# Body of Knowledge

*CIPP/E - CIPM - CIPT - BoK*

**Instructor Guide** | **An Introduction to Privacy for Technology Professionals** | **Strategic Privacy by Design**

# Exam

*Min-max*

*The IAPP currently offers three certification programs:The Certified Information Privacy Professional (CIPP), the Certified Information Privacy Manager (CIPM) and the Certified Information Privacy Technologist (CIPT).*

## Certificate (CIPP/E) European Privacy Certification for the Certified Information Privacy Professional/ Europe — 90

*European Privacy Certification*
*Outline of the Body of Knowledge for the Certified Information Privacy Professional/Europe (CIPP/E)*
*Version 1.2.2 (1.9.2020.)*

*The CIPP is the "**what**" of privacy. Earning this designation demonstrates your mastery of a principles-based framework in information privacy in a legal or practical specialization.Within the CIPP, there are four concentrations:*

- *Asian privacy (CIPP/A)*
- *Canadian privacy (CIPP/C)*
- *European privacy (CIPP/E)*
- *U.S. private-sector privacy (CIPP/US)*

## Certificate (CIPM) Privacy Manager Certification for the Certified Information Privacy Manager — 90

*Privacy Manager Certification*
*Outline of the Body of Knowledge (BOK) for the Certified Information Privacy Manager (CIPM)*
*Version 2.0.1 (1.9.2020.)*

*The CIPM is the "**how**" of operations. Earning this designation shows you understand how to manage privacy in an organization through process and technology.*

## Certificate CIPT Privacy Technology Certification for the Certified Information Privacy Technologist — 90

*Privacy Technology Certification*
*Outline of the Body of Knowledge (BOK) for the Certified Information Privacy Technologist (CIPT)*
*Version 3.0.0 (01.01.2020.)*

*The CIPT is the "**how**" of technology. Earning this designation shows you know how to manage and build privacy requirements and controls into technology.*

*CIPT Exam Format*
*The CIPT is an 2.5 hour exam comprised of 90 multiple choice items (questions). Some of the multiple choice items are associated with scenarios.There are no essay questions. Each correct answer is worth one point.*

*The official IAPP textbooks that encompasses the content referenced in the Body of Knowledge (BoK):*
*IntroP2IT: An Introduction to Privacy for Technology Professionals*
*StratPdB: Strategic Privacy by Design*

*v. 4.0.0 Updated: 07/15/2020*

*Privacy Technologist Certification Authoritative Resource List*
*The IAPP and the Exam Development Board compiled the following list of resources for the purpose of furthering education in information privacy. These selections support the Certified Information Privacy Technologist (CIPT) credentialing program which assesses candidates' understanding of information privacy laws and practices that apply primarily to Information Privacy Technology.*
*Resource Breakdown:*

- *The primary resources are the official IAPP textbooks that encompasses the content referenced in the Body of Knowledge (BoK). While the IAPP does not draw from a single source to develop exams, these are the main texts that support the program.*
- *The supplemental resources are other notable sources that may focus on specific areas of the Body of Knowledge; therefore, the IAPP strongly suggests that you incorporate supplemental reading into your regimen for exam preparation based on your individual needs.*

