iapp

The Skill Set Needed to Implement a Privacy Risk Management Framework

IAPP Research Director Caitlin Fennessy, CIPP/US

The Skill Set Needed to Implement a Privacy Risk Management Framework

NIST Privacy Framework Version 1.0 alignment with IAPP CIPM certification

IAPP Research Director Caitlin Fennessy, CIPP/US

In January 2020, the U.S. National Institute of Standards and Technology released the NIST Privacy Framework Version 1.0. To offer insight into the professional skill set 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 skill set 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 NIST Privacy Framework is a tool to help enterprises assess and mitigate privacy risk, implement privacy engineering, and design products and services to help protect individuals' privacy. The Privacy Framework follows the structure of and is designed to be implemented in tandem with NIST's widely adopted Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). This alignment offers organizations the opportunity to better integrate their privacy and security programs.

The release of version 1.0 of NIST's Privacy Framework followed a one-and-a-half-year multi-stakeholder development process that brought together privacy professionals from across sectors and disciplines. By collecting feedback from security professionals, lawyers, product designers, software developers, business managers and others, NIST created a common privacy lexicon. The Privacy Framework is designed to support communication across an organization and a collaborative approach to address privacy risk.

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, skill sets more closely aligned with IAPP's regionally based CIPP bodies of knowledge. Similarly, privacy engineers assessing options for deidentification 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 attached 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. This mapping serves the dual purpose of informing privacy professionals seeking to understand the skill set to needed implement the NIST Privacy Framework and IAPP's ongoing work to ensure its certifications are continually refined to meet the needs of the privacy profession across sectors and disciplines.

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge
Identify-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**Domain II. A. a. iv.** Data, systems and process assessment • Map data inventories, flows and classification • Create "record of authority" of systems processing personal information within the organization • Map and document data flow in systems and applications • Analyze and classify types and uses of data
	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.	**Domain I. A. c. iii. 1.** Business alignment • Finalize the operational business case for privacy • Identify stakeholders • Leverage key functions • Create a process for interfacing within organization • Align organizational culture and privacy/data protection objectives • Obtain funding/budget for privacy and the privacy team

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge

	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.	**Domain II. A. a. v, c, d, & e**
		Document current baseline of your privacy program
		• Risk assessment (PIAs, etc.)
		Physical assessments
		• Identify operational risk
		  • Data centers and offices
		  • Physical access controls
		  • Document destruction
		  • Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.)
		  • Device forensics
		  • Device security (e.g., mobile, IoT, geo-tracking, imaging/copier hard drive security controls)
		Mergers, acquisitions and divestitures
		• Due diligence
		• Risk assessment
		Conduct analysis and assessments, as needed or appropriate
		• Privacy Threshold Analysis (PTAs) on systems, applications and processes
		• Privacy Impact Assessments (PIAs)
		  • Define a process for conducting Privacy Impact Assessments
		  • Understand the life cycle of a PIA
		  • Incorporate PIA into system, process, product life cycles

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge

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

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge

Govern-P (GV-P): 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.	**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.	**Domain I. Privacy Program Governance**
		Organization Level
		• Create a company vision
		  • Acquire knowledge on privacy approaches
		  • Evaluate the intended objective
		  • Gain executive sponsor approval for this vision
		• Establish Data Governance model
		  • Centralized
		  • Distributed
		  • Hybrid
		• 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
		  Business alignment
		  • Finalize the operational business case for privacy
		  • Identify stakeholders
		  • Leverage key functions
		  • Create a process for interfacing within organization
		  • Align organizational culture and privacy/data protection objectives
		  • Obtain funding/budget for privacy and the privacy team
		• Structure the privacy team
		  • Establish the organizational model, responsibilities and reporting structure appropriate to the size of the organization
		  Large organizations
		  • Chief privacy officer
		  • Privacy manager
		  • Privacy analysts
		  • Business line privacy leaders
		  • "First responders"

