The Skill Set Needed to Implement the NIST Privacy Framework

By IAPP Data Scientist & Strategist Suzannah Hicks
The Skill Set Needed to Implement the NIST Privacy Framework

NIST Privacy Framework Version 1.0 alignment with IAPP CIPM certification

By IAPP Data Scientist & Strategist Suzannah Hicks

To offer insight into the professional skillset needed to implement the NIST Privacy Framework, the International Association of Privacy Professionals’ Westin Research Center mapped the Privacy Framework’s Core to the Body of Knowledge for a Certified Information Privacy Manager. This body of knowledge was created by the IAPP’s certification advisory board to reflect the skillset and knowledge required by a privacy professional working in the field. It is annually updated, as required by IAPP’s ANSI accreditation, through a formal process to determine what professionals in the field are currently doing, under what conditions, and with what levels of knowledge and skill. The IAPP’s CIPM certification is then updated to align with this body of knowledge. The CIPM Body of Knowledge was updated June 1, 2020 and this document reflects the current version.

As a privacy risk management framework, NIST’s Privacy Framework aligns closely with the CIPM body of knowledge. However, it should be noted that as a framework designed to bring together stakeholders across disciplines, additional skills are needed to go deeper into certain aspects of the Privacy Framework. For instance, lawyers implementing the governance policies, processes, and procedures category will require greater familiarity with the legal regimes in the jurisdictions in which their organizations operate, skillsets more closely aligned with IAPP’s regionally based CIPP bodies of knowledge. Similarly, privacy engineers assessing options for de-identification techniques under the disassociated processing category will need more technical knowledge, such as that reflected in IAPP’s CIPT body of knowledge. The NIST Framework and the CIPM body of knowledge can serve as the bridge between these stakeholders.

The IAPP’s Westin Research Center developed the following table to document how NIST’s Privacy Framework, and more generally a risk management framework designed to bring together security and privacy professionals, aligns with IAPP’s CIPM certification. The first mapping of the NIST Privacy Framework’s Core to the CIPM Body of Knowledge can help inform privacy professionals seeking
to understand the skillset needed to implement the Privacy Framework. The second mapping of the CIPM to the NIST Framework will inform IAPP’s own work to ensure its certifications are continually refined to meet the needs of the privacy profession across sectors and disciplines.

### Mapping the NIST privacy framework core v1.0 to IAPP’s CIPM body of knowledge v2.04

<table>
<thead>
<tr>
<th>NIST Privacy Framework Core</th>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identify-P (ID-P):</strong></td>
<td><strong>Domain III. Privacy Operational Life Cycle: Assess</strong></td>
</tr>
<tr>
<td>Develop the organizational understanding to manage privacy risk for individuals arising from data processing.</td>
<td>A. Document current baseline of your privacy program.</td>
</tr>
<tr>
<td><strong>Inventory and Mapping (ID.IM-P):</strong></td>
<td>a. Education and awareness.</td>
</tr>
<tr>
<td>Data processing by systems, products, or services is understood and informs the management of privacy risk.</td>
<td>b. Monitoring and responding to the regulatory environment.</td>
</tr>
<tr>
<td></td>
<td>c. Internal policy compliance.</td>
</tr>
<tr>
<td></td>
<td>d. Data, systems and process assessment.</td>
</tr>
<tr>
<td></td>
<td>i. Map data inventories, flows and classification.</td>
</tr>
<tr>
<td></td>
<td>ii. Create “record of authority” of systems processing personal information within the organization.</td>
</tr>
<tr>
<td></td>
<td>1. Map and document data flow in systems and applications.</td>
</tr>
<tr>
<td></td>
<td>2. Analyze and classify types and uses of data.</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Business Environment (ID.BE-P): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.</td>
<td></td>
</tr>
</tbody>
</table>

**Domain I. Developing a Privacy Program**

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

C. Establish 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.
      a. Business alignment.
         i. Finalize the operational business case for privacy.
         ii. Identify stakeholders.
         iii. Leverage key functions.
         iv. Create a process for interfacing within organization.
         v. Align organizational culture and privacy/data protection objectives.
      b. Obtain funding/budget for privacy and the privacy team.
      c. Develop a data governance strategy for personal information (collection, authorized use, access, destruction).
      d. Plan inquiry/complaint handling procedures (customers, regulators, etc.).
      e. Ensure program flexibility in order to incorporate legislative/regulatory/market/business requirements.
### Risk Assessment (ID.RA-P)

The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.

<table>
<thead>
<tr>
<th>NIST Privacy Framework Core</th>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Function</strong></td>
<td><strong>Category</strong></td>
</tr>
<tr>
<td><strong>Domain III. Privacy Operational Life Cycle: Assess</strong></td>
<td></td>
</tr>
<tr>
<td>A. Document current baseline of your privacy program.</td>
<td></td>
</tr>
<tr>
<td>d. Data, systems and process assessment.</td>
<td></td>
</tr>
<tr>
<td>i. Map data inventories, flows and classification.</td>
<td></td>
</tr>
<tr>
<td>ii. Create “record of authority” of systems processing personal information within the organization.</td>
<td></td>
</tr>
<tr>
<td>e. Risk assessment (PIAs, etc.).</td>
<td></td>
</tr>
<tr>
<td><strong>C. Physical assessments.</strong></td>
<td></td>
</tr>
<tr>
<td>a. Identify operational risk.</td>
<td></td>
</tr>
<tr>
<td>i. Data centers and offices.</td>
<td></td>
</tr>
<tr>
<td>ii. Physical access controls.</td>
<td></td>
</tr>
<tr>
<td>iii. Document destruction.</td>
<td></td>
</tr>
<tr>
<td>iv. Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.).</td>
<td></td>
</tr>
<tr>
<td>v. Device forensics.</td>
<td></td>
</tr>
<tr>
<td>vi. Device security (e.g., mobile devices, Internet of Things (IoT), geo-tracking, imaging/copier hard drive security controls).</td>
<td></td>
</tr>
<tr>
<td><strong>D. Mergers, acquisitions and divestitures.</strong></td>
<td></td>
</tr>
<tr>
<td>a. Due diligence.</td>
<td></td>
</tr>
<tr>
<td>b. Risk assessment.</td>
<td></td>
</tr>
<tr>
<td><strong>E. Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs).</strong></td>
<td></td>
</tr>
<tr>
<td>a. Privacy Threshold Analysis (PTAs) on systems, applications and processes.</td>
<td></td>
</tr>
<tr>
<td>b. Privacy Impact Assessments (PIAs).</td>
<td></td>
</tr>
<tr>
<td>i. Define a process for conducting Privacy Impact Assessments.</td>
<td></td>
</tr>
<tr>
<td>1. Understand the life cycle of a PIA.</td>
<td></td>
</tr>
<tr>
<td>2. Incorporate PIA into system, process, product life cycles.</td>
<td></td>
</tr>
</tbody>
</table>
## NIST Privacy Framework Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Processing Ecosystem Risk Management (ID.DE-P):</td>
<td></td>
</tr>
<tr>
<td>The organization’s priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.</td>
<td></td>
</tr>
</tbody>
</table>