*The IAPP How to Prepare link connects you to our Daily Dashboard, Resource Center, Podcast,BoKsandmuchmore. Thissiteisupdateddailyandoffersawealthof supplemental information.*
*While we recommend these as comprehensive, widely recognized privacy resources that cover the topics outlined in the BoK, candidates for certification must understand that no published text can keep pace with the rapidly changing privacy landscape.*
*We continuously adjust our exam content to represent the latest regulatory and technological changes and we expect candidates for IAPP certification to know about the important developments in their sector that may modify or supplant information in the authoritative texts.*
*Primary Resources:*
*Breaux, Travis. An Introduction to Privacy for Technology Professionals. Portsmouth. IAPP Publication, 2020. (Print & Digital copies available).*
*Cronk, Jason. Strategic Privacy by Design. Portsmouth. IAPP Publication, 2018. (Print & Digital copies available).*
*Supplemental Resources: (In alphabetical order)*
*BSI. Topics: BSI Home for Industry Reports, Research, Blogs and News. The British Standards Institution. 2020.*
*Finneran Dennedy , Michelle et al. The Privacy Engineer's Companion: A Workbook of Guidance, Tools, Methodologies, and Templates ApressOpen. 2020.*
*Herold, Rebecca. Privacy Professor. Rebecca Herold and Associates, LLC. 2020.*
*Stallings, William. Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices, 1st Edition. Addison- Wesley Professional. 2019.*
*Wheeler, David M. et al. The IoT Architect's Guide to Attainable Security and Privacy. Auerbach Publications. 2019.*
*IAPP Resource Center:*
*The IAPP Resource Center is a searchable Privacy Library containing the most up to date articles, research, and practical guidance on a wide range of privacy topics and issues. Certification can didates are advised to supplement their preparation by referring to this valuable content.*
*The Resource Center also houses the IAPP Glossary of Privacy Terms, which contains important definitions and descriptions catalogued by certification designation.*

| | | | | |
|---|---|---|---|---|
| ☑ **Domain I Foundational Principles** | **Module 1** | **Chapter 1** | | **8-10** |
| ☑ *Topic A Privacy Risk Models and Frameworks* | *Module 1* | *2.2.1* | | *0-2* |
| ☑ 1. Nissenbaum's Contextual Integrity | Module 1 | 2.2.1.5 | | |
| ☑ 2. Calo's Harms Dimensions | Module 1 | 2.2.1.3 | Chapter 6 | |
| ☑ 3. Legal Compliance | Module 1 | 2.2.1.1 | | |
| ☑ 4. FIPPs | Module 1 | 2.2.1.2 | | |
| ☑ 5. NIST/NICE frameworks | Module 1 | 2.2.1.6 | | |