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge
		Small organizations/sole data protection officer (DPO) including when not only job • Designate a point of contact for privacy issues • Establish/endorse the measurement of professional competency Develop the Privacy Program Framework • Develop organizational privacy policies, standards and/or guidelines • Define privacy program activities • Education and awareness • Monitoring and responding to the regulatory environment • Internal policy compliance • Data inventories, data flows, and classification • Risk assessment (Privacy Impact Assessments [PIAs]) (e,g., DPIAs etc.) • Incident response and process, including jurisdictional regulations • Remediation • Program assurance, including audits 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 • Understand when national laws and regulations apply (e.g. GDPR, CCPA) • Understand when local laws and regulations apply • Understand penalties for noncompliance with laws and regulations • Understand the scope and authority of oversight agencies (e.g., Data Protection Authorities, Privacy Commissioners, Federal Trade Commission, etc.)

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge
		• Understand privacy implications of doing business with or basing operations in countries with inadequate, or without, privacy laws • Maintain the ability to manage a global privacy function • Maintain the ability to track multiple jurisdictions for changes in privacy law • Understand international data sharing arrangement agreements
	Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**Domain I. B. b. v.** Risk assessment (Privacy Impact Assessments [PIAs]) (e,g., DPIAs etc.)

	Awareness and Training (GV.AT-P): 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.	**Domain II. A. a. i.**
		Education and awareness
		
		Domain II. C. d. ii.
		Targeted employee, management and contractor training
		• Privacy policies
		• Operational privacy practices (e.g., standard operating instructions), such as
		  • Data creation/usage/ retention/disposal
		  • Access control
		  • Reporting incidents
		  • Key contacts

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge

	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.	**Domain I. A. c. iii. 3.**
		Plan inquiry/complaint handling procedures (customers, regulators, etc.)
		
		Domain I. B. b. i-iii, vi-viii.
		Define privacy program activities
		• Education and awareness
		• Monitoring and responding to the regulatory environment
		• Internal policy compliance
		• Incident response and process, including jurisdictional regulations
		• Remediation
		• Program assurance, including audits
		
		Domain I. D.
		Metrics
		• Identify intended audience for metrics
		• Define reporting resources
		• Define privacy metrics for oversight and governance per audience
		  • Compliance metrics (examples, will vary by organization): Collection (notice); Responses to data subject inquiries; Use; Retention; Disclosure to third parties; Incidents (breaches, complaints, inquiries); Employees trained; PIA metrics; Privacy risk indicators; and Percent of company functions represented by governance mechanisms
		  • Trending
		  • Privacy program return on investment (ROI)
		  • Business resiliency metrics
		  • Privacy program maturity level
		  • Resource utilization
		• Identify systems/application collection points

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge

		Domain II. A. a. ii, iii, viii, & ix
		• Monitoring and responding to the regulatory environment iii. Internal policy compliance
		• Determine desired state and perform gap analysis against an accepted standard or law (including GDPR) ix. Program assurance, including audits
		
		Domain II. C. e.
		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)
		  • Internal audit
		  • Self-regulation
		  • Retention strategy
		  • Exit strategy
		
		Domain II. D. b. ii. 2-4, iii, v.7, & vii.
		• Develop a privacy incident response plan
		• Identify elements of the privacy incident response plan
		• Integrate privacy incident response into business continuity planning
		• Incident detection
		  • Define what constitutes a privacy incident
		  • Identify reporting process
		  • Coordinate detection capabilities
		  • Organization IT
		  • Physical security
		  • Human resources
		  • Investigation teams
		  • Vendors
		• Follow incident response process to ensure meeting jurisdictional, global and business requirements
		  • Review and apply lessons learned
		• Incident metrics—quantify the cost of a privacy incident

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge
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 Management Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) consistent with the organization's risk strategy to protect individuals' privacy.	**Domain I. A. c. iii. 2.** Develop a data governance strategy for personal information (collection, authorized use, access, destruction) **Domain II. B. c.** Privacy by Design • Integrate privacy throughout the system development life cycle (SDLC) • Establish privacy gates as part of the system development framework **Domain II. C. a. ii-iv. & b.** Measure • 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 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