### Domain III. Privacy Operational Life Cycle: Assess

#### 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 Processors and third-party vendor assessment.
### Domain I. Developing a Privacy Program

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

B. Establish Data Governance model.
   a. Centralized.
   b. Distributed.
   c. Hybrid.

C. Establish 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.
      a. Business alignment.
         i. Finalize the operational business case for privacy.
         ii. Identify stakeholders.
         iii. Leverage key functions.
         iv. Create a process for interfacing within organization.
         v. Align organizational culture and privacy/data protection objectives.
      b. Obtain funding/budget for privacy and the privacy team.
      c. Develop a data governance strategy for personal information (collection, authorized use, access, destruction).
      d. Plan inquiry/complaint handling procedures (customers, regulators, etc.).
      e. Ensure program flexibility in order to incorporate legislative/regulatory/market/business requirements.

---

### NIST Privacy Framework Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Govern-P (GV-P):</strong> Develop and implement the organizational governance structure to enable an ongoing understanding of the organization’s risk management priorities that are informed by privacy risk.</td>
<td></td>
</tr>
<tr>
<td><strong>Governance Policies, Processes, and Procedures (GV.PO-P):</strong> The policies, processes, and procedures to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.</td>
<td></td>
</tr>
<tr>
<td>NIST Privacy Framework Core</td>
<td>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
</tr>
<tr>
<td>D. Structure the privacy team.</td>
<td></td>
</tr>
<tr>
<td>a. Establish the organizational model, responsibilities and reporting structure appropriate to the size of the organization.</td>
<td></td>
</tr>
<tr>
<td>i. Large organizations.</td>
<td></td>
</tr>
<tr>
<td>1. Chief privacy officer.</td>
<td></td>
</tr>
<tr>
<td>2. Privacy manager.</td>
<td></td>
</tr>
<tr>
<td>3. Privacy analysts.</td>
<td></td>
</tr>
<tr>
<td>4. Business line privacy leaders.</td>
<td></td>
</tr>
<tr>
<td>5. “First responders.”</td>
<td></td>
</tr>
<tr>
<td>ii. Small organizations/sole data protection officer (DPO) including when not only job.</td>
<td></td>
</tr>
<tr>
<td>b. Designate a point of contact for privacy issues.</td>
<td></td>
</tr>
<tr>
<td>c. Establish/endorse the measurement of professional competency.</td>
<td></td>
</tr>
<tr>
<td>E. Communicate.</td>
<td></td>
</tr>
<tr>
<td>a. Awareness.</td>
<td></td>
</tr>
<tr>
<td>i. Create awareness of the organization’s privacy program internally and externally.</td>
<td></td>
</tr>
<tr>
<td>ii. Develop internal and external communication plans to ingrain organizational accountability.</td>
<td></td>
</tr>
<tr>
<td>iii. Identify, catalog and maintain documents requiring updates as privacy requirements changes.</td>
<td></td>
</tr>
<tr>
<td>NIST Privacy Framework Core</td>
<td>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Domain II. Privacy Program Framework</strong></td>
<td></td>
</tr>
<tr>
<td>A. Develop the Privacy Program Framework.</td>
<td></td>
</tr>
<tr>
<td>a. Develop organizational privacy policies, standards and/or guidelines.</td>
<td></td>
</tr>
<tr>
<td>b. Define privacy program activities.</td>
<td></td>
</tr>
<tr>
<td>i. Education and awareness.</td>
<td></td>
</tr>
<tr>
<td>ii. Monitoring and responding to the regulatory environment.</td>
<td></td>
</tr>
<tr>
<td>iii. Internal policy compliance.</td>
<td></td>
</tr>
<tr>
<td>iv. Data inventories, data flows, and classification.</td>
<td></td>
</tr>
<tr>
<td>v. Risk assessment (Privacy Impact Assessments [PIAs]) (e.g., DPIAs etc.).</td>
<td></td>
</tr>
<tr>
<td>vi. Incident response and process, including jurisdictional regulations.</td>
<td></td>
</tr>
<tr>
<td>vii. Remediation.</td>
<td></td>
</tr>
<tr>
<td>viii. Program assurance, including audits.</td>
<td></td>
</tr>
<tr>
<td>B. Implement the Privacy Program Framework.</td>
<td></td>
</tr>
<tr>
<td>a. Communicate the framework to internal and external stakeholders.</td>
<td></td>
</tr>
<tr>
<td>b. Ensure continuous alignment to applicable laws and regulations to support the development of an organizational privacy program framework.</td>
<td></td>
</tr>
<tr>
<td>i. Understand when national laws and regulations apply (e.g. GDPR).</td>
<td></td>
</tr>
<tr>
<td>ii. Understand when local laws and regulations apply (e.g. CCPA).</td>
<td></td>
</tr>
<tr>
<td>iii. Understand penalties for noncompliance with laws and regulations.</td>
<td></td>
</tr>
<tr>
<td>iv. Understand the scope and authority of oversight agencies (e.g., Data Protection Authorities, Privacy Commissioners, Federal Trade Commission, etc.).</td>
<td></td>
</tr>
<tr>
<td>v. Understand privacy implications of doing business with or basing operations in countries with inadequate, or without, privacy laws.</td>
<td></td>
</tr>
<tr>
<td>NIST Privacy Framework Core</td>
<td>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
</tr>
<tr>
<td>vi.</td>
<td>Maintain the ability to manage a global privacy function.</td>
</tr>
<tr>
<td>vii.</td>
<td>Maintain the ability to track multiple jurisdictions for changes in privacy law.</td>
</tr>
<tr>
<td>viii.</td>
<td>Understand international data sharing arrangement agreements.</td>
</tr>
<tr>
<td>The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</td>
<td>E. Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs).</td>
</tr>
<tr>
<td></td>
<td>a. Privacy Threshold Analysis (PTAs) on systems, applications and processes.</td>
</tr>
<tr>
<td></td>
<td>b. Privacy Impact Assessments (PIAs).</td>
</tr>
<tr>
<td></td>
<td>i. Define a process for conducting Privacy Impact Assessments.</td>
</tr>
<tr>
<td></td>
<td>1. Understand the life cycle of a PIA.</td>
</tr>
<tr>
<td></td>
<td>2. Incorporate PIA into system, process, product life cycles.</td>
</tr>
<tr>
<td><strong>Awareness and Training (GV.AT-P):</strong></td>
<td><strong>Domain I. Developing a Privacy Program</strong></td>
</tr>
<tr>
<td>The organization’s workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.</td>
<td>E. Communicate.</td>
</tr>
<tr>
<td></td>
<td>a. Awareness.</td>
</tr>
<tr>
<td></td>
<td>i. Create awareness of the organization’s privacy program internally and externally.</td>
</tr>
<tr>
<td></td>
<td>ii. Develop internal and external communication plans to ingrain organizational accountability.</td>
</tr>
<tr>
<td></td>
<td>iii. Identify, catalog and maintain documents requiring updates as privacy requirements changes.</td>
</tr>
<tr>
<td></td>
<td>Education and awareness.</td>
</tr>
<tr>
<td>NIST Privacy Framework Core</td>
<td>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Function</strong></td>
<td><strong>Category</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain V. Privacy Operational Life Cycle: Sustain</td>
</tr>
<tr>
<td>B. Audit</td>
<td></td>
</tr>
<tr>
<td>e. Targeted employee, management and contractor training.</td>
<td></td>
</tr>
<tr>
<td>i. Privacy policies.</td>
<td></td>
</tr>
<tr>
<td>ii. Operational privacy practices (e.g., standard operating instructions), such as:</td>
<td></td>
</tr>
<tr>
<td>1. Data creation/usage/retention/disposal.</td>
<td></td>
</tr>
<tr>
<td>2. Access control.</td>
<td></td>
</tr>
<tr>
<td>3. Reporting incidents.</td>
<td></td>
</tr>
<tr>
<td>4. Key contacts.</td>
<td></td>
</tr>
</tbody>
</table>

