Certified Information Privacy Manager (CIPM) Training

Developing a Privacy Program

1. Create a company vision
- Acquire knowledge on privacy approaches
- Evaluate the intended objective
- Gain executive sponsor approval for this vision
1. Establish a Data Governance model
- Centralized
- Distributed
- Hybrid
1. Establish a privacy program
- Define program scope and charter
- Identify the source, types, and uses of personal information (PI) within the organization and the applicable laws
- Develop a privacy strategy
1. Structure the privacy team
- Establish the organizational model, responsibilities and reporting structure appropriate to the size of the organization
- Designate a point of contact for privacy issues
- Establish/endorse the measurement of professional competency
1. Communicate
- Awareness

Privacy Program Framework

1. Develop the Privacy Program Framework
- Develop organizational privacy policies, standards, and/or guidelines
- Define privacy program activities
1. Implement the Privacy Program Framework
- Communicate the framework to internal and external stakeholders
- Ensure continuous alignment to applicable laws and regulations to support the development of an organizational privacy program framework
1. Develop Appropriate Metrics
- Identify intended audience for metrics
- Define reporting resources
- Define privacy metrics for oversight and governance per audience
- Identify systems/application collection points

Privacy Operational Life Cycle: Assess

1. Document current baseline of your privacy program
- Education and awareness
- Monitoring and responding to the regulatory environment
- Internal policy compliance

- Data, systems and process assessment
- Risk assessment (PIAs, etc.)
- Incident response
- Remediation
- Determine desired state and perform gap analysis against an accepted standard or law (including GDPR)
- Program assurance, including audits

1. Processors and third-party vendor assessment

- Evaluate processors and third-party vendors, insourcing and outsourcing privacy risks, including rules of international data transfer
- Understand and leverage the different types of relationships
- Risk assessment
- Contractual requirements
- Ongoing monitoring and auditing

1. Physical assessments

- Identify operational risk

1. Mergers, acquisitions and divestitures

- Due diligence
- Risk assessment

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

- Privacy Threshold Analysis (PTAs) on systems, applications and processes
- Privacy Impact Assessments (PIAs)

Privacy Operational Life Cycle: Protect

1. Information security practices

- Access controls for physical and virtual systems
- Technical security controls
- Implement appropriate administrative safeguards

1. Privacy by Design

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

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

- Information security
- IT operations and development
- Business continuity and disaster recovery planning
- Mergers, acquisitions and divestitures
- Human resources
- Compliance and ethics
- Audit
- Marketing/business development

- Public relations
- Procurement/sourcing
- Legal and contracts
- Security/emergency services
- Finance
- Others

1. Other organizational measures

- Quantify the costs of technical controls
- Manage data retention with respect to the organization's policies
- Define the methods for physical and electronic data destruction
- Define roles and responsibilities for managing the sharing and disclosure of data for internal and external use

Privacy Operational Life Cycle: Sustain

1. Monitor

- Environment (e.g., systems, applications) monitoring
- Monitor compliance with established privacy policies
- Monitor regulatory and legislative changes
- Compliance monitoring (e.g. collection, use and retention)

1. Audit

- Align privacy operations to an internal and external compliance audit program
- Audit compliance with privacy policies and standards
- Audit data integrity and quality and communicate audit findings with stakeholders
- Audit information access, modification and disclosure accounting
- Targeted employee, management and contractor training

Privacy Operational Life Cycle: Respond

1. Data-subject information requests and privacy rights

- Access
- Redress
- Correction
- Managing data integrity
- Right of Erasure
- Right to be informed
- Control over use of data

1. Privacy incident response

- Legal compliance
- Incident response planning
- Incident detection
- Incident handling

- Follow incident response process to ensure meeting jurisdictional, global and business requirements
- Identify incident reduction techniques
- Incident metrics—quantify the cost of a privacy incident