| BoK | CIPT Module | IntroP2IT | StratPdB | ExamQ |
|---|---|---|---|---|
| ☑ 6. FAIR (Factors Analysis in Information Risk)<br>*see:*<br>*Measuring and Managing Information Risk: A FAIR Approach – 2014, by Jack Freund, Jack Jones*<br>*https://www.youtube.com/watch?v=vxBpAnSBaGM*<br>*https://www.youtube.com/watch?v=j890UTSyGS8* | Module 1 | 2.2 / 2.2.1. | Chapter 7 | |
| ☑ *Topic B Privacy by Design Foundational Principles* | *Module 1* | | *Chapter 1, 10* | *1-3* |
| ☑ 1. Full Life Cycle Protection | Module 1 | | pg 2, pg 251 | |
| ☑ 2. Embedded into Design | Module 1 | | pg 3, pg 252 | |
| ☑ 3. Full Functionality | Module 1 | | pg 4, pg 252 | |
| ☑ 4. Visibility and Transparency | Module 1 | | pg 5, pg 253 | |
| ☑ 5. Proactive not Reactive | Module 1 | | pg 6, pg 254 | |
| ☑ 6. Privacy by Default | Module 1 | | pg 7, pg 254 | |
| ☑ 7. Respect for Users | Module 1 | | pg 8, pg 255 | |
| ☑ *Topic C Value Sensitive Design* | *Module 1* | *5.3.3* | | *1-3* |
| ☑ 1. How Design Affects Users | Module 1 | 5.3.3 | | |
| ☑ 2. 14 Methods<br>*A Survey of Value Sensitive Design MethodsBatya Friedman; David G. Hendry; Alan Borning* | Module 1 | 5.3.3 | | |
| ☑ 3. Strategies for Skillful practice | Module 1 | 5.3.3 | | |
| ☑ *Topic D The Data Life Cycle*<br>*Table 1-1*<br>*Compare later to Dark Pattern* | *Module 1* | *1.6* | | *3-5* |
| ☑ 1. Collection<br>*Case: Nomi Technologies (2015 FTC USA)* | Module 1 | 1.6 | | |
| ☑ 2. Use<br>*Case: Hearst Communications (2018 US DC Manhattan USA)* | Module 1 | 1.6 | | |
| ☑ 3. Disclosure<br>*Case: EmblemHealth (2018 NYC AG USA)* | Module 1 | 1.6 | | |
| ☑ 4. Retention<br>*Case: Social Metric (2017 PDPC Singapore)* | Module 1 | 1.6 | | |
| ☑ 5. Destruction<br>*Cse: Dentist (2015 Indiana AG USA)* | Module 1 | 1.6 | | |
| ▾ ⊟ **Domain II The Role of IT in Privacy** | **Module 2** | **Chapter 1, 2** | | **10-12** |
| ☑ *Topic A Fundamentals of privacy-related IT* | *Module 2* | | | *2-4* |
| ☑ 1. Organization privacy notice | Module 1+2 | | | |
| ☑ 2. Organization internal privacy policies | Module 1+2 | | | |
| ☑ 3. Organization security policies, including data classification policies and schema, data retention and data deletion | Module 2 | | | |
| ☑ 4. Other commitments made by the organization (contracts, agreements) | Module 2 | | | |
| ☑ 5. Common IT Frameworks (COBIT, ITIL, etc.) | Module 2 | | | |
| ☑ 6. Data inventories | Module 2 | | | |
| ☑ 7. Enterprise architecture and data flows, including cross-border transfers | Module 2 | | | |
| ☑ 8. Privacy impact assessments (PIAs) | Module 2 | | | |
| ☐ *Topic B Information Security* | *Module 2* | *2.2* | | *5-7* |
| ☐ 1. Transactions which collect confidential data for use in later processing activities | Module 2 | | | |
| ☐ 2. Breach/disclosure incident investigations and responses—security and privacy perspectives | Module 2 | | | |
| ☐ 3. Security and privacy in the systems development life cycle (SDLC) process | Module 2 | 2.1.2 | | |
| ☐ 4. Privacy and security regulations with specific IT requirements | Module 2 | | | |
| ☑ *Topic C The privacy responsibilities of the IT professional* | *Module 2* | | | *1-3* |
| ☑ 1. Providing feedback on policies | Module 2 | | | |
| ☑ 2. Providing feedback on contractual and regulatory requirements | Module 2 | | | |