**Domain I. Developing a Privacy Program**

C. Establish a privacy program.

c. Develop a privacy strategy.

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

**Domain II. Privacy Program Framework**

A. Develop the Privacy Program Framework.

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.

**Monitoring and Review (GV. MT-P):** The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>C. Develop Appropriate Metrics.</td>
<td></td>
</tr>
<tr>
<td>a. Identify intended audience for metrics.</td>
<td></td>
</tr>
<tr>
<td>b. Define reporting resources.</td>
<td></td>
</tr>
<tr>
<td>c. Define privacy metrics for oversight and governance per audience.</td>
<td></td>
</tr>
<tr>
<td>i. Compliance metrics (examples, will vary by organization).</td>
<td></td>
</tr>
<tr>
<td>1. Collection (notice).</td>
<td></td>
</tr>
<tr>
<td>2. Responses to data subject inquiries.</td>
<td></td>
</tr>
<tr>
<td>3. Use.</td>
<td></td>
</tr>
<tr>
<td>4. Retention.</td>
<td></td>
</tr>
<tr>
<td>5. Disclosure to third parties.</td>
<td></td>
</tr>
<tr>
<td>6. Incidents (breaches, complaints, inquiries).</td>
<td></td>
</tr>
<tr>
<td>7. Employees trained.</td>
<td></td>
</tr>
<tr>
<td>8. PIA metrics.</td>
<td></td>
</tr>
<tr>
<td>10. Percent of company functions represented by governance mechanisms.</td>
<td></td>
</tr>
<tr>
<td>ii. Trending.</td>
<td></td>
</tr>
<tr>
<td>iii. Privacy program return on investment (ROI).</td>
<td></td>
</tr>
<tr>
<td>iv. Business resiliency metrics Privacy program maturity level.</td>
<td></td>
</tr>
<tr>
<td>v. Resource utilization.</td>
<td></td>
</tr>
<tr>
<td>d. Identify systems/application collection points.</td>
<td></td>
</tr>
<tr>
<td>NIST Privacy Framework Core</td>
<td>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Domain 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.  

