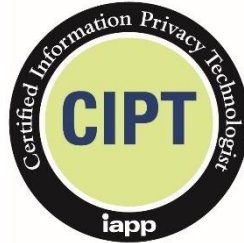


Privacy Technology Certification

Outline of the Body of Knowledge (BOK) for the Certified Information Privacy Technologist (CIPT)



I. Foundational Principles

- A. General Understanding of Privacy Risk Models and Frameworks and their Roles in Laws and Guidance
 - a. FIPPs and OECD Principles
 - b. Privacy frameworks (e.g., NIST/NICE, ISO/IEC 27701 and BS100112 Privacy Information Management System)
 - c. Nissenbaum's Contextual Integrity
 - d. Calo's Harms Dimensions
 - e. FAIR (Factor Analysis in Information Risk)
- B. General Understanding of Privacy by Design Principles
 - a. Full Life Cycle Protection
 - b. Embedded into Design
 - c. Full Functionality
 - d. Visibility and Transparency
 - e. Proactive not Reactive
 - f. Privacy by Default
 - g. Respect for Users
- C. General Understanding of Privacy-related Technology Fundamentals
 - a. Risk concepts (e.g., threats, vulnerability)
 - b. Data/security incidents vs. personal data/privacy breaches
 - c. Privacy and security practices within an organization
 - d. Understanding how technology supports information governance in an organization
 - e. External Data Protection and Privacy notices
 - f. Internal Data Protection and Privacy guidelines, policies and procedures
 - g. Third-party contracts and agreements
 - h. Data inventories, classification and records of processing
 - i. Enterprise architecture and data flows, including cross-border transfers
 - j. Data Protection and Privacy impact assessments (DPIA/PIAs)
 - k. Privacy related Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs)
- D. General Understanding of the Data Life Cycle
 - a. Collection



- b. Use
- c. Disclosure
- d. Transfer
- e. Retention
- f. Destruction

II. The Privacy Technologist’s Role in the Context of the Organization

A. General responsibilities

- a. Understanding various roles within the privacy team (e.g., DPO, CPO, legal compliance, security)
- b. Implementing industry Privacy Standards and Frameworks
- c. Translating legal and regulatory requirements into practical technical and/or operational solutions
- d. Consulting on internal privacy notices and external privacy policies
- e. Consulting on contractual and regulatory requirements

B. Technical Responsibilities

- a. Advising on technology elements of privacy and security practices
- b. Advising on the privacy implications of new and emerging technologies
- c. Implementing privacy and security technical measures
- d. Implementing and developing privacy-enhancing technologies and tools
- e. Advising on the effective selection and implementation during acquisition of privacy impacting products
- f. Advising on privacy by design and security and privacy impact assessments in systems development
- g. Handling individuals’ rights requests (e.g., access, deletion)
- h. Supporting records of processing activities (RoPA), automation of inventory and data flow mapping
- i. Reviewing security incidents/investigations and advising on breach notification
- j. Performing and supporting IT privacy oversights and audits including 3rd party assessment
- k. Developing, compiling and reporting Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs)

III. Privacy Risks, Threats and Violations

A. Data Ethics

- a. Legal versus Ethical (e.g., when working with countries that lack privacy laws)
- b. Moral issues (e.g., gaining access to sensitive personal information through illegal means and using information for personal advantage)
- c. Societal issues (e.g., manipulating societal conversations and attitudes on controversial topics)
- d. Bias/discrimination (e.g., incorporating personal preference into data decisions)

