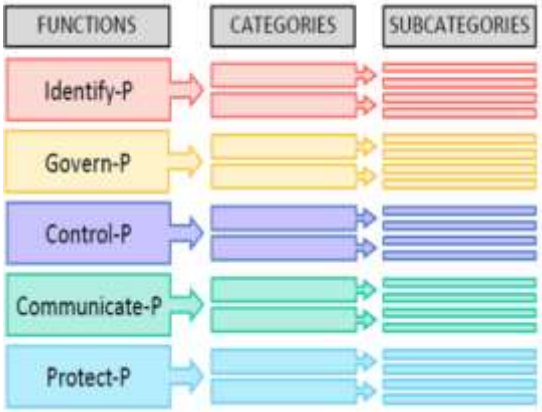
NIST PRIVACY FRAMEWORK GLOSSARY

Terminology is important. You will notice that I use terms in a very deliberate and formal fashion. Using terms in this manner aids in communication and thinking about privacy and the NIST Privacy Framework. The full glossary is available in the NIST Privacy Framework v1.0. **NS** in this glossary represents non-standardized definitions that are not in the NIST Privacy Framework glossary.

Organizational Terms

The following terms describe the organizational aspect of the NIST Privacy Framework

CORE - A set of privacy protection activities and outcomes. The Framework Core comprises three elements: **Functions**, **Categories**, and **Subcategories**.



Function - A component of the Core that provides the highest level of structure for organizing basic privacy activities into Categories and Subcategories.

Category - The subdivision of a Function into groups of privacy outcomes closely tied to programmatic needs and particular activities.

Subcategory - The further divisions of a Category into specific outcomes of technical and/or management activities.

NIST Privacy Framework Functions

Identify-P *- Develop the organizational understanding to manage privacy risk for individuals arising from data processing.*

Govern-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.*

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

Communicate-P *- 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.*

Protect-P *- Develop and implement appropriate data processing safeguards.*

PROFILE - A selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk.

Current Profile (NS) – the selection of Functions, Categories, and Subcategories outcomes the organization is currently achieving.

Target Profile (NS) – the selection of Functions, Categories, and Subcategories outcomes the organization needs to achieve the desired privacy risk management goals.

IMPLEMENTATION TIERS - Provides a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk. Tiers include:

Partial (NS) – The organization has a limited understanding of privacy risk and a limited understanding of how the objectives of the privacy framework can assist in reducing risk.

Risk Informed (NS) - The organization reviews outside sources to identify potential risks. It has some understanding of how its capabilities reduce risks.

Repetitive (NS) - The organization has an assessment process and can assess activities for risk reduction.

Adaptive (NS) - The organization continuously measures privacy risks and dynamically adjusts operations and objectives to address changes in risk.

Key Concepts

Critical to understanding the NIST Privacy Framework is the need to understand how Data Actions lead to Privacy Risk. The following terms are relevant to that understanding.

Data Terms

Data - A representation of information, including digital and non-digital formats.

Data Action (Adapted from NIST IR 8062 [5]) - A system/product/service data life cycle operation, including, but not limited to, collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal.

Data Element - The smallest named item of data that conveys meaningful information.

Data Processing (Adapted from NIST IR 8062 [5]) - The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal).

Data Processing Ecosystem - The complex and interconnected relationships among entities involved in creating or deploying systems, products, or services or any components that process data.

Problematic Data Action (Adapted from NIST IR 8062 [5]) - A data action that could cause an adverse effect for individuals.

Privacy Event - The occurrence or potential occurrence of problematic data actions.

Risk Terms

Privacy Risk - The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.

Privacy Risk Assessment - A privacy risk management sub-process for identifying and evaluating specific privacy risks.

Privacy Risk Management - A cross-organizational set of processes for identifying, assessing, and responding to privacy risks.

Risk Management - The process of identifying, assessing, and responding to risk.

Risk Tolerance (NIST SP 800-39 [6]) - The level of risk or degree of uncertainty that is acceptable to organizations.

Privacy Outcome (NS) - A result of the organization's privacy program activities.

Privacy Requirement - A specification for system/product/service functionality to meet stakeholders' desired privacy outcomes.

Privacy Control (Adapted from NIST SP 800-37 [7]) - The administrative, technical, and physical safeguards employed within an organization to satisfy privacy requirements.