**Domain 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.
## NIST Privacy Framework Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
</table>

### IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04

#### Domain VI. Privacy Operational Life Cycle: Respond

**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.
      - 1. Information security.
      - 2. Legal.
      - 3. Audit.
      - 4. Human resources.
      - 5. Marketing.
      - 7. Communications and public relations.
    - 8. 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.**
  - 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.
<table>
<thead>
<tr>
<th>NIST Privacy Framework Core</th>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Function</strong></td>
<td><strong>Category</strong></td>
</tr>
<tr>
<td></td>
<td>d. Incident handling.</td>
</tr>
<tr>
<td></td>
<td>1. Understand key roles and responsibilities.</td>
</tr>
<tr>
<td></td>
<td>2. Develop a communications plan to notify executive management.</td>
</tr>
<tr>
<td></td>
<td>e. Follow incident response process to ensure meeting jurisdictional, global and business requirements.</td>
</tr>
<tr>
<td></td>
<td>1. Engage privacy team.</td>
</tr>
<tr>
<td></td>
<td>2. Review the facts.</td>
</tr>
<tr>
<td></td>
<td>3. Conduct analysis.</td>
</tr>
<tr>
<td></td>
<td>4. Determine actions (contain, communicate, etc.).</td>
</tr>
<tr>
<td></td>
<td>5. Execute.</td>
</tr>
<tr>
<td></td>
<td>7. Review and apply lessons learned.</td>
</tr>
<tr>
<td></td>
<td>f. Identify incident reduction techniques.</td>
</tr>
<tr>
<td></td>
<td>g. Incident metrics—quantify the cost of a privacy incident.</td>
</tr>
</tbody>
</table>

**Control-P (CT-P):** Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

**Data Processing Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization’s risk strategy to protect individuals’ privacy.

**Domain I. Developing a Privacy Program**

C. Establish a privacy program.

c. Develop a privacy strategy.

iii. Develop a data governance strategy for personal information (collection, authorized use, access, destruction).
<table>
<thead>
<tr>
<th>NIST Privacy Framework Core</th>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>Category</td>
</tr>
<tr>
<td></td>
<td>Domain IV. Privacy Operational Life Cycle: Protect</td>
</tr>
<tr>
<td></td>
<td>B. Privacy by Design.</td>
</tr>
<tr>
<td></td>
<td>a. Integrate privacy throughout the system development life cycle (SDLC).</td>
</tr>
<tr>
<td></td>
<td>b. Establish privacy gates as part of the system development framework C.</td>
</tr>
<tr>
<td></td>
<td>Integrate privacy requirements and representation into functional areas across the organization.</td>
</tr>
<tr>
<td></td>
<td>i. Information security.</td>
</tr>
<tr>
<td></td>
<td>ii. IT operations and development.</td>
</tr>
<tr>
<td></td>
<td>iii. Business continuity and disaster recovery planning.</td>
</tr>
<tr>
<td></td>
<td>iv. Mergers, acquisitions and divestitures.</td>
</tr>
<tr>
<td></td>
<td>v. Human resources.</td>
</tr>
<tr>
<td></td>
<td>vi. Compliance and ethics.</td>
</tr>
<tr>
<td></td>
<td>vii. Audit.</td>
</tr>
<tr>
<td></td>
<td>viii. Marketing/business development.</td>
</tr>
<tr>
<td></td>
<td>ix. Public relations.</td>
</tr>
<tr>
<td></td>
<td>x. Procurement/sourcing.</td>
</tr>
<tr>
<td></td>
<td>xi. Legal and contracts.</td>
</tr>
<tr>
<td></td>
<td>xii. Security/emergency services.</td>
</tr>
<tr>
<td></td>
<td>xiii. Finance.</td>
</tr>
<tr>
<td></td>
<td>xiv. Others.</td>
</tr>
<tr>
<td></td>
<td>D. Other Organizational Measures.</td>
</tr>
<tr>
<td></td>
<td>a. Quantify the costs of technical controls.</td>
</tr>
<tr>
<td></td>
<td>b. Manage data retention with respect to the organization’s policies.</td>
</tr>
<tr>
<td></td>
<td>c. Define the methods for physical and electronic data destruction.</td>
</tr>
<tr>
<td></td>
<td>d. Define roles and responsibilities for managing the sharing and disclosure of data for internal and external use.</td>
</tr>
<tr>
<td>NIST Privacy Framework Core</td>
<td>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Data Processing Management (CT. DM-P):** Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization). | **Domain III. Privacy Operational Life Cycle: Assess**

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.

**Domain 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.
<table>
<thead>
<tr>
<th>NIST Privacy Framework Core</th>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Function</strong></td>
<td><strong>Domain I. Developing a Privacy Program</strong></td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>C. Establish a privacy program.</td>
</tr>
<tr>
<td>Disassociated Processing (CT. DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).</td>
<td>c. Develop a privacy strategy.</td>
</tr>
<tr>
<td></td>
<td>iii. Develop a data governance strategy for personal information (collection, authorized use, access, destruction).</td>
</tr>
<tr>
<td></td>
<td><strong>Domain IV. Privacy Operational Life Cycle: Protect</strong></td>
</tr>
<tr>
<td></td>
<td>B. Privacy by Design.</td>
</tr>
<tr>
<td></td>
<td>a. Integrate privacy throughout the system development life cycle (SDLC).</td>
</tr>
<tr>
<td></td>
<td>b. Establish privacy gates as part of the system development framework.</td>
</tr>
<tr>
<td></td>
<td><strong>Domain VI. Privacy Operational Life Cycle: Respond</strong></td>
</tr>
<tr>
<td></td>
<td>B. Privacy incident response.</td>
</tr>
<tr>
<td></td>
<td>a. Legal compliance.</td>
</tr>
<tr>
<td></td>
<td>ii. Collection limitations.</td>
</tr>
<tr>
<td><strong>Communicate-P (CM-P):</strong></td>
<td><strong>Domain I. Developing a Privacy Program</strong></td>
</tr>
<tr>
<td></td>
<td>E. Communicate.</td>
</tr>
<tr>
<td>Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.</td>
<td>a. Awareness.</td>
</tr>
<tr>
<td></td>
<td>i. Create awareness of the organization's privacy program internally and externally.</td>
</tr>
<tr>
<td></td>
<td>ii. Develop internal and external communication plans to ingrain organizational accountability.</td>
</tr>
<tr>
<td></td>
<td>iii. Identify, catalog and maintain documents requiring updates as privacy requirements changes.</td>
</tr>
<tr>
<td><strong>Communication Policies, Processes, and Procedures (CM.PO-P):</strong> Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.</td>
<td></td>
</tr>
</tbody>
</table>
### NIST Privacy Framework Core

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Data Processing Awareness (CM. AW-P):** Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization’s risk strategy to protect individuals’ privacy.

### IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04

**Domain I. Developing a Privacy Program**

**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 changes.

**Domain VI. Privacy Operational Life Cycle: Respond**

**A. Data-subject information requests and privacy rights.**

a. **Access.**

b. **Redress.**

c. **Correction.**

d. **Managing data integrity.**

**B. Privacy incident response.**

a. **Legal compliance.**
   i. Preventing harm.
   ii. Collection limitations.
   iii. Accountability.
   iv. Monitoring and enforcement.
<table>
<thead>
<tr>
<th>NIST Privacy Framework Core</th>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>Category</td>
</tr>
<tr>
<td></td>
<td>b. Incident response planning.</td>
</tr>
<tr>
<td></td>
<td>i. Understand key roles and responsibilities.</td>
</tr>
<tr>
<td></td>
<td>1. Identify key business stakeholders.</td>
</tr>
<tr>
<td></td>
<td>2. Information security.</td>
</tr>
<tr>
<td></td>
<td>3. Legal.</td>
</tr>
<tr>
<td></td>
<td>4. Audit.</td>
</tr>
<tr>
<td></td>
<td>5. Human resources.</td>
</tr>
<tr>
<td></td>
<td>8. Communications and public relations.</td>
</tr>
<tr>
<td></td>
<td>9. Other.</td>
</tr>
<tr>
<td></td>
<td>2. Establish incident oversight teams.</td>
</tr>
<tr>
<td></td>
<td>3. Develop a privacy incident response plan.</td>
</tr>
<tr>
<td></td>
<td>4. Identify elements of the privacy incident response plan.</td>
</tr>
<tr>
<td></td>
<td>5. Integrate privacy incident response into business continuity planning.</td>
</tr>
<tr>
<td></td>
<td>c. Incident detection.</td>
</tr>
<tr>
<td></td>
<td>1. Define what constitutes a privacy incident.</td>
</tr>
<tr>
<td></td>
<td>2. Identify reporting process.</td>
</tr>
<tr>
<td></td>
<td>3. Coordinate detection capabilities.</td>
</tr>
<tr>
<td></td>
<td>a. Organization IT.</td>
</tr>
<tr>
<td></td>
<td>b. Physical security.</td>
</tr>
<tr>
<td></td>
<td>c. Human resources.</td>
</tr>
<tr>
<td></td>
<td>d. Investigation teams.</td>
</tr>
<tr>
<td></td>
<td>e. Vendors.</td>
</tr>
<tr>
<td></td>
<td>d. Incident handling.</td>
</tr>
<tr>
<td></td>
<td>1. Understand key roles and responsibilities.</td>
</tr>
<tr>
<td></td>
<td>2. Develop a communications plan to notify executive management.</td>
</tr>
<tr>
<td></td>
<td>e. Follow incident response process to ensure meeting jurisdictional, global and business requirements.</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>1. Engage privacy team.</td>
<td></td>
</tr>
<tr>
<td>2. Review the facts.</td>
<td></td>
</tr>
<tr>
<td>3. Conduct analysis.</td>
<td></td>
</tr>
<tr>
<td>4. Determine actions (contain, communicate, etc.).</td>
<td></td>
</tr>
<tr>
<td>5. Execute.</td>
<td></td>
</tr>
<tr>
<td>7. Review and apply lessons learned.</td>
<td></td>
</tr>
<tr>
<td>f. Identify incident reduction techniques.</td>
<td></td>
</tr>
<tr>
<td>g. Incident metrics—quantify the cost of a privacy incident.</td>
<td></td>
</tr>
</tbody>
</table>

**Domain VI. Privacy Operational Life Cycle: Respond**

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.
            1. Information security.
            2. Legal.
            3. Audit.
            4. Human resources.
            5. Marketing.
            7. Communications and public relations.
            8. 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.

