

IT Privacy Certification

Examination Blueprint for the Certified Information Privacy Technologist (CIPT™)



The examination blueprint indicates the minimum and maximum number of question items that are included on the CIPT 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 CIPT examination. For example, questions from domains III, IV, and VI will likely comprise 60% of the exam.

I. Understanding the need for privacy in the IT environment	8	14
A. Evolving Compliance Requirements GDPR considerations	1	3
B. Major risks to a company's IT framework Client-side, server-side, application, personnel, network, storage, mistakes organizations make	2	4
C. Stakeholder expectations for Privacy	2	3
D. Privacy vs. Security IT governance vs. data governance, the role of the IT professional and other players in preserving privacy	3	4
II. Core Privacy Concepts	8	14
A. Foundational Elements for Embedding Privacy in IT Privacy notices, privacy policies, data classification policies, common IT frameworks, incident response, SDLC process, cross-border transfers, PIAs	5	9
B. Common Privacy Principles Collection limitation, data quality, use limitation, security safeguards, openness, accountability	3	5
III. Privacy Considerations in the Information Life Cycle	16	27
A. Collection Notice, choice/consent, collection limitations, secure transfer, collection from third parties	4	6
B. Use Compliance with regulation, data minimization, secondary uses, user authentication, using PII in testing	3	5
C. Disclosure	3	5

According to notice, anonymize, minimize, define limitations,
vendor management programs

D. Retention	4	8
Working with records management, regulatory limitations, providing data subject access, secure storage and archiving		
E. Destruction	2	3
Digital, portable media, hard copy, identifying appropriate time		

IV. Privacy in Systems and Applications	13	24
--	-----------	-----------

A. The Enterprise IT Environment--Common Challenges	2	4
Architecture considerations, mergers and acquisitions		
B. Identity and Access Management	2	3
Principle of least privilege required, role-based and user-based access controls, cross-enterprise authentication		
C. Credit Card Information and Processing	1	3
Application of Payment Card Industry Data Security Standard (PCI DSS)		
D. Remote Access, Telecommuting, and Bringing Devices to Work	2	3
Privacy and security considerations, device, network, and architecture controls		
E. Data Encryption	3	5
Regulations and standards, file and disk encryption, application or field encryption		
F. Other Privacy-Enhancing Technologies	1	3
Data masking and obfuscation, data loss prevention, automated system audits		
G. Customer-Facing Applications	2	3
Software-based notice and consent, agreements		

V. Privacy Techniques	5	13
------------------------------	----------	-----------

A. Authentication Techniques	2	5
User name and password, single and multi-factor authentication		
B. Identifiability	2	5
Labels that point to individuals, weak and strong identifiers, pseudonymous and anonymous data, degrees of identifiability (including considerations in Europe and in the U.S.)		
C. Privacy by Design	1	3
Overview of Principles		

VI. Online Privacy Issues	11	22
----------------------------------	-----------	-----------

A. Specific Requirements for the Online Environment	2	4
Regulatory requirements, children's online privacy		
B. Social Media	2	3
Personal information shared and collected, chatbots		
C. Online Threats	2	3
Phishing, SQL injection, cross-site scripting, spam, ransomware, safeguards		
D. Online Advertising	1	3
E. Tracking Technologies	2	3
Cookies, beacons, responsible practices		
F. Web Browser Privacy and Security	1	3
Tracking Protection, do not track		
G. Web Security Protocols	1	3
HTTPS, SFTP, FTPS		

VII. Technologies with Privacy Considerations	8	17
A. Cloud Computing	2	5
Types of clouds, privacy and security concerns		
B. Wireless IDs	2	3
Bluetooth, Wi-Fi, cell phones and tablets		
C. Location-based Services	1	2
Overview of Principles		
D. Smart Technologies	1	3
Data analytics, deep learning, Internet of Things (IOT), vehicular automation		
E. Video/data/audio surveillance	1	2
Drones		
F. Biometrics	1	2