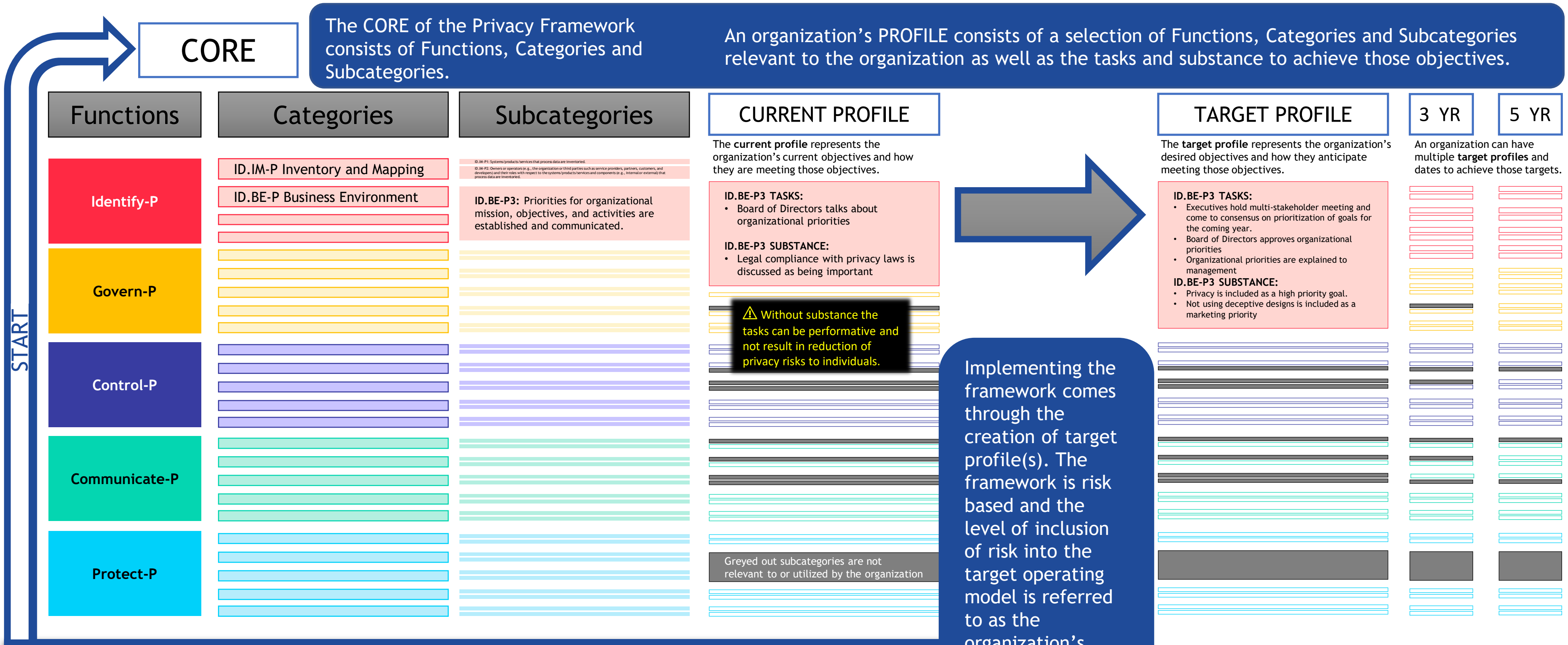


START

CORE

The CORE of the Privacy Framework consists of Functions, Categories and Subcategories.

An organization's PROFILE consists of a selection of Functions, Categories and Subcategories relevant to the organization as well as the tasks and substance to achieve those objectives.

Functions	Categories	Subcategories
Identify-P	ID.IM-P Inventory and Mapping	ID.IM-P1: Systems/products/services that process data are inventoried. ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.
	ID.BE-P Business Environment	**ID.BE-P3:** Priorities for organizational mission, objectives, and activities are established and communicated.
Govern-P		
Control-P		
Communicate-P		
Protect-P		

CURRENT PROFILE

The **current profile** represents the organization's current objectives and how they are meeting those objectives.

ID.BE-P3 TASKS:
- Board of Directors talks about organizational priorities

ID.BE-P3 SUBSTANCE:
- Legal compliance with privacy laws is discussed as being important

⚠ Without substance the tasks can be performative and not result in reduction of privacy risks to individuals.

Greyed out subcategories are not relevant to or utilized by the organization

TARGET PROFILE

The **target profile** represents the organization's desired objectives and how they anticipate meeting those objectives.

ID.BE-P3 TASKS:
- Executives hold multi-stakeholder meeting and come to consensus on prioritization of goals for the coming year.
- Board of Directors approves organizational priorities
- Organizational priorities are explained to management

ID.BE-P3 SUBSTANCE:
- Privacy is included as a high priority goal.
- Not using deceptive designs is included as a marketing priority

3 YR

5 YR

An organization can have multiple **target profiles** and dates to achieve those targets.

Implementing the framework comes through the creation of target profile(s). The framework is risk based and the level of inclusion of risk into the target operating model is referred to as the organization's **Implementation Tier.**

IMPLEMENTING THE NIST PRIVACY FRAMEWORK

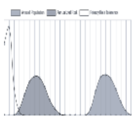
IMPLEMENTATION TIERS

Partial

Determination of the target profile is based on a limited understanding of privacy risk and a limited understanding of how the objectives of the privacy framework can assist in reducing risk.

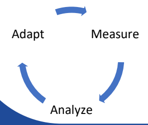
Risk Informed

The organization reviews legal requirements, industry standards, news reports and consults with lawyers and consultants to identify potential risks. It has some understanding of how its capabilities reduce that risk.



Repeatable

The organization has a privacy risk model and assessment process. Proposed capabilities are assessed for risk reduction and the target profile is developed based on measurable risk reducing capabilities.



Adaptive

The organization continuously measures privacy risks. Objectives, tasks and the substantive contents of those tasks are dynamically adjusted to address changes in risk.

Maturity Level: DEFINED	CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.	TIER
	Written Policy: The organization must publish a privacy notice on it's website.	Partial
	Written Policy: The organization must publish a privacy notice that informs consumers of the risk of spam (a known risk for this organization).	Risk Informed
	Written Policy: The organization must publish a privacy notice on its website. The organization must also survey consumers to see if they are taking precautions against being spammed. If not, it must adjust its policy on where and how the notice is published to reduce risky behavior.	Repeatable

⚠ Tiers are not maturity levels

Tiers are often mistaken for maturity levels under a privacy program maturity model. Tiers are about the sophistication of the organization's inclusion of risk in their target operations. Maturity level is about maturity of the organization's operation. For instance, in the above table all the tasks would indicate an organizational maturity of **DEFINED** (e.g. policies are written) but with differing levels of risk inclusion.

The NIST Privacy Framework identifies four elements (shown below) which contribute to determination of the organization's **Implementation Tier.**

The formality of its **Privacy Risk Management Process.**	The level of privacy knowledge and skills of its **Workforce.**
The sophistication of understanding it has about its and others roles in the **Data Processing Ecosystem.**	The amount a **Privacy Risk Management Program** is integrated across the organization.

NIST Privacy Framework training available
https://privacybydesign.training/nist

Provided by Enterprivacy Consulting Group