**Data Protection Policies, Processes, and Procedures (PR.PO-P):**

Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.
<table>
<thead>
<tr>
<th>NIST Privacy Framework Core</th>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>Category</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Domain V. Privacy Operational Life Cycle: Sustain</strong></td>
<td></td>
</tr>
<tr>
<td>A. Monitor.</td>
<td></td>
</tr>
<tr>
<td>a. Environment (e.g., systems, applications) monitoring.</td>
<td></td>
</tr>
<tr>
<td>b. Monitor compliance with established privacy policies.</td>
<td></td>
</tr>
<tr>
<td>c. Monitor regulatory and legislative changes.</td>
<td></td>
</tr>
<tr>
<td>d. Compliance monitoring (e.g. collection, use and retention).</td>
<td></td>
</tr>
<tr>
<td>i. Internal audit.</td>
<td></td>
</tr>
<tr>
<td>ii. Self-regulation.</td>
<td></td>
</tr>
<tr>
<td>iii. Retention strategy.</td>
<td></td>
</tr>
<tr>
<td>iv. Exit strategy.</td>
<td></td>
</tr>
<tr>
<td><strong>Identity Management, Authentication, and Access Control (PR.AC-P):</strong></td>
<td></td>
</tr>
<tr>
<td>Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.</td>
<td></td>
</tr>
<tr>
<td><strong>Domain V. Privacy Operational Life Cycle: Protect</strong></td>
<td></td>
</tr>
<tr>
<td>A. Information security practices.</td>
<td></td>
</tr>
<tr>
<td>a. Access controls for physical and virtual systems.</td>
<td></td>
</tr>
<tr>
<td>i. Access control on need to know.</td>
<td></td>
</tr>
<tr>
<td>ii. Account management (e.g., provision process).</td>
<td></td>
</tr>
<tr>
<td>iii. Privilege management.</td>
<td></td>
</tr>
<tr>
<td><strong>Data Security (PR.DS-P):</strong> Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.</td>
<td></td>
</tr>
<tr>
<td><strong>Domain V. Privacy Operational Life Cycle: Protect</strong></td>
<td></td>
</tr>
<tr>
<td>A. Information security practices.</td>
<td></td>
</tr>
<tr>
<td>b. Technical security controls.</td>
<td></td>
</tr>
<tr>
<td>NIST Privacy Framework Core</td>
<td>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Function</strong></td>
<td><strong>Domain V. Privacy Operational Life Cycle: Protect</strong></td>
</tr>
<tr>
<td>Maintenance (PR.MA-P)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System maintenance and repairs are performed consistent with policies, processes, and procedures.</td>
</tr>
<tr>
<td></td>
<td><strong>Domain III. Privacy Operational Life Cycle: Assess</strong></td>
</tr>
<tr>
<td>Protective Technology (PR.PT-P)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.</td>
</tr>
<tr>
<td></td>
<td>C. Physical assessments.</td>
</tr>
<tr>
<td></td>
<td>a. Identify operational risk.</td>
</tr>
<tr>
<td></td>
<td>i. Data centers and offices.</td>
</tr>
<tr>
<td></td>
<td>ii. Physical access controls.</td>
</tr>
<tr>
<td></td>
<td>iii. Document destruction.</td>
</tr>
<tr>
<td></td>
<td>iv. Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.).</td>
</tr>
<tr>
<td></td>
<td>v. Device forensics.</td>
</tr>
<tr>
<td></td>
<td>vi. Device security (e.g., mobile devices, Internet of Things (IoT), geo-tracking, imaging/copier hard drive security controls).</td>
</tr>
</tbody>
</table>
## Mapping IAPP’s CIPM body of knowledge v2.04 to the NIST privacy framework core v1.0

<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain I. Developing a Privacy Program</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **A. Create a company vision** | **Business Environment (ID.BE-P):** The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.  
**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. |
| a. Acquire knowledge on privacy approaches.  
b. Evaluate the intended objective.  
c. Gain executive sponsor approval for this vision. |  |
| **B. Establish a Data Governance model** | **Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. |
| a. Centralized.  
b. Distributed.  
c. Hybrid. |  |
<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
</table>
| 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.  
a. Business alignment.  
   i. Finalize the operational business case for privacy.  
   ii. Identify stakeholders.  
   iii. Leverage key functions.  
   iv. Create a process for interfacing within organization.  
   v. Align organizational culture and privacy/data protection objectives.  
b. Obtain funding/budget for privacy and the privacy team.  
c. Develop a data governance strategy for personal information (collection, authorized use, access, destruction).  
e. Plan inquiry/complaint handling procedures (customers, regulators, etc.).  
f. Ensure program flexibility in order to incorporate legislative/regulatory/market/business requirements. | **Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.  
**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes, and procedures to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. |
## D. Structure the privacy team

<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
</table>
| 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. | Governance Policies, Processes, and Procedures (GV.PO-P): The policies, processes, and procedures to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. |
### Communicate

<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E. Communicate</strong></td>
<td><strong>Awareness and Training (GV.AT-P):</strong> The organization’s workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.</td>
</tr>
<tr>
<td>a. Awareness.</td>
<td><strong>Communication Policies, Processes, and Procedures (CM.PO-P):</strong> Policies, processes, and procedures are maintained and used to increase transparency of the organization’s data processing practices (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) and associated privacy risks.</td>
</tr>
<tr>
<td>i. Create awareness of the organization’s privacy program internally and externally.</td>
<td><strong>Data Processing Awareness (CM.AW-P):</strong> Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization’s risk strategy to protect individuals’ privacy.</td>
</tr>
<tr>
<td>ii. Develop internal and external communication plans to ingrain organizational accountability.</td>
<td></td>
</tr>
<tr>
<td>iii. Identify, catalog and maintain documents requiring updates as privacy requirements change.</td>
<td></td>
</tr>
<tr>
<td>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</td>
<td>NIST Privacy Framework Core</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Domain II. Privacy Program Framework</strong></td>
<td><strong>Governance Policies, Processes, and Procedures (GV.PO-P):</strong> The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td><strong>A. Develop the Privacy Program Framework</strong></td>
<td><strong>Inventory and Mapping (ID.IM-P):</strong> Data processing by systems, products, or services is understood and informs the management of privacy risk.</td>
</tr>
<tr>
<td>a. Develop organizational privacy policies, standards and/or guidelines.</td>
<td><strong>Risk Assessment (ID.RA-P):</strong> The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, reputation, other risk management priorities (e.g. compliance, financial), reputation, workforce, and culture.</td>
</tr>
<tr>
<td>b. Define privacy program activities.</td>
<td><strong>Awareness and Training (GV.AT-P):</strong> The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.</td>
</tr>
<tr>
<td>i. Education and awareness.</td>
<td><strong>Monitoring and Review (GV.MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>ii. Monitoring and responding to the regulatory environment.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>iii. Internal policy compliance.</td>
<td></td>
</tr>
<tr>
<td>iv. Data inventories, data flows, and classification.</td>
<td></td>
</tr>
<tr>
<td>v. Risk assessment (Privacy Impact Assessments [PIAs]) (e.g., DPIAs etc.).</td>
<td></td>
</tr>
<tr>
<td>vi. Incident response and process, including jurisdictional regulations.</td>
<td></td>
</tr>
<tr>
<td>vii. Remediation.</td>
<td></td>
</tr>
<tr>
<td>viii. Program assurance, including audits.</td>
<td></td>
</tr>
</tbody>
</table>
### B. Implement the Privacy Program Framework

