IAPP CIPT Class Outline

Module 1: Foundational principles

1. The data life cycle (8)
2. Privacy by Design (23)
3. Risk models and frameworks (30)
4. Value-sensitive design (39)

Module 2: The role of the technology professional in privacy

1.The privacy responsibilities of the technology professional (50)
2. Fundamentals of privacy-related IT: policies and procedures (58)
3. Fundamentals of privacy-related IT: contracts and assessments (65)
4. Information security (71)

Module 3: Privacy threats and violations

1. Data Collection (83)
2. Data use (89)
3. Data dissemination (95)
4. Interference (104)
5. Software security (110)

Module 4: Technical measures and privacy-enhancing technologies

1. Strategies and techniques for protecting privacy (part 1) (117)
2. Strategies and techniques for protecting privacy (part 2) (124)
3. Process-oriented strategies (140)
4. Data-oriented strategies

Module 5: Privacy-by-design methodology

1. The privacy-by-design process (156)
2. Ongoing vigilance (169)

Module 6: Privacy engineering

1. The privacy engineering role in the organization (177)
2. Privacy engineering objectives (181)
3. Privacy design patterns (188)

Module 7: Technology challenges for privacy

1. Automated decision making (199)
2. Tracking and surveillance (205)
3. Anthropomorphism (214)
4. Ubiquitous computing (221)
5. Mobile Social Computing (230)

IAPP CIPT BODY OF KNOWLEDGE

Certified Information Privacy Technologist

Domain I — The privacy technologist's role in the context of the organization

This domain addresses the general and technical responsibilities inherent to the role of the Privacy Technologist.

I.A Identify and implement legal and procedural roles and responsibilities.

1. Understand various roles and responsibilities related to the privacy function (e.g., Data Governance, [DPO, Data Owner, Data Steward, Data Custodian], legal compliance, cybersecurity).
2. Translate legal and regulatory requirements into practical technical and/or operational solutions.
3. Implement internal and external data protection and privacy notices, policies, guidelines and procedures.

I.B Identify and implement technical roles and responsibilities.

1. Oversee technical elements of privacy operations and audits including third-party assessments.
2. Provide technical privacy support to identify and respond to privacy breaches and other types of incidents.
3. Understand risk concepts (e.g., threat, vulnerability, attack, security exploit).

I.C Demonstrate knowledge of privacy risk models and frameworks and their roles in legal requirements and guidance.

1. Apply common privacy risk models and frameworks (e.g., Nissenbaum's Contextual Integrity, Calo's Harms Dimensions, Factor Analysis in Information Risk (FAIR) model, NIST/NICE framework, FIPPS, OECD principles).
2. Understand and apply common privacy threat models and frameworks (e.g., LINDDUN and MITRE PANOPTIC™).

I.D Understand the connection between data ethics and data privacy.

1. Differentiate legal versus ethical processing of personal data (e.g., when comparing different jurisdictions).
2. Understand the social and ethical issues when advising on privacy impacting designs and technologies (e.g., unlawful or unauthorized access to personal data, manipulating societal conversations and attitudes on controversial topics).
3. Identify and minimize bias/discrimination when advising/designing tools with automated decision-making (e.g., incorporating personal preference into data decisions).

Domain II — Data collection, use, dissemination and destruction

This domain covers strategies and best practices to ensure responsible and secure processing of personal information, minimizing privacy risks during personal data collection, use, dissemination, retention and destruction.

II.A Demonstrate how to minimize privacy risk during personal data collection.

1. Understand and apply requirements to provide data subjects with control over the processing of their personal data including consent requirements for personal data collection, use, disclosure, and retention (e.g., clear and accessible privacy notices, settings, dashboards, other consent management mechanisms).
2. Implement measures to manage privacy risks associated with automatic collection of personal data.
3. Leverage techniques to minimize risk when extracting personal data from publicly available sources.
4. Practice appropriate data retention and destruction techniques.

II.B Demonstrate how to minimize privacy risk during personal data use.

1. Practice appropriate data minimization techniques (e.g., abstract personal data for a specific use case).
2. Implement data processing segregation.

3. Use data analysis and other procedures to minimize privacy risk associated with the aggregation of
personal data.
4. Employ appropriate privacy-enhancing techniques (e.g., anonymization, pseudonymization, differential privacy) to reduce risk exposure.
5. Use technical approaches that minimize the risks associated with secondary uses of personal data (e.g., profiling).