B. During Data Collection



- a. Asking individuals to reveal personal information
 - b. Tracking and surveillance (e.g., geo-tagging, geo-social patterns)
 - c. Lack of informed consent
 - d. Automatic collection
 - e. Inaccuracies
 - f. Extracting from publicly available sources
 - g. Jurisdictional implications (e.g., localization, government access)
- C. During Data Use
- a. Insecurity
 - b. Identification/re-identification
 - c. Aggregation
 - d. Secondary Use
 - e. Exclusion
 - f. Profiling
- D. During Data Dissemination
- a. Disclosure
 - b. Distortion
 - c. Exposure
 - d. Breach of Confidentiality (personal data breaches)
 - e. Increased accessibility
 - f. Blackmail
 - g. Appropriation
- E. Intrusion, Decisional Interference and Self-Representation
- a. Behavioral advertising
 - b. Cyberbullying
 - c. Social engineering
 - d. Blackmail
 - e. Dark patterns
- F. Software Security
- a. Vulnerability management
 - b. Intrusion detection and prevention
 - c. Change management (e.g., patches, upgrades)
 - d. Open-source vs Closed-source
 - e. Possible violations by service providers

IV. Privacy-Enhancing Strategies, Techniques and Technologies

- A. Data Oriented Strategies
- a. Separate
 - b. Minimize
 - c. Abstract
 - d. Hide
- B. Process Oriented Strategies
- a. Informing the Individual
 - b. User Control
 - c. Policy and Process Enforcement

d. Demonstrate Compliance

C. Techniques

- a. Aggregation
- b. De-identification
- c. Anonymization
- d. Pseudonymization

- e. Encryption
- f. Identity and access management
- g. Authentication
- h. Technology implications of Privacy Regulations and Techniques needed for:
 - i. Processing/verification of Individual Rights Request (IRR)
 - ii. Ability for record processing activities related to customer data
 - iii. Notice and Consent; obligations management
 - iv. Retention Requirements
 - v. Privacy Incident Reporting

V. Privacy Engineering

A. The Privacy Engineering role in the organization

- a. Effective Implementation
- b. Technological Controls
- c. Protecting Privacy during the Development Lifecycle

B. Privacy Engineering Objectives

- a. Predictability
- b. Manageability
- c. Disassociability

C. Privacy Design Patterns

- a. Design patterns to emulate
- b. Dark patterns to avoid

D. Privacy Risks in Software

- a. Controls/countermeasures

VI. Privacy by Design Methodology

A. The Privacy by Design Process

- a. Goal Setting
- b. Documenting Requirements
- c. Understanding quality attributes
- d. Identify information needs
- e. Privacy risk assessment and analysis
- f. High-level design
- g. Low-level design and implementation
- h. Impose controls
 - i. Architect



- ii. Secure
- iii. Supervise
- iv. Balance
- i. Testing and validation
- B. Privacy Interfaces and User Experience
 - a. Design Effects on User Behavior
 - b. UX Design and Useability of privacy-related functions
 - c. Privacy Notices, Setting and Consent Management
 - d. Usability Testing
- C. Value Sensitive Design
 - a. How Design Affects Users
 - b. Strategies for Skillful Practice
- D. Ongoing Vigilance
 - a. Privacy audits and IT control reviews
 - b. Code reviews
 - c. Code audits
 - d. Runtime behavior monitoring
 - e. Software evolution
 - f. Data cleansing in production and non-production environments

VII. Evolving or Emerging Technologies in Privacy

- A. Robotics and Internet of Things (IoT)
 - a. Mobile phones
 - b. Wearable devices
 - c. Edge Computing
 - d. Smart homes and cities (e.g., CCTV and tracking/surveillance)
 - e. Robots
 - f. Drones
- B. Internet/eCommerce
 - a. Adtech
 - b. Cookies and other webtracking technologies
 - c. Alerts and notifications
 - d. Location tracking
 - e. Chatbots
 - f. Online/mobile payments
- C. Biometrics
 - a. Facial recognition
 - b. Speech recognition
 - c. Fingerprint ID
 - d. Behavioral profiling
- D. Corporate IT Services
 - a. Shared Data centers
 - b. Cloud-based infrastructure



- c. Third-party vendor IT solutions
- d. Remote working
- e. Video calls and conferencing

E. Advanced Computing

- a. Data Management and Analytics
- b. Artificial Intelligence
- c. Quantum computing
- d. Blockchain
- e. Cryptocurrencies
- f. Non-fungible tokens (NFT)
- g. Machine and Deep Learning

F. Social Networks

- a. Social media
- b. Messaging and video calling
- c. Virtual/Augmented reality