<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Communicate the framework to internal and external stakeholders.</td>
<td><strong>Communication Policies, Processes, and Procedures (CM.PO-P):</strong> Policies, processes, and procedures are maintained and used to increase transparency of the organization’s data processing practices (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) and associated privacy risks.</td>
</tr>
<tr>
<td>b. Ensure continuous alignment to applicable laws and regulations to support the development of an organizational privacy program framework.</td>
<td><strong>Data Processing Awareness (CM.AW-P):</strong> Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization’s risk strategy to protect individuals’ privacy.</td>
</tr>
<tr>
<td>i. Understand when national laws and regulations apply (e.g. GDPR).</td>
<td><strong>Governance Policies, Processes, and Procedures (GV.PO-P):</strong> The policies, processes, and procedures to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>ii. Understand when local laws and regulations apply (e.g. CCPA).</td>
<td></td>
</tr>
<tr>
<td>C. Develop Appropriate Metrics</td>
<td>Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization’s privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>a. Identify intended audience for metrics.</td>
<td></td>
</tr>
<tr>
<td>b. Define reporting resources.</td>
<td></td>
</tr>
<tr>
<td>c. Define privacy metrics for oversight and governance per audience.</td>
<td></td>
</tr>
<tr>
<td>i. Compliance metrics (examples, will vary by organization):</td>
<td></td>
</tr>
<tr>
<td>1. Collection (notice).</td>
<td></td>
</tr>
<tr>
<td>2. Response to data subject inquiries.</td>
<td></td>
</tr>
<tr>
<td>3. Use.</td>
<td></td>
</tr>
<tr>
<td>4. Retention.</td>
<td></td>
</tr>
<tr>
<td>5. Disclosure to third parties.</td>
<td></td>
</tr>
<tr>
<td>6. Incidents (breaches, complaints, inquiries).</td>
<td></td>
</tr>
<tr>
<td>7. Employees trained.</td>
<td></td>
</tr>
<tr>
<td>8. PIA metrics.</td>
<td></td>
</tr>
<tr>
<td>10. Percent of company functions represented by governance mechanisms.</td>
<td></td>
</tr>
<tr>
<td>ii. Trending.</td>
<td></td>
</tr>
<tr>
<td>iii. Privacy program return on investment (ROI).</td>
<td></td>
</tr>
<tr>
<td>iv. Business resiliency metrics.</td>
<td></td>
</tr>
<tr>
<td>v. Privacy program maturity level.</td>
<td></td>
</tr>
<tr>
<td>vi. Resource utilization.</td>
<td></td>
</tr>
<tr>
<td>d. Identify systems/application collection points.</td>
<td></td>
</tr>
</tbody>
</table>
### Domain 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).
- h. Program assurance, including audits.

### NIST Privacy Framework Core

**Inventory and Mapping (ID.IM-P):**
Data processing by systems, products, or services is understood and informs the management of privacy risk.

**Risk Assessment (ID.RA-P):** The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, reputation, other risk management priorities (e.g. compliance, financial), reputation, workforce, and culture.
<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
</table>
| 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. | Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem. |
| 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. | |
| 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, IoT, geo-tracking, imaging/copier hard drive security controls). | Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, reputation, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture. |
<p>| D. Physical assessments | |</p>
<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>C. Mergers, acquisitions and divestitures</strong></td>
<td><strong>Risk Assessment (ID.RA-P):</strong> The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, reputation, other risk management priorities (e.g. compliance, financial), reputation, workforce, and culture.</td>
</tr>
</tbody>
</table>
| a. Due diligence.  
b. Risk assessment. | |
| **E. Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIs)** | **Monitoring and Review (GV. MT-P):** The policies, processes, and procedures for ongoing review of the organization’s privacy posture are understood and inform the management of privacy risk. |
| 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. | |
### Domain IV. Privacy Operational Life Cycle: Protect

#### A. Information security practices

<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
</table>
| 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. | **Data Security (PR.DS-P):** Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy and maintain data confidentiality, integrity, and availability. **Identity Management, Authentication, and Access Control (PR.AC-P):** Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access. **Maintenance (PR.MA-P):** System maintenance and repairs are performed consistent with policies, processes, and procedures. **Protective Technology (PR.PT-P):** Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements. |
# B. Privacy by design

<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Integrate privacy throughout the system development life cycle (SDLC).</td>
<td><strong>Data Processing Policies, Processes, and Procedures (CT.PO-P):</strong> Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization’s risk strategy to protect individuals’ privacy.</td>
</tr>
<tr>
<td>b. Establish privacy gates as part of the system development framework.</td>
<td><strong>Data Processing Management (CT.DM-P):</strong> Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).</td>
</tr>
<tr>
<td><strong>Disassociated Processing (CT.DP-P):</strong> Data processing solutions increase disassociability consistent with related policies, processes, procedures, and agreements and the organization’s risk strategy to protect individuals’ privacy and enable implementation of privacy principles (e.g., data minimization).</td>
<td></td>
</tr>
<tr>
<td>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</td>
<td>NIST Privacy Framework Core</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>C. Integrate privacy requirements and representation into functional areas across the organization</strong></td>
<td>Data Processing Policies, Processes, and Procedures (CT.PO-P): Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization’s risk strategy to protect individuals’ privacy.</td>
</tr>
<tr>
<td>i. Information security. ii. IT operations and development. iii. Business continuity and disaster recovery planning. iv. Mergers, acquisitions and divestitures. v. Human resources. vi. Compliance and ethics. vii. Audit. viii. Marketing/business development. ix. Public relations. x. Procurement/sourcing. xi. Legal and contracts. xii. Security/emergency services. xiii. Finance. xiv. Others.</td>
<td>Data Processing Management (CT.DM-P): Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).</td>
</tr>
<tr>
<td><strong>D. Other Organizational Measures</strong></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