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge

	Data 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 II. A. e.**
		Conduct analysis and assessments, as needed or appropriate
		• Privacy Threshold Analysis (PTAs) on systems, applications and processes
		• Privacy Impact Assessments (PIAs)
		  • Define a process for conducting Privacy Impact Assessments
		  • Understand the life cycle of a PIA
		  • Incorporate PIA into system, process, product life cycles
		
		Domain II. B. a. & c.
		Data life cycle and governance (creation to deletion)
		Privacy by Design
		• Integrate privacy throughout the system development life cycle (SDLC)
		• Establish privacy gates as part of the system development framework

	Disassociated Processing (CT. DP-P): 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).	**Domain I. A. c. 2.** Develop a data governance strategy for personal information (collection, authorized use, access, destruction) **Domain II. B. c.** Privacy by Design • Integrate privacy throughout the system development life cycle (SDLC) **Domain II. D. b. i. 2.** Collection limitations

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge
Communicate-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** 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.	**Domain I. C. a.** Communicate the framework to internal and external stakeholders
	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.	**Domain II. C. d. i.** Awareness • Create awareness of the organization's privacy program internally and externally • Ensure policy flexibility in order to incorporate legislative/regulatory/market requirements • Develop internal and external communication plans to ingrain organizational accountability • Identify, catalog and maintain documents requiring updates as privacy requirements change **Domain II. D.** Information requests • Access • Redress • Correction • Managing data integrity

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge

		Incident response planning
		• Understand key roles and responsibilities
		  • Identify key business stakeholders
		  • Information security
		  • Legal
		  • Audit
		  • Human resources
		  • Marketing
		  • Business development
		  • Communications and public relations
		  • Other
		  • Establish incident oversight teams
		Incident detection
		• Define what constitutes a privacy incident
		• Identify reporting process
		• Coordinate detection capabilities
		  • Organization IT
		  • Physical security
		  • Human resources
		  • Investigation teams
		  • Vendors
		Incident handling
		• Understand key roles and responsibilities
		• Develop a communications plan to notify executive management
		Follow incident response process to ensure meeting jurisdictional, global and business requirements
		• Engage privacy team
		  • Review the facts
		  • Conduct analysis
		  • Determine actions (contain, communicate, etc.)
		  • Execute
		  • Monitor

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge

Protect-P (PR-P): Develop and implement appropriate data processing safeguards.	**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.	**Domain II. A. a. vi. & D. b. i. & ii.2-4**
		Incident response
		Privacy incidents
		• Legal compliance
		  • Preventing harm
		  • Collection limitations
		  • Accountability
		  • Monitoring and enforcement
		• Develop a privacy incident response plan
		• Identify elements of the privacy incident response plan
		• Integrate privacy incident response into business continuity planning
		
		Domain II. C. e. ii. & iv.
		Monitor
		• Monitor compliance with established privacy policies
		• Compliance monitoring (e.g. collection, use and retention)
		  • Internal audit
		  • Self-regulation
		  • Retention strategy
		  • Exit strategy

	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.	**Domain II. B. b. i.** Access controls for physical and virtual systems • Access control on need to know • Account management (e.g., provision process) • Privilege management

NIST Privacy Framework Integrated Core		IAPP Certified Information Privacy Manager (CIPM) Body of Knowledge
	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.	**Domain II. B. b. ii.** Technical security controls
	Maintenance (PR. MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**Domain II. B. b. iii.** Implement appropriate administrative safeguards
	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.	**Domain II. A. c. i.** Identify operational risk • Data centers and offices • Physical access controls • Document destruction • Media sanitization and disposal (e.g., hard drives, USB/thumb drives, etc.) • Device forensics • Device security (e.g., mobile, IoT, geo-tracking, imaging/copier hard drive security controls)