states, recent developments	1	3