International Association of Privacy Professionals • iapp.org
<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domain V. Privacy Operational Life Cycle: Sustain</strong></td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td><strong>A. Monitor</strong></td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>a. Environment (e.g. systems, applications) monitoring.</td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>b. Monitor compliance with established privacy policies.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>c. Monitor regulatory and legislative changes.</td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>d. Compliance monitoring (e.g. collections, use and retention).</td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>i. Internal audit.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>ii. Self-regulation.</td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>iii. Retention strategy.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>iv. Exit strategy.</td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td><strong>B. Audit</strong></td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>a. Align privacy operations to an internal and external compliance audit program.</td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>i. Knowledge of audit processes.</td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>ii. Align to industry standards.</td>
<td><strong>Monitoring and Review (GV. MT-P):</strong> The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.</td>
</tr>
<tr>
<td>b. Audit compliance with privacy policies and standards.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>c. Audit data integrity and quality and communicate audit findings with stakeholders.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>d. Audit information access, modification and disclosure accounting.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>e. Targeted employee, management and contractor training.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>i. Privacy policies.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>ii. Operational privacy practices (e.g., standard operating instructions), such as:</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>1. Data creation/usage/retention/disposal.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>2. Access control.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>3. Reporting incidents.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>4. Key contacts.</td>
<td><strong>Data Protection Policies, Processes, and Procedures (PR.PO-P):</strong> Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.</td>
</tr>
<tr>
<td>Domain VI. Privacy Operational Life Cycle: Respond</td>
<td>NIST Privacy Framework Core</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>A. Data-subject information requests and privacy rights</td>
<td><strong>Data Processing Policies, Processes, and Procedures (CT.PO-P):</strong> Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy.</td>
</tr>
<tr>
<td></td>
<td><strong>Data Processing Management (CT.DM-P):</strong> Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).</td>
</tr>
<tr>
<td></td>
<td><strong>Data Processing Awareness (CM.AW-P):</strong> Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.</td>
</tr>
<tr>
<td>a. Access.</td>
<td></td>
</tr>
<tr>
<td>b. Redress.</td>
<td></td>
</tr>
<tr>
<td>c. Correction.</td>
<td></td>
</tr>
<tr>
<td>d. Managing data integrity.</td>
<td></td>
</tr>
<tr>
<td>B. Privacy incident response</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td></td>
</tr>
<tr>
<td>a. Legal compliance.</td>
<td></td>
</tr>
<tr>
<td>i. Preventing harm.</td>
<td></td>
</tr>
<tr>
<td>ii. Collection limitations.</td>
<td></td>
</tr>
<tr>
<td>iii. Accountability.</td>
<td></td>
</tr>
<tr>
<td>iv. Monitoring and enforcement.</td>
<td></td>
</tr>
<tr>
<td>b. Incident response planning.</td>
<td></td>
</tr>
<tr>
<td>i. Understand key roles and responsibilities.</td>
<td></td>
</tr>
<tr>
<td>1. Identify key business stakeholders.</td>
<td></td>
</tr>
<tr>
<td>1. Information security.</td>
<td></td>
</tr>
<tr>
<td>2. Legal.</td>
<td></td>
</tr>
<tr>
<td>3. Audit.</td>
<td></td>
</tr>
<tr>
<td>4. Human resources.</td>
<td></td>
</tr>
<tr>
<td>5. Marketing.</td>
<td></td>
</tr>
<tr>
<td>7. Communications and public relations.</td>
<td></td>
</tr>
<tr>
<td>8. Other.</td>
<td></td>
</tr>
<tr>
<td>2. Establish incident oversight teams.</td>
<td></td>
</tr>
<tr>
<td>3. Develop a privacy incident response plan.</td>
<td></td>
</tr>
<tr>
<td>4. Identify elements of the privacy incident response plan.</td>
<td></td>
</tr>
<tr>
<td>5. Integrate privacy incident response into business continuity planning.</td>
<td></td>
</tr>
<tr>
<td>c. Incident detection.</td>
<td></td>
</tr>
<tr>
<td>1. Define what constitutes a privacy incident.</td>
<td></td>
</tr>
<tr>
<td>2. Identify reporting process.</td>
<td></td>
</tr>
<tr>
<td>3. Coordinate detection capabilities.</td>
<td></td>
</tr>
<tr>
<td>a. Organization IT.</td>
<td></td>
</tr>
<tr>
<td>b. Physical security.</td>
<td></td>
</tr>
<tr>
<td>c. Human resources.</td>
<td></td>
</tr>
<tr>
<td>d. Investigation teams.</td>
<td></td>
</tr>
<tr>
<td>e. Vendors.</td>
<td></td>
</tr>
</tbody>
</table>

<p>| Governance Policies, Processes, and Procedures (GV.PO-P): The policies, processes, and procedures to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. |
| Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization’s privacy posture are understood and inform the management of privacy risk. |
| Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization’s risk strategy to protect individuals’ privacy. |
| Data Protection Policies, Processes, and Procedures (PR.PO-P): Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data. |</p>
<table>
<thead>
<tr>
<th>IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge v2.04</th>
<th>NIST Privacy Framework Core</th>
</tr>
</thead>
</table>
| d. Incident handling.  
  1. Understand key roles and responsibilities.  
  2. Develop a communications plan to notify executive management. | e. 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.  
  7. Review and apply lessons learned. |
| f. Identify incident reduction techniques. | g. Incident metrics—quantify the cost of a privacy incident. |