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

The CIPM certification is comprised of six domains: **Developing a Privacy Program (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. Create an organizational vision

   a. Evaluate the intended objective
   b. Gain executive sponsor approval for this vision

B. Establish a Data Governance model

   a. Centralized
   b. Distributed
   c. Hybrid

C. Define a privacy program

   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 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 processing personal information (e.g. collect, use, access, share, transfer, destroy)
    iv. 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 (eg Chief Privacy Officer, DPO, Privacy manager, Privacy analysts, Privacy champions, "First responders")
b. Designate a point of contact for privacy issues
c. Establish/endorse the measurement of professional competency

E. Communicate

a. Create awareness of the organization's privacy program internally and externally (e.g. PR, Corporate Communication, HR)
b. Develop internal and external communication plans to ingrain organizational accountability
c. Ensure employees have access to policies and procedures and updates relative to their role

II. Privacy Program Framework

A. Develop the Privacy Program Framework

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

b. Define privacy program activities
    i. Education and awareness
    ii. Monitoring and responding to the regulatory environment
    iii. Monitoring internal privacy policy compliance
    iv. Data inventories, data flows, and classifications designed to identify what personal data your organization processes
    v. Risk assessment (Privacy Impact Assessments [PIAs]) (e,g., DPIAs etc.)
    vi. Incident response and process, including jurisdictional requirements
    vii. Remediation oversight
    viii. Program assurance, including audits
    ix. Plan inquiry/complaint handling procedures (customers, regulators, etc.)

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 territorial regulations and/or laws (eg GDPR, CCPA, LGPD)
    ii. Understand sectoral and industry regulations and/or laws (eg HIPAA, GLBA)
    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
c. Understanding data sharing agreements
    i. International data sharing agreements
    ii. Vendor agreement
    iii. Affiliate and subsidiary 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. Retention
        4. Disclosure to third parties
        5. Incidents (breaches, complaints, inquiries)
        6. Employees trained
        7. PIA/DPIA metrics
        8. Privacy risk indicators
        9. Percent of company functions represented by governance mechanisms
    ii. Trend Analysis
    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. Assess policy compliance against internal and external requirements
d. Data, systems and process assessment
    i. Map data inventories, flows, lifecycle and system integrations
e. Risk assessment methods
f. Incident management, response and remediation

g. Determine desired state and perform gap analysis against an accepted standard or law (including GDPR)
h. 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. Review and set limits on vendor internal use of 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. Technologies and processing methods deployed (eg Cloud Computing)
    iv. Legal compliance
    v. Records retention
    vi. Contractual requirements (incident response, etc.)
    vii. Determine minimum standards for safeguarding information
    viii. Cross-border transfers
d. Contractual requirements and review process
e. Ongoing monitoring and auditing

C. Physical assessments

a. Identify operational risk
    i. Data centers and offices
    ii. Physical access controls
    iii. Document retention and 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 procedures
b. Review contractual and data sharing obligations
c. Risk assessment
d. Risk and control alignment
e. Post integration planning and risk mitigation

E. Privacy Assessments and Documentation

a. Privacy Threshold Analysis (PTAs) on systems, applications and processes
b. Define a process for conducting privacy assessments (e.g., PIA, DPIA, TIA, LIA)
    i. Understand the life cycle of each assessment type
    ii. Incorporate privacy assessments into system, process, data life cycles

IV. Privacy Operational Life Cycle: Protect

A. Information security practices

   a. Access controls for physical and virtual systems
      i. Least privileged access (eg need to know)
      ii. Account management (e.g., provision process)
      iii. Privilege management
   b. Technical security controls (including relevant policies and procedures)
   c. Incident response plans

B. Privacy by Design (PbD)

   a. Integrate privacy throughout the system development life cycle (SDLC)
   b. Establish privacy gates as part of the system development framework
   c. Integrate privacy through business processes
   d. Communicate with stakeholders the importance of PIAs and PbD

C. Integrate privacy requirements and representation into functional areas across the organization (eg Information Security, Human Resources, Marketing, Legal and Contracts, Mergers, Acquisitions & Divestitures)

D. Technical and Organizational measures

   a. Quantify the costs of technical and organizational 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
   e. Determine and implement guidelines for secondary uses (ex: research, etc.)
   f. Define policies related to the processing (including collection, use, retention, disclosure and disposal) of organization's data holdings, taking into account both legal and ethical requirements
   g. Implement appropriate administrative safeguards, such as policies, procedures, and contracts

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 and maintenance of an "audit trail"

ii. Assess against industry standards
iii. Utilize and report on regulator compliance assessment tools

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, including objection to processing
h. Complaints including file reviews

B. Privacy incident response

a. Legal compliance
    i. Preventing harm
    ii. Collection limitations
    iii. Accountability
    iv. Monitoring and enforcement
    v. Mandatory reporting
b. Incident response planning
    i. Understand key roles and responsibilities
        1. Identify key business stakeholders
            a) Information security
            b) Legal
            c) Head of compliance
            d) Audit
            e) Human resources
            f) Marketing
            g) Business development
            h) Communications and public relations
            i) External parties
        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. Conduct risk assessment
    iii. Perform containment activities
    iv. Identify and implement remediation measures
    v. Develop a communications plan to notify executive management
    vi. Notify regulator, impacted individuals and/or the responsible data controller

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. Maintain an incident register and associated records of the incident management
    vii. Monitor
    viii. Review and apply lessons learned

f. Identify incident reduction techniques
g. Incident metrics—quantify the cost of a privacy incident