II.C Demonstrate how to minimize privacy risk during personal data dissemination.

1. Use technical approaches that minimize risks associated with disclosure and accessibility.
2. Leverage approaches and techniques that minimize the threat of:
   a. Data distortion.
   b. Data exposure.
   c. Breach of confidentiality (personal data breaches).
   d. Blackmail.
   e. Appropriation.
3. Implement other defense in-depth techniques (e.g., identity and access management, authentication mechanisms) to protect personal data from risk exposure.

Domain III: Privacy risk management

This domain addresses the critical connection between data ethics and privacy, gaining insights into the ethical
considerations that underpin responsible data handling. This domain covers strategies and best practices to ensure responsible and secure processing of personal information, minimizing privacy risks during personal data collection, use and dissemination, as well as addressing concerns on intrusion, decisional interference and software security.

III.A Demonstrate how to minimize the threat of intrusion and decisional interference.

1. Implement technical approaches that minimize the risks of various types of interference (e.g., behavioral
advertising, behavioral profiling, cyberbullying, social engineering).
2. Avoid the use of dark patterns that limit privacy-preserving response options, and recognize which design patterns to emulate.

III.B Identify privacy risks related to software security.

1. Implement measures to detect and fix software privacy vulnerabilities.
2. Leverage intrusion detection and prevention tools and techniques.
3. Implement measures to reduce privacy risks during change management (e.g., patches, upgrades).
4. Recognize possible privacy violations by service providers.

III.C Understand the privacy risks and impact of techniques that enable tracking and surveillance.

1. Understand the privacy risks and impact associated with e-commerce (e.g., behavioral advertising, cookies, chatbots, payments, behavioral profiling).
2. Demonstrate knowledge of the privacy risks and impact of audio and video surveillance, including those involved in wearables and IoT technologies (e.g., smart home devices and IoT technology for smart cities).
3. Understand privacy issues around biometrics (e.g., facial recognition, speech recognition, fingerprint identification, DNA).
4. Demonstrate knowledge of the privacy risks and impacts of location tracking.

5. Demonstrate knowledge of the privacy risks and impacts of internet monitoring and web tracking.

III.D Understand the privacy risks and impact involved when using workplace technologies.

1. Identify and minimize privacy risks involved when using artificial intelligence, machine learning and
   deep learning.
2. Identify and minimize privacy risk involved in the use of communications technologies (e.g., video calls
   and conferencing, messaging, mobile devices, social media, gaming platforms).

III.E Demonstrate how to monitor and manage privacy risk

1. Conduct privacy audits and IT control reviews.
2. Develop, compile, report, and monitor privacy Key Risk Indicators and Key Performance Indicators.
3. Complete privacy and data protection impact assessments.

Domain IV – Privacy by design

This domain focuses on the strategic integration of principles to effectively manage privacy risks within user experiences, implement value sensitive design practices, and establish robust management and monitoring controls for comprehensive privacy governance.

IV.A Implement privacy by design principles.

1. Understand and apply the seven privacy by design principles.
2. Define and communicate privacy goals and objectives to guide privacy by design within anorganization.
3. Interpret high-level specifications and align them via low-level specifications with the privacy by design principles.

IV.B Evaluate privacy risks in user experiences.

1. Understand and apply UX concepts, including how UX decisions impact user behavior.
2. Perform usability testing where relevant to assess effectiveness of privacy-related functions.
3. Understand and apply value sensitive design.

Domain V – Privacy engineering and privacy governance

This domain explains how to integrate privacy into an organization's technology policies and procedures, including the privacy engineering's role within the organization, privacy engineering objectives, privacy design patterns and privacy risk management throughout the phases of the development life cycle.

V.A Understand and implement privacy engineering objectives.

1. Apply the NIST Privacy Engineering Objectives: predictability, manageability and dissociability.
2. Understand enterprise architecture, use of data flow diagrams/data lineage tools, including cross-border transfer considerations.
3. Manage privacy risks in the development life cycle.

V.B Manage and monitor privacy-related functions and controls.

1. Catalog data assets, develop a data inventory and implement a record of processing activities.
2. Conduct code reviews to identify potential privacy gaps that require attention.
3. Conduct runtime behavior monitoring.