| BoK | CIPT Module | IntroP2IT | StratPdB | ExamQ |
|---|---|---|---|---|
| ☑ 3. Understanding how Information Technology and Information Security support information governance in an organization | Module 2 | | | |
| ▾ ☐ **Domain III Privacy Threats and Violations** | **Module 3** | **Chapter 7** | **Chapter 3** | **12-14** |
| ☐ *Topic A During Data Collection* | *Module 3* | *2.2.1.4* | *pg 42* | *2-4* |
| ☐ 1. Asking people to reveal personal information | Module 3 | | pg 43 | |
| ☐ 2. Surveillance | Module 3 | | pg 42 | |
| ☐ *Topic B During Use* | *Module 3* | *2.2.1.4* | *pg 45* | *2-4* |
| ☐ 1. Insecurity | Module 3 | | pg 46 | |
| ☐ 2. Identification | Module 3 | | pg 48 | |
| ☐ 3. Aggregation | Module 3 | | pg 45 | |
| ☐ 4. Secondary Use | Module 3 | | pg 49 | |
| ☐ 5. Exclusion | Module 3 | | pg 52 | |
| ☐ *Topic C During Dissemination* | *Module 3* | *2.2.1.4* | *pg 54* | *2-4* |
| ☐ 1. Disclosure | Module 3 | | pg 55 | |
| ☐ 2. Distortion | Module 3 | | pg 62 | |
| ☐ 3. Exposure | Module 3 | | pg 56 | |
| ☐ 4. Breach of Confidentiality | Module 3 | | pg 54 | |
| ☐ 5. Increased accessibility | Module 3 | | pg 57 | |
| ☐ 6. Blackmail | Module 3 | | pg 59 | |
| ☐ 7. Appropriation | Module 3 | | pg 60 | |
| ☐ *Topic D Intrusion, Decisional Interference and Self Representation* | *Module 3* | *Chapter 7, 2.2.1.4* | *pg 63, pg 67* | *1-3* |
| ☐ 1. Behavioral advertising | Module 3 | 7.2.3 | | |
| ☐ 2. Cyberbullying | Module 3 | 7.2.5 | | |
| ☐ 3. Social engineering | Module 3 | | | |
| ☐ *Topic E Software Security* | *Module 3* | *Chapter 9* | | *1-3* |
| ☐ 1. Vulnerability management | Module 3 | | | |
| ☐ 2. Intrusion reports | Module 3 | | | |
| ☐ 3. Patches | Module 3 | | | |
| ☐ 4. Upgrades | Module 3 | | | |
| ☐ 5. Open-source vs Closed-source | Module 3 | 9.5 | | |
| ▾ ☐ **Domain IV Technical Measures and Privacy Enhancing Technologies** | **Module 4** | | **Chapter 4** | **13-15** |
| ☐ *Topic A Data Oriented Strategies* | *Module 4* | | *pg 88* | *3-5* |
| ☐ 1. Separate | Module 4 | | pg 89 | |
| ☐ i. Distribute | Module 4 | | pg 89 | |
| ☐ ii. Isolate | Module 4 | | pg 91 | |
| ☐ 2. Minimize | Module 4 | | pg 92 | |
| ☐ i. Exclude | Module 4 | | pg 93 | |
| ☐ ii. Select | Module 4 | | pg 94 | |
| ☐ iii. Strip | Module 4 | | pg 95 | |
| ☐ iv. Destroy | Module 4 | | pg 96 | |
| ☐ 3. Abstract | Module 4 | | pg 101 | |
| ☐ i. Group | Module 4 | | pg 101 | |
| ☐ ii. Summarize | Module 4 | | pg 102 | |
| ☐ iii. Perturb | Module 4 | | pg 103 | |
| ☐ 4. Hide | Module 4 | | pg 96 | |
| ☐ i. Restrict | Module 4 | | pg 97 | |
| ☐ ii. Mix | Module 4 | | pg 97 | |
| ☐ iii. Obfuscate | Module 4 | | pg 98 | |

