Published on *The National Law Review* https://natlawreview.com

Prioritizing Privacy Programs Based on the NIST Privacy Framework

Article By:

Kenric Tom

Our team recently published a series of articles on how to implement the five core functions of the National Institute of Standards and Technology (NIST) Privacy Framework. We wrote an initial article on how organizations can use the NIST Privacy Framework to assess privacy risk and build a privacy program. We then published five subsequent articles on each function within the NIST Privacy Framework: Identify, Govern, Control, Communicate, and Protect.

In this article, we provide an overview of how the NIST Privacy Framework can support and prioritize your organization's specific privacy program, including how different business functions or groups can be incorporated into the program.

How can the NIST Privacy Framework support organizational privacy programs?

The NIST Privacy Framework consists of 18 categories and 100 subcategories within 5 core functions. The functions and categories are listed below in Table 1.

Table 1	
Function	**Category**
Identify	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.
	Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.
	Risk Assessment (ID.RA-P): The organization understands the privacy risks to individua how such privacy risks may create follow-on impacts on organizational operations, includi mission, functions, other risk management priorities (e.g., compliance, financial), reputatio workforce, and culture.
	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities constraints, risk tolerance, and assumptions are established and used to support risk deci associated with managing privacy risk and third parties within the data processing ecosyst organization has established and implemented the processes to identify, assess, and mar privacy risks within the data processing ecosystem.
Govern	**Governance Policies, Processes, and Procedures (GV.PO-P):** The policies, processes

	procedures to manage and monitor the organization's regulatory, legal, risk, environmenta operational requirements are understood and inform the management of privacy risk.
	Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tol and assumptions are established and used to support operational risk decisions.
	Awareness and Training (GV.AT-P): The organization's workforce and third parties enga data processing are provided privacy awareness education and are trained to perform the related duties and responsibilities consistent with related policies, processes, procedures, agreements, and organizational privacy values.
	Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing the organization's privacy posture are understood and inform the management of privacy r
Control	**Data Processing Policies, Processes, and Procedures (CT.PO-P):** Policies, processes procedures are maintained and used to manage data processing (e.g., purpose, scope, ro responsibilities in the data processing ecosystem, and management commitment) consiste the organization's risk strategy to protect individuals' privacy.
	Data Processing Management (CT.DM-P): Data are managed consistent with the organ risk strategy to protect individuals' privacy, increase manageability, and enable the implem of privacy principles (e.g., individual participation, data quality, data minimization).
	Disassociated Processing (CT.DP-P): Data processing solutions increase disassociabili consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).
Communicate	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes 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 processir ecosystem, and management commitment) and associated privacy risks.
	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable kn about data processing practices and associated privacy risks, and effective mechanisms a and maintained to increase predictability consistent with the organization's risk strategy to individuals' privacy.
Protect	**Data Protection Policies, Processes, and Procedures (PR.PO-P):** Security and privacy (e.g., purpose, scope, roles, and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to mana protection of data.
	Identity Management, Authentication, and Access Control (PR.AC-P): Access to data devices is limited to authorized individuals, processes, and devices, and is managed cons the assessed risk of unauthorized access.
	Data Security (PR.DS-P): Data are managed consistent with the organization's risk strate protect individuals' privacy and maintain data confidentiality, integrity, and availability.
	Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with processes, and procedures.
	Protective Technology (PR.PT-P): Technical security solutions are managed to ensure t security and resilience of systems/products/services and associated data, consistent with policies, processes, procedures, and agreements.

The five functions in the NIST Privacy Framework support different privacy activities for a mature privacy program. Although the functions are interrelated, organizations and specific business groups within an organization may rely on certain functions more heavily than others. The prioritization of functions depends on the maturity of your program and level of interdependency between operational business lines. In Table 2 below, we present key privacy activities and the common business groups

involved for each NIST Privacy Framework function in Table 2.

Table 2		
Function	**Privacy Management Activity**	**Business Gro**
Identify	Deliver self-assessment/privacy risk assessment report(s)	IT, Legal, Com
	Create a data inventory/map of personal information or personal data	
Govern	Establish privacy governance/committee	HR, Legal, Cor
	Implement vendor risk management program	Business/Mark
	Regularly monitor, review and update privacy policies and procedures	Information Se
Control	Create privacy notice(s)	HR, Legal, Cor
	Develop privacy policies and procedures (e.g., Internal Privacy Policy, Consent Management, Data Retention, Privacy by Design)	Business/Mark Information Se
	Create Data Subject/Consumer Rights Request policy and procedure	
	Implement Data Protection Impact Assessments/Privacy Risk Assessments	
Communicate	Deliver privacy training and awareness	HR, Legal, Cor
	Deliver training to employees handling personal information or personal data	
Protect	Create and manage Written Information Security Policy (WISP)	IT, Information
	Implement technical and organizational security measures to protect personal information or personal data	
	Develop security policies and procedures (e.g., Acceptable Use, Access Control, Incident Response, Business Continuity, Disaster Recovery)	

How do we prioritize privacy programs based on the NIST Privacy Framework?

While each activity outlined above is critical for building a mature privacy program, we understand that time and budget are limiting factors, especially when involving other business areas and ensuring company-wide buy in. Organizations can prioritize these activities and create a stepwise approach to address each function in the Framework according to maturity, size, industry, and overall regulatory exposure.

If your organization has little to no privacy controls in place, the best place to start may be with a privacy risk or gap assessment report. Identifying your organization’s current privacy activities, risk posture, and a list of prioritized subsequent activities is a key first step. Creating an inventory of personal information is also critical for any organization. A data inventory maps where and how personal data is collected, processed, and stored within the organization, and forms the building block for later privacy program activities. If you do not know where all your personal data is held or where such data is sent, it is difficult to properly protect such information.

Once your organization is aware of its key risk areas, you can next prioritize activities based on business needs and risks. For example, if your organization operates in a Direct to Consumer capacity, or you have an eCommerce business, you may receive a high number of Data Subject Rights or Consumer Rights requests. In this case, prioritizing a Data Subject Rights policy and procedure and building a workflow process is necessary to address this risk area. Similarly, if you have a large number of service providers who access sensitive personal information, taking steps to modernize your third party vendor risk management program may also be a priority activity.

Industry also drives privacy priorities. For software companies, having strong technical security measures in place and implementing Privacy by Design is critical during the software development lifecycle (SDLC). Companies in the biotech or pharma space that conduct clinical trials with participants overseas should account for appropriate transfer mechanisms. This includes conducting proper data protection impact assessments and transfer impact assessments. If your organization heavily relies on marketing using third-party cookies or tracking technologies, implementing appropriate consent management and cookie management policies, notices, and banners should be prioritized.

Lastly, organizations should consider regulatory exposure based on jurisdictions and corresponding privacy laws. While everything outlined in this article is relevant to the current privacy landscape, organizations should also plan for the future as the privacy landscape continues to grow and evolve.

National Law Review, Volume XIII, Number 214