NIST PRIVACY FRAMEWORK

COMMUNITY DAY SEPT 21ST, 2022

SPEAKERS

R. Jason Cronk

CIPP/US, CIPM, CIPT, FIP

Privacy Engineer , Enterprivacy Consulting Group

Chair, Institute of Operational Privacy Design

Privacy Training: https://privacybydesign.training

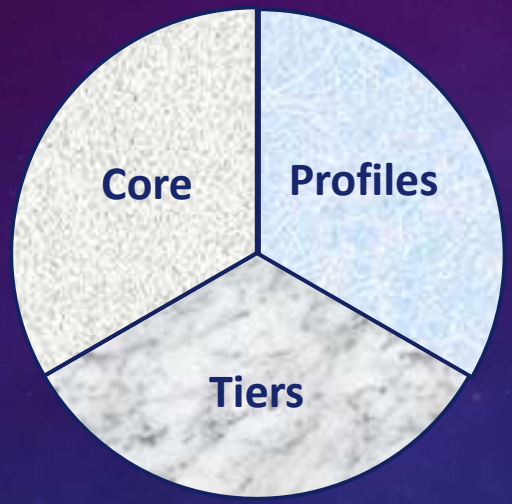
TODAY'S TALK

I. NIST Privacy Framework
   i. Cybersecurity Framework to Privacy Framework
   ii. Core
   iii. Profiles
   iv. Tiers
   v. Key Features
II. Questions and Answers