| BoK | CIPT Module | IntroP2IT | StratPdB | ExamQ |
|---|---|---|---|---|
| ☐ iv. Dissociate | Module 4 | | pg 100 | |
| ☐ *Topic B Techniques* | *Module 4* | | | *7-9* |
| ☐ 1. Aggregation | Module 4 | Chapter 4 | | |
| ☐ i. Frequency and magnitude data | Module 4 | 4.4.4 | | |
| ☐ ii. Noise addition through differential privacy | Module 4 | 4.4.4 | | |
| ☐ iii. Differential identifiability | Module 4 | 4.4.4 | | |
| ☐ 2. De-identification | Module 4 | Chapter 4 | | |
| ☐ i. Anonymize | Module 4 | 4.4 | | |
| ☐ ii. Pseudonymize | Module 4 | 4.4 | | |
| ☐ iii. Labels that point to individuals | Module 4 | 4.4 | | |
| ☐ iv. Strong and weak identifiers | Module 4 | 4.4 | | |
| ☐ v. Degrees of Identifiability | Module 4 | 4.4 | | |
| ☐ vi. k-anonymity, l-diversity, t-closeness | Module 4 | 4.4.3 | | |
| ☐ vii. Tokenization | Module 4 | 2.4.3.3 | | |
| ☐ 3. Encryption | Module 4 | Chapter 3 | | |
| ☐ i. Algorithms and Keys | Module 4 | | | |
| ☐ ii. Symmetric and Asymmetric | Module 4 | | | |
| ☐ iii. Crypto design and implementation considerations | Module 4 | | | |
| ☐ iv. Application or field encryption | Module 4 | | | |
| ☐ v. Quantum encryption | Module 4 | | | |
| ☐ vi. Public Key Infrastructure | Module 4 | | | |
| ☐ vii. Homomorphic | Module 4 | 9.4. | | |
| ☐ viii. Polymorphic | Module 4 | | | |
| ☐ ix. Mix networks | Module 4 | | | |
| ☐ x. Secure multi-party computation | Module 4 | | | |
| ☐ xi. Private information retrieval | Module 4 | | | |
| ☐ 4. Identity and access management | Module 4 | 4.1, 9.4 | | |
| ☐ i. Limitations of access management as a privacy tool | Module 4 | | | |
| ☐ ii. Principle of least-privilege required | Module 4 | | | |
| ☐ iii. Role-based access control (RBAC) | Module 4 | 9.4.3 | | |
| ☐ iv. User-based access controls | Module 4 | | | |
| ☐ v. Context of authority | Module 4 | | | |
| ☐ vi. Cross-enterprise authentication and authorization models | Module 4 | 9.4.4 | | |
| ☐ vii. Federated identity | Module 4 | 9.4.4 | | |
| ☐ viii. Bring your own device (BYOD) concerns | Module 4 | 9.5 | | |
| ☐ 5. Authentication | Module 4 | 4.2 | | |
| ☐ i. Single/multi factor authentication | Module 4 | 4.2.5 | | |
| ☐ ii. Something you know (usernames, passwords) | Module 4 | | | |
| ☐ iii. Something you are (biometrics, facial recognition, location) | Module 4 | | | |
| ☐ iv. Something you have (tokens, keys) | Module 4 | | | |
| ☐ *Topic C Process Oriented Strategies* | *Module 4* | | | *1-3* |
| ☐ 1. Informing the Individual | Module 4 | | pg 112 | |
| ☐ i. Supply | Module 4 | | pg 112 | |
| ☐ ii. Notify | Module 4 | | pg 114 | |
| ☐ iii. Explain | Module 4 | | pg 114 | |
| ☐ 2. User Control | Module 4 | | pg 116 | |
| ☐ i. Consent | Module 4 | | pg 117 | |
| ☐ ii. Choose | Module 4 | | pg 117 | |
| ☐ iii. Update | Module 4 | | pg 117 | |
| ☐ iv. Retract | Module 4 | | pg 117 | |
| ☐ 3. Policy and Process Enforcement | Module 4 | | pg 104 | |
| ☐ i. Create | Module 4 | | pg 104 | |
| ☐ ii. Maintain | Module 4 | | pg 108 | |
| ☐ iii. Uphold | Module 4 | | pg 108 | |
| ☐ 4. Demonstrate Compliance | Module 4 | | pg 110 | |

