Privacy Manager Certification

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

The CIPM certification is comprised of two domains: **Privacy Program Governance (I)** and **Privacy Program Operational Life Cycle (II)**.

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 details the management and operations of the privacy program governance model within the context of the organization's privacy strategy. The Privacy Program Operational Life Cycle domain is built upon a common industry-accepted framework of: **Assessing** or analyzing an organization's privacy regime; **Protecting** information assets through the implementation of industry-leading privacy and security controls and technology; **Sustaining** the privacy program through communication, training and management actions; and **Responding** to privacy incidents.

I. Privacy Program Governance

A. Organization Level

a. Create a company vision
   i. Acquire knowledge on privacy approaches
   ii. Evaluate the intended objective
   iii. Gain executive sponsor approval for this vision

b. Establish Data Governance model
   1. Centralized
   2. Distributed
   3. Hybrid

c. Establish a privacy program
   i. Define program scope and charter
   ii. Identify the source, types, and uses of personal information (PI) within the organization and the applicable laws
   iii. Develop a privacy strategy
      1. Business alignment
         a. Finalize the operational business case for privacy
         b. Identify stakeholders
         c. Leverage key functions
         d. Create a process for interfacing within organization

e. Align organizational culture and privacy/data protection objectives
f. Obtain funding/budget for privacy and the privacy team

2. Develop a data governance strategy for personal information (collection, authorized use, access, destruction)
3. Plan inquiry/complaint handling procedures (customers, regulators, etc.)

d. Structure the privacy team
   i. Establish the organizational model, responsibilities and reporting structure appropriate to the size of the organization
      1. Large organizations
         a. Chief privacy officer
         b. Privacy manager
         c. Privacy analysts
         d. Business line privacy leaders
         e. "First responders"
      2. Small organizations/sole data protection officer (DPO) including when not only job
   ii. Designate a point of contact for privacy issues
   iii. Establish/endorse the measurement of professional competency

B. 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

C. 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, CCPA)
   ii. Understand when local laws and regulations apply
   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

D. 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

II. Privacy Operational Life Cycle

A. Assess Your Organization

a. Document current baseline of your privacy program
    i. Education and awareness
    ii. Monitoring and responding to the regulatory environment
    iii. Internal policy compliance
    iv. Data, systems and process assessment
        1. Map data inventories, flows and classification
        2. Create "record of authority" of systems processing personal information within the organization
        3. Map and document data flow in systems and applications
        4. Analyze and classify types and uses of data
    v. Risk assessment (PIAs, etc.)
    vi. Incident response
    vii. Remediation
    viii. Determine desired state and perform gap analysis against an accepted standard or law (including GDPR)
    ix. Program assurance, including audits
b. Processors and third-party vendor assessment
    i. Evaluate processors and third-party vendors, insourcing and outsourcing privacy risks, including rules of international data transfer
        1. Privacy and information security policies
        2. Access controls
        3. Where personal information is being held
        4. Who has access to personal information
    ii. Understand and leverage the different types of relationships
        1. Internal audit

2. Information security
3. Physical security
4. Data protection authority

iii. Risk assessment
1. Type of data being outsourced
2. Location of data
3. Implications of cloud computing strategies
4. Legal compliance
5. Records retention
6. Contractual requirements (incident response, etc.)
7. Establish minimum standards for safeguarding information

iv. Contractual requirements
v. Ongoing monitoring and auditing

c. Physical assessments
i. Identify operational risk
1. Data centers and offices
2. Physical access controls
3. Document destruction
4. Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.)
5. Device forensics
6. Device security (e.g., mobile devices, Internet of Things (IoT), geo-tracking, imaging/copier hard drive security controls)

d. Mergers, acquisitions and divestitures
i. Due diligence
ii. Risk assessment

e. Conduct analysis and assessments, as needed or appropriate
i. Privacy Threshold Analysis (PTAs) on systems, applications and processes
ii. Privacy Impact Assessments (PIAs)
1. Define a process for conducting Privacy Impact Assessments
a. Understand the life cycle of a PIA
b. Incorporate PIA into system, process, product life cycles

