IT Privacy Certification

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

I. Understanding the need for privacy in the IT environment

A. Evolving compliance requirements

a. GDPR considerations

B. IT risks

a. Client-side
b. Server-side
c. Security policy and personnel
d. Application
e. Network
f. Storage

C. Stakeholders expectations for privacy

D. Mistakes organizations make

a. Recent security incidents and enforcement actions

E. Privacy vs. security—what's alike and what's different

F. IT governance vs. data governance

G. The role of the IT professional, and those of other players, in preserving privacy

II. Core privacy concepts

A. Foundational elements for embedding privacy in IT

a. Organization privacy notice
b. Organization internal privacy policies
c. Organization security policies, including data classification policies, data retention and data deletion
d. Other commitments made by the organization (contracts, agreements)
e. Common IT Frameworks (COBIT, ITIL, etc.)
f. Data inventory
g. Incident response—security and privacy perspectives
h. Security and privacy in the systems development life cycle (SDLC) process
i. Enterprise architecture and data flows, including cross border transfers

j. Privacy impact assessments (PIAs)
k. Privacy and security regulations with specific IT requirements
l. Common standards and framework of relevance

B. The information life cycle: an introduction

a. Collection
b. Use
c. Disclosure
d. Retention
e. Destruction

C. Common privacy principles

a. Collection limitation
b. Data quality
c. Purpose specification
d. Use limitation
e. Security safeguards
f. Openness
g. Individual participation
h. Accountability

III. Privacy considerations in the information life cycle

A. Collection

a. Notice
b. Choice/consent
c. Collection limitations
d. Secure transfer
e. Reliable sources/collection from third parties
f. Collection of information from individuals other than the data subject

B. Use

a. Compliance to regulations and commitments
b. Data minimization
c. Secondary uses
d. User authentication, access control, audit trails
e. Secure when in use and not in use
f. Using personally identifiable information (PII) in testing
g. Limitations on use when sources of data are unclear

C. Disclosure

a. According to notice
b. Anonymize, minimize
c. Define limitations
d. Vendor management programs
e. Inventory and secure transfers, secure remote access, review data protection capabilities prior to engaging
f. Using intermediaries for the processing of sensitive information

D. Retention

a. Working with records management

b. Regulatory limitations, legal restrictions, limit retention of sensitive data if not necessary
c. Provide data subject access
    i. Legal requirements
    ii. Business rationale
    iii. Access mechanisms
    iv. Handling requests
d. Secure transfer to archiving, secure storage of information and meta data
e. Considerations for business continuity and disaster recovery
f. Portable media challenges

E. Destruction

a. Digital content, portable media, hard copy
b. Identify appropriate time
c. Secure transfer and disposal of information and media, return information from third parties
d. Regulatory requirements defining destruction standards

IV. Privacy in systems and applications

A. The enterprise IT environment—common challenges

a. Architecture considerations
b. IT involvement through mergers and acquisitions
c. Industry and function specific systems

B. Identity and access management

a. Limitations of access management as a privacy tool
b. Principle of least-privilege required
c. Role-based access control (RBAC)
d. User-based access controls
e. Context of authority
f. Cross-enterprise authentication and authorization models

C. Credit card information and processing

a. Cardholder data types
b. Application of Payment Card Industry Data Security Standard (PCI DSS)
c. Implementation of Payment Application Data Security Standard (PCI PA DSS)

D. Remote access, telecommuting, and bring your own devices to work

a. Privacy considerations
b. Security considerations
c. Access to computers
d. Device controls
e. Network controls
f. Architecture controls

E. Data encryption

a. Crypto design and implementation considerations
b. Application or field encryption
c. File encryption
d. Disk encryption
e. Encryption regulation

f. Encryption standards

F. Other privacy enhancing technologies (PET) in the enterprise environment

a. Automated data retrieval
b. Automated system audits
c. Data masking and data obfuscation
d. Data loss prevention (DLP) implementation and maintenance

G. Specific considerations for customer-facing applications

a. Software-based notice and consent
b. Agreements
   i. End-user license agreement (EULA)
   ii. Terms of service
   iii. Terms of use for nonlicensed products
   iv. Mechanisms

V. Privacy techniques

A. Authentication techniques and degrees of strength

a. User name and password
b. Single/multi factor authentication
c. Biometrics
d. Portable media supporting authentication

B. Identifiability

a. Labels that point to individuals
b. Strong and weak identifiers
c. Pseudonymous and anonymous data
d. Degrees of Identifiability
   i. Definition under the GDPR
   ii. U.S. regulations (HIPAA, FACTA, FERPA, etc.)
   iii. Other regulations addressing identity in data
   iv. Privacy stages and system characteristics
   v. Identifiable versus identified
   vi. Linkable versus linked
e. Data aggregation

C. Privacy by Design—overview of principles

D. Privacy by ReDesign—review of framework

VI. Online privacy issues

A. Specific requirements for the online environment

a. Organizational privacy strategy
b. Regulatory requirements specific to the online environment
c. Consumer expectations
d. Children's online privacy

B. Social media and websites that present a higher level of privacy challenges

a. Personal information shared
b. Personal information collected

c. No clear owner of content published or data collected
d. Chatbots

C. Online threats

a. Phishing, whaling, etc.
b. SQL injection
c. Cross-site scripting (XSS)
d. Spam
e. Ransomware
f. Common safeguards against threats (DMARC, Unified Threat Management systems, etc.)

D. E-commerce personalization

a. End user benefits
b. End user privacy concerns

E. Online advertising

a. Understanding the common models of online advertising
b. Key considerations when working with third parties to post ads on your company's website

F. Understanding cookies, beacons and other tracking technologies

a. Common types
b. Privacy considerations
c. Responsible practices

G. Machine-readable privacy policy languages

a. Platform for Privacy Preferences Project (P3P)
b. Application Preference Exchange Language (APPEL)
c. Enterprise Privacy Authorization Language (EPAL)
d. Security Assertion Markup Language (SAML)
e. eXtensible Access Control Markup Language (XACML)

H. Web browser privacy and security features

a. Private browsing
b. Tracking protection
c. Do not track

I. Web security protocols

a. Secure sockets layer / transport security layer (SSL / TLS)
b. Hypertext transfer protocol secure (HTTPS)
c. Limiting or preventing automated data capture
d. Combating threats and exploits
e. Anonymity tools

VII. Technologies with privacy considerations

A. Cloud computing

a. Types of cloud
b. Common privacy concerns
c. Common security concerns
d. Associations and standards

B. Wireless IDs

   a. Radio frequency identification
   b. Bluetooth devices
   c. Wi-Fi
   d. Cellular telephones and tablet computers

C. Location-based services

   a. Evolution of location based services on mobile phones and personal digital assistants (PDAs)
   b. Global positioning systems (GPS)
   c. Geographic information systems (GIS)

D. "Smart" technologies

   a. Data analytics
   b. Deep learning
   c. Internet of Things (IoT)
   d. Vehicular automation

E. Video/data/audio surveillance

   a. Drones

F. Biometric recognition