| BoK | CIPT Module | IntroP2IT | StratPdB | ExamQ |
|---|---|---|---|---|
| ☐ i. Log | Module 4 | | pg 110 | |
| ☐ ii. Audit | Module 4 | | pg 111 | |
| ☐ iii. Report | Module 4 | | pg 112 | |
| ▾ ☐ **Domain V Privacy Engineering** | **Module 5 +3,6** | **Chapter 8** | | **8-10** |
| ☐ *Topic A The Privacy Engineering role in the organization* | *Module 5* | | | *0-2* |
| ☐ *Topic B Privacy Engineering Objectives* | *Module 5* | *8.2.5* | | *0-2* |
| ☐ 1. Predictability | Module 5 | | | |
| ☐ 2. Manageability | Module 5 | | | |
| ☐ 3. Disassociability | Module 5 | | | |
| ☐ *Topic C Privacy Design Patterns* | *Module 5* | | | *3-5* |
| ☐ 1. Design patterns to emulate | Module 5 | 2.4.2.4 | | |
| ☐ 2. Dark patterns to avoid<br>https://edps.europa.eu/press-publications/publications/podcasts/democratic-societies-digital-age-ep2-dark-patterns-and_en | Module 5 | 2.4.2.6 | | |
| ☐ *Topic D Privacy Risks in Software* | *Module 3,5,6* | | | *2-4* |
| ☐ 1. Risks | Module 3,5,6 | | | |
| ☐ 2. Countermeasures | Module 3,5,6 | | | |
| ▾ ☐ **Domain VI Privacy by Design Methodology** | **Module 6** | | **Chapter 9** | **7-9** |
| ☐ *Topic A The Privacy by Design Process* | *Module 6* | | | *3-5* |
| ☐ 1. Goal Setting | Module 6 | | | |
| ☐ 2. Documenting Requirements | Module 6 | 2.3.1 | | |
| ☐ 3. Understanding quality attributes | Module 6 | | | |
| ☐ 4. Identify information needs | Module 6 | | | |
| ☐ 5. High level design | Module 6 | | | |
| ☐ 6. Low level design and implementation | Module 6 | | | |
| ☐ 7. Impose controls | Module 6 | | | |
| ☐ i. Architect | Module 6 | | | |
| ☐ ii. Secure | Module 6 | | | |
| ☐ iii. Supervise | Module 6 | | | |
| ☐ iv. Balance | Module 6 | | | |
| ☐ 8. Testing and validation | Module 6 | | | |
| ☐ *Topic B Ongoing Vigilance* | *Module 6* | | | *3-5* |
| ☐ 1. Code reviews | Module 6 | | | |
| ☐ 2. Code audits | Module 6 | | | |
| ☐ 3. Runtime behavior monitoring | Module 6 | | | |
| ☐ 4. Software evolution | Module 6 | | | |
| ▾ ☐ **Domain VII Technology Challenges for Privacy** | **Module 7** | **Chapter 6, 7** | | **10-12** |
| ☐ *Topic A Automated decision making* | *Module 7* | *7.2.* | | *2-4* |
| ☐ 1. Machine learning | Module 7 | 7.2.4 | | |
| ☐ 2. Deep learning | Module 7 | | | |
| ☐ 3. Artificial Intelligence (AI) | Module 7 | | | |
| ☐ 4. Context aware computing | Module 7 | | | |
| ☐ *Topic B Tracking and Surveillance* | *Module 7* | *Chapter 6* | | *2-4* |
| ☐ 1. Internet monitoring | Module 7 | 6.1 | | |
| ☐ 2. Web tracking | Module 7 | 6.2, 6.3 | | |
| ☐ 3. Location tracking | Module 7 | 6.4 | | |
| ☐ 4. Audio and Video Surveillance | Module 7 | 6.5 | | |
| ☐ 5. Drones | Module 7 | | | |
| ☐ *Topic C Anthropomorphism* | *Module 7* | *7.2.5* | | *0-2* |
| ☐ 1. Speech recognition | Module 7 | 6.5.4 | | |

| BoK | CIPT Module | IntroP2IT | StratPdB | ExamQ |
|---|---|---|---|---|
| ☐2. Natural language understanding | Module 7 | | | |
| ☐3. Natural language generation | Module 7 | | | |
| ☐4. Chat bots | Module 7 | 7.2.5 | | |
| ☐5. Robots | Module 7 | | | |
| ☐ *Topic D Ubiquitous computing* | *Module 7* | *6.6.1, 7.2.4* | | *2-4* |
| ☐1. Internet of Things (IoT) | Module 7 | 6.6.3 | | |
| ☐2. Vehicular automation | Module 7 | 6.6.5 | | |
| ☐3. Wearable devices | Module 7 | 6.6.6 | | |
| ☐ *Topic E Mobile Social Computing* | *Module 7* | *7.3* | | *0-2* |
| ☐1. Geo-tagging | Module 7 | 6.4.2 | | |
| ☐2. Geo-social patterns | Module 7 | 6.7 | | |
| ▸ ☐ **Certificate CIPT Example Questions** | | | | |