B. <u>Protect</u>

a. Data life cycle and governance (creation to deletion)
b. Information security practices
i. Access controls for physical and virtual systems
1. Access control on need to know
2. Account management (e.g., provision process)
3. Privilege management

ii. Technical security controls
iii. Implement appropriate administrative safeguards

c. Privacy by Design
i. Integrate privacy throughout the system development life cycle (SDLC)
ii. Establish privacy gates as part of the system development framework

C. <u>Sustain</u>

a. Measure
i. Quantify the costs of technical controls
ii. Manage data retention with respect to the organization's policies

iii. Define the methods for physical and electronic data destruction
iv. Define roles and responsibilities for managing the sharing and disclosure of data for internal and external use

b. Align
   i. Integrate privacy requirements and representation into functional areas across the organization
      1. Information security
      2. IT operations and development
      3. Business continuity and disaster recovery planning
      4. Mergers, acquisitions and divestitures
      5. Human resources
      6. Compliance and ethics
      7. Audit
      8. Marketing/business development
      9. Public relations
      10. Procurement/sourcing
      11. Legal and contracts
      12. Security/emergency services
      13. Finance
      14. Others

c. Audit
   i. Align privacy operations to an internal and external compliance audit program
      1. Knowledge of audit processes
      2. Align to industry standards
   ii. Audit compliance with privacy policies and standards
   iii. Audit data integrity and quality and communicate audit findings with stakeholders
   iv. Audit information access, modification and disclosure accounting

d. Communicate
   i. Awareness
      1. Create awareness of the organization's privacy program internally and externally
      2. Ensure policy flexibility in order to incorporate legislative/regulatory/market requirements
      3. Develop internal and external communication plans to ingrain organizational accountability
      4. Identify, catalog and maintain documents requiring updates as privacy requirements change
   ii. Targeted employee, management and contractor training
      1. Privacy policies
      2. Operational privacy practices (e.g., standard operating instructions), such as
         a. Data creation/usage/retention/disposal
         b. Access control
         c. Reporting incidents
         d. Key contacts

e. Monitor
   i. Environment (e.g., systems, applications) monitoring
   ii. Monitor compliance with established privacy policies
   iii. Monitor regulatory and legislative changes
   iv. Compliance monitoring (e.g. collection, use and retention)
      1. Internal audit

2. Self-regulation
3. Retention strategy
4. Exit strategy

D. Respond

a. Information requests
   i. Access
   ii. Redress
   iii. Correction
   iv. Managing data integrity

b. Privacy incidents
   i. Legal compliance
      1. Preventing harm
      2. Collection limitations
      3. Accountability
      4. Monitoring and enforcement
   ii. Incident response planning
      1. Understand key roles and responsibilities
         a. Identify key business stakeholders
            1. Information security
            2. Legal
            3. Audit
            4. Human resources
            5. Marketing
            6. Business development
            7. Communications and public relations
            8. Other
         b. Establish incident oversight teams
      2. Develop a privacy incident response plan
      3. Identify elements of the privacy incident response plan
      4. Integrate privacy incident response into business continuity planning
   iii. Incident detection
      1. Define what constitutes a privacy incident
      2. Identify reporting process
      3. Coordinate detection capabilities
         a. Organization IT
         b. Physical security
         c. Human resources
         d. Investigation teams
         e. Vendors
   iv. Incident handling
      1. Understand key roles and responsibilities
      2. Develop a communications plan to notify executive management
   v. Follow incident response process to ensure meeting jurisdictional, global and business requirements
      1. Engage privacy team
      2. Review the facts
      3. Conduct analysis
      4. Determine actions (contain, communicate, etc.)
      5. Execute
      6. Monitor

7. Review and apply lessons learned

vi. Identify incident reduction techniques

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