Outline of the Body of Knowledge (BoK) for the Certified Information Privacy Manager (CIPM)

The CIPM certification is comprised of six domains: **Privacy Program Governance (I)**, **Privacy Program Framework (II), Privacy Program Operational Life Cycle – Assessment (III), Privacy Program Operational Life Cycle – Protect (IV) Privacy Program Operational Life Cycle – Sustain (V),** and **Privacy Program Operational Life Cycle – Respond (VI)**.

Domain I provides a solid foundation for the governance of a privacy program and defines how the privacy program may be developed, measured and improved;

Domain II focuses on the management and operations of the privacy program governance model within the context of the organization's privacy strategy;

Domain III details important components supporting the assessment or analysis of an organization's privacy regime;

Domain IV outlines the protection of assets through the implementation of industry-leading privacy and security controls and technology;

Domain V details how the privacy program is sustained through communication, training and management actions; and

Domain VI provides information a solid foundation regarding the response to privacy incidents.

I. Developing a Privacy Program

A. <u>Create a company vision</u>

   a. Acquire knowledge on privacy approaches
   b. Evaluate the intended objective
   c. Gain executive sponsor approval for this vision

B. <u>Establish a Data Governance model</u>

   a. Centralized
   b. Distributed
   c. Hybrid

C. <u>Establish a privacy program</u>

   a. Define program scope and charter

b. Identify the source, types, and uses of personal information (PI) within the organization and the applicable laws

c. Develop a privacy strategy

i. Business alignment

1. Finalize the operational business case for privacy
2. Identify stakeholders
3. Leverage key functions
4. Create a process for interfacing within organization
5. Align organizational culture and privacy/data protection objectives

ii. Obtain funding/budget for privacy and the privacy team

iii. Develop a data governance strategy for personal information (collection, authorized use, access, destruction)

iv. Plan inquiry/complaint handling procedures (customers, regulators, etc.)

v. Ensure program flexibility in order to incorporate legislative/regulatory/market/business requirements

D. Structure the privacy team

a. Establish the organizational model, responsibilities and reporting structure appropriate to the size of the organization

i. Large organizations

1. Chief privacy officer
2. Privacy manager
3. Privacy analysts
4. Business line privacy leaders
5. “First responders”

ii. Small organizations/sole data protection officer (DPO) including when not only job

b. Designate a point of contact for privacy issues

c. Establish/endorse the measurement of professional competency

E. Communicate

a. Awareness

i. Create awareness of the organization’s privacy program internally and externally

ii. Develop internal and external communication plans to ingrain organizational accountability

iii. Identify, catalog and maintain documents requiring updates as privacy requirements change

II. Privacy Program Framework

A. Develop the Privacy Program Framework

a. Develop organizational privacy policies, standards, and/or guidelines

b. Define privacy program activities

i. Education and awareness

ii. Monitoring and responding to the regulatory environment

iii. Internal policy compliance

iv. Data inventories, data flows, and classification

    v. Risk assessment (Privacy Impact Assessments [PIAs]) (e,g., DPIAs etc.)
    vi. Incident response and process, including jurisdictional regulations
    vii. Remediation
    viii. Program assurance, including audits

B. Implement the Privacy Program Framework

- a. Communicate the framework to internal and external stakeholders
- b. Ensure continuous alignment to applicable laws and regulations to support the development of an organizational privacy program framework
    - i. Understand when national laws and regulations apply (e.g. GDPR)
    - ii. Understand when local laws and regulations apply (e.g. CCPA)
    - iii. Understand penalties for noncompliance with laws and regulations
    - iv. Understand the scope and authority of oversight agencies (e.g., Data Protection Authorities, Privacy Commissioners, Federal Trade Commission, etc.)
    - v. Understand privacy implications of doing business with or basing operations in countries with inadequate, or without, privacy laws
    - vi. Maintain the ability to manage a global privacy function
    - vii. Maintain the ability to track multiple jurisdictions for changes in privacy law
    - viii. Understand international data sharing arrangement agreements

C. Develop Appropriate Metrics

- a. Identify intended audience for metrics
- b. Define reporting resources
- c. Define privacy metrics for oversight and governance per audience
    - i. Compliance metrics (examples, will vary by organization)
        1. Collection (notice)
        2. Responses to data subject inquiries
        3. Use
        4. Retention
        5. Disclosure to third parties
        6. Incidents (breaches, complaints, inquiries)
        7. Employees trained
        8. PIA metrics
        9. Privacy risk indicators
        10. Percent of company functions represented by governance mechanisms
    - ii. Trending
    - iii. Privacy program return on investment (ROI)
    - iv. Business resiliency metrics
    - v. Privacy program maturity level
    - vi. Resource utilization
- d. Identify systems/application collection points

III. Privacy Operational Life Cycle: Assess

A. Document current baseline of your privacy program

- a. Education and awareness
- b. Monitoring and responding to the regulatory environment
- c. Internal policy compliance

- d. Data, systems and process assessment
  - i. Map data inventories, flows and classification
  - ii. Create "record of authority" of systems processing personal information within the organization
    - 1. Map and document data flow in systems and applications
    - 2. Analyze and classify types and uses of data
- e. Risk assessment (PIAs, etc.)
- f. Incident response
- g. Remediation
- h. Determine desired state and perform gap analysis against an accepted standard or law (including GDPR)
- i. Program assurance, including audits