EVOLUTION

NIST introduces Cybersecurity Framework V1.0

Feb 2014



V1.1 Apr 2018

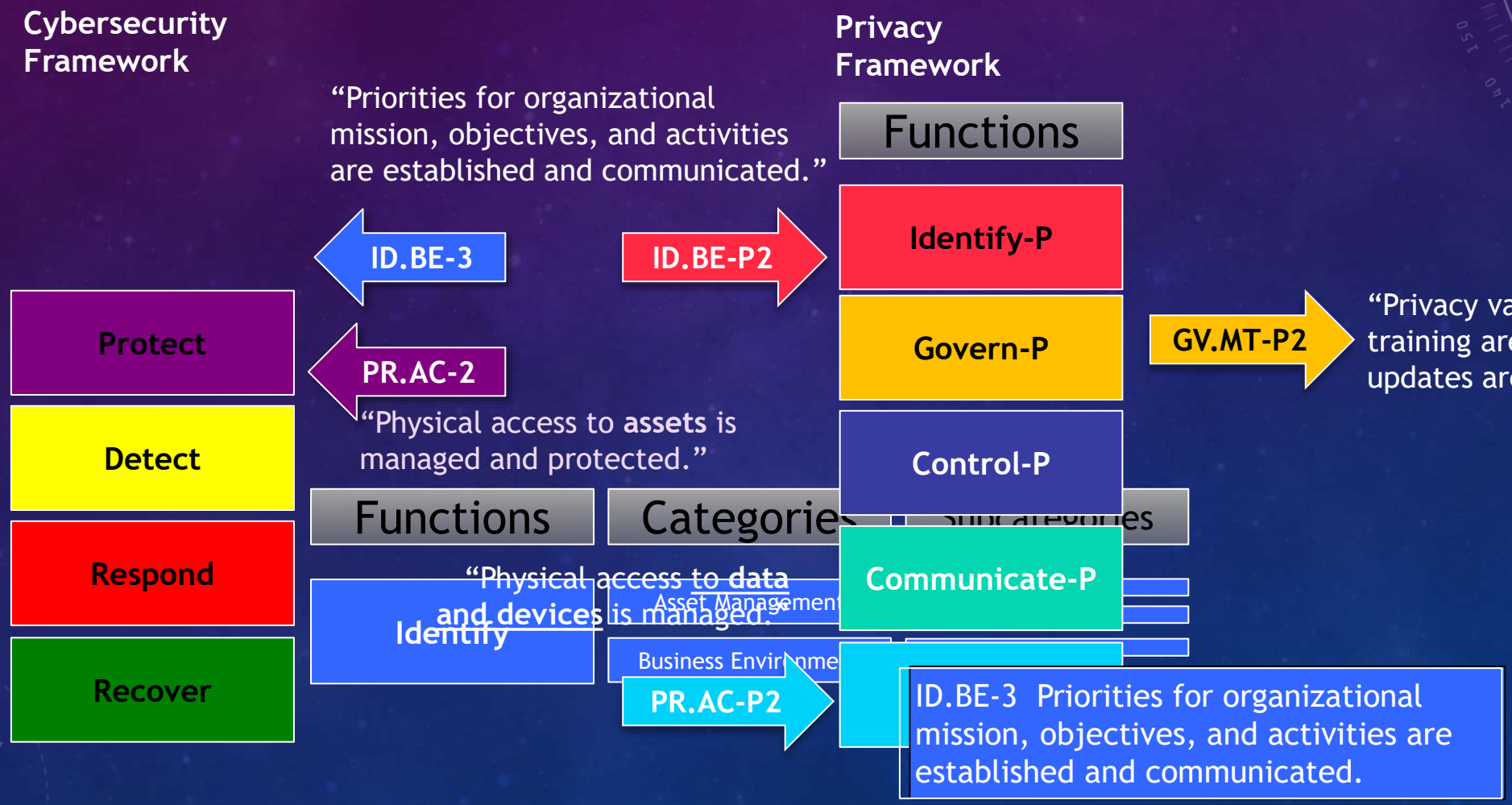
NIST introduces Privacy Framework V1.0

Jan 2020

CORE

Functions	Categories	Subcategories
Identify	Asset Management	
	Business Environment	ID.BE-3 Priorities for organizational mission, objectives, and activities are established and communicated.

CYBERSECURITY VS PRIVACY

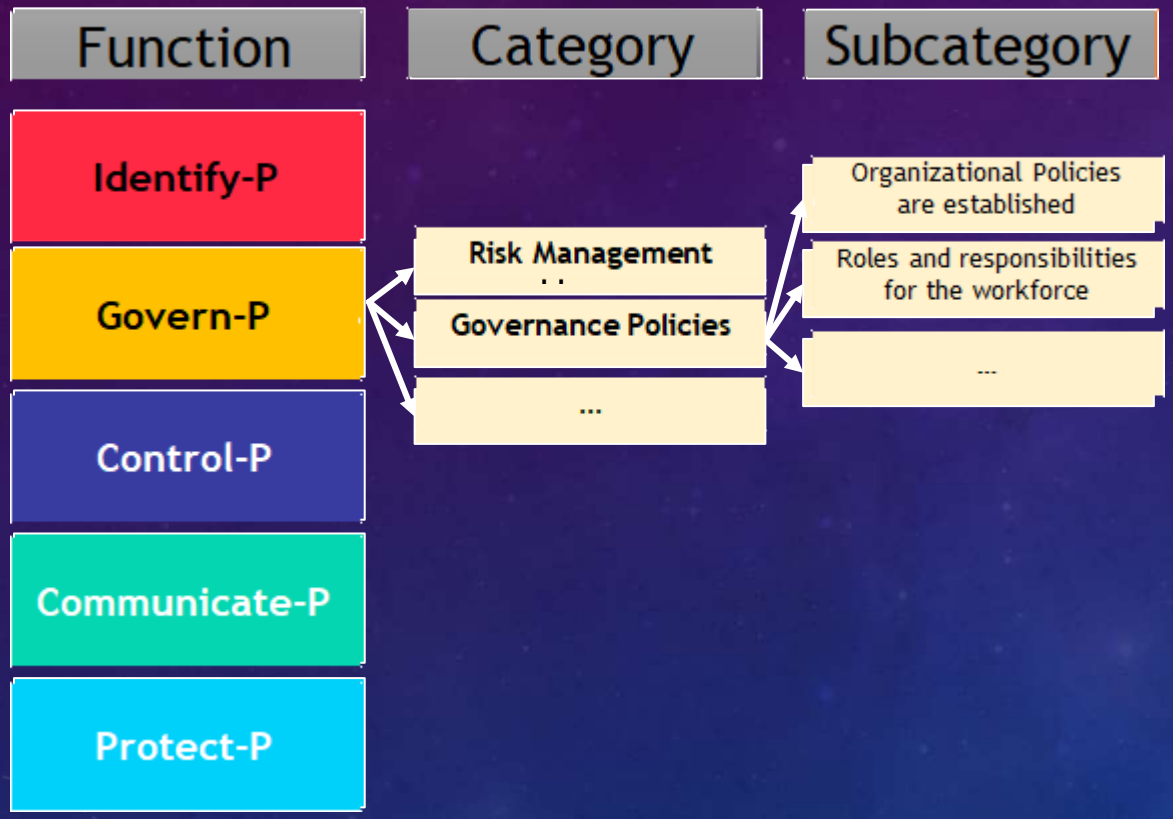


CROSSWALK