B. Processors and third-party vendor assessment

- a. Evaluate processors and third-party vendors, insourcing and outsourcing privacy risks, including rules of international data transfer
  - i. Privacy and information security policies
  - ii. Access controls
  - iii. Where personal information is being held
  - iv. Who has access to personal information
- b. Understand and leverage the different types of relationships
  - i. Internal audit
  - ii. Information security
  - iii. Physical security
  - iv. Data protection authority
- c. Risk assessment
  - i. Type of data being outsourced
  - ii. Location of data
  - iii. Implications of cloud computing strategies
  - iv. Legal compliance
  - v. Records retention
  - vi. Contractual requirements (incident response, etc.)
  - vii. Establish minimum standards for safeguarding information
- d. Contractual requirements
- e. Ongoing monitoring and auditing

C. Physical assessments

- a. Identify operational risk
  - i. Data centers and offices
  - ii. Physical access controls
  - iii. Document destruction
  - iv. Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.)
  - v. Device forensics
  - vi. Device security (e.g., mobile devices, Internet of Things (IoT), geo-tracking, imaging/copier hard drive security controls)

D. Mergers, acquisitions and divestitures

- a. Due diligence
- b. Risk assessment

E. Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs)

- a. Privacy Threshold Analysis (PTAs) on systems, applications and processes

b. Privacy Impact Assessments (PIAs)
    i. Define a process for conducting Privacy Impact Assessments
        1. Understand the life cycle of a PIA
        2. Incorporate PIA into system, process, product life cycles

IV. Privacy Operational Life Cycle: Protect

A. Information security practices

a. Access controls for physical and virtual systems
    i. Access control on need to know
    ii. Account management (e.g., provision process)
    iii. Privilege management
b. Technical security controls
c. Implement appropriate administrative safeguards

B. Privacy by Design

a. Integrate privacy throughout the system development life cycle (SDLC)
b. Establish privacy gates as part of the system development framework

C. Integrate privacy requirements and representation into functional areas across the organization

a. Information security
b. IT operations and development
c. Business continuity and disaster recovery planning
d. Mergers, acquisitions and divestitures
e. Human resources
f. Compliance and ethics
g. Audit
h. Marketing/business development
i. Public relations
j. Procurement/sourcing
k. Legal and contracts
l. Security/emergency services
m. Finance
n. Others

D. Other Organizational Measures

a. Quantify the costs of technical controls
b. Manage data retention with respect to the organization’s policies
c. Define the methods for physical and electronic data destruction
d. Define roles and responsibilities for managing the sharing and disclosure of data for internal and external use

V. Privacy Operational Life Cycle: Sustain

A. Monitor

a. Environment (e.g., systems, applications) monitoring
b. Monitor compliance with established privacy policies
c. Monitor regulatory and legislative changes

- d. Compliance monitoring (e.g. collection, use and retention)
  - i. Internal audit
  - ii. Self-regulation
  - iii. Retention strategy
  - iv. Exit strategy

B. Audit

- a. Align privacy operations to an internal and external compliance audit program
  - i. Knowledge of audit processes
  - ii. Align to industry standards
- b. Audit compliance with privacy policies and standards
- c. Audit data integrity and quality and communicate audit findings with stakeholders
- d. Audit information access, modification and disclosure accounting
- e. Targeted employee, management and contractor training
  - i. Privacy policies
  - ii. Operational privacy practices (e.g., standard operating instructions), such as
    - 1. Data creation/usage/retention/disposal
    - 2. Access control
    - 3. Reporting incidents
    - 4. Key contacts

VI. Privacy Operational Life Cycle: Respond

A. Data-subject information requests and privacy rights

- a. Access
- b. Redress
- c. Correction
- d. Managing data integrity
- e. Right of Erasure
- f. Right to be informed
- g. Control over use of data

B. Privacy incident response

- a. Legal compliance
  - i. Preventing harm
  - ii. Collection limitations
  - iii. Accountability
  - iv. Monitoring and enforcement
- b. Incident response planning
  - i. Understand key roles and responsibilities
    - 1. Identify key business stakeholders
      - a) Information security
      - b) Legal
      - c) Audit
      - d) Human resources
      - e) Marketing
      - f) Business development
      - g) Communications and public relations
      - h) Other
    - 2. Establish incident oversight teams

3. Develop a privacy incident response plan
4. Identify elements of the privacy incident response plan
5. Integrate privacy incident response into business continuity planning

c. Incident detection
   i. Define what constitutes a privacy incident
   ii. Identify reporting process
   iii. Coordinate detection capabilities
      1. Organization IT
      2. Physical security
      3. Human resources
      4. Investigation teams
      5. Vendors

d. Incident handling
   i. Understand key roles and responsibilities
   ii. Develop a communications plan to notify executive management

e. Follow incident response process to ensure meeting jurisdictional, global and business requirements
   i. Engage privacy team
   ii. Review the facts
   iii. Conduct analysis
   iv. Determine actions (contain, communicate, etc.)
   v. Execute
   vi. Monitor
   vii. Review and apply lessons learned

f. Identify incident reduction techniques

g. Incident metrics—quantify the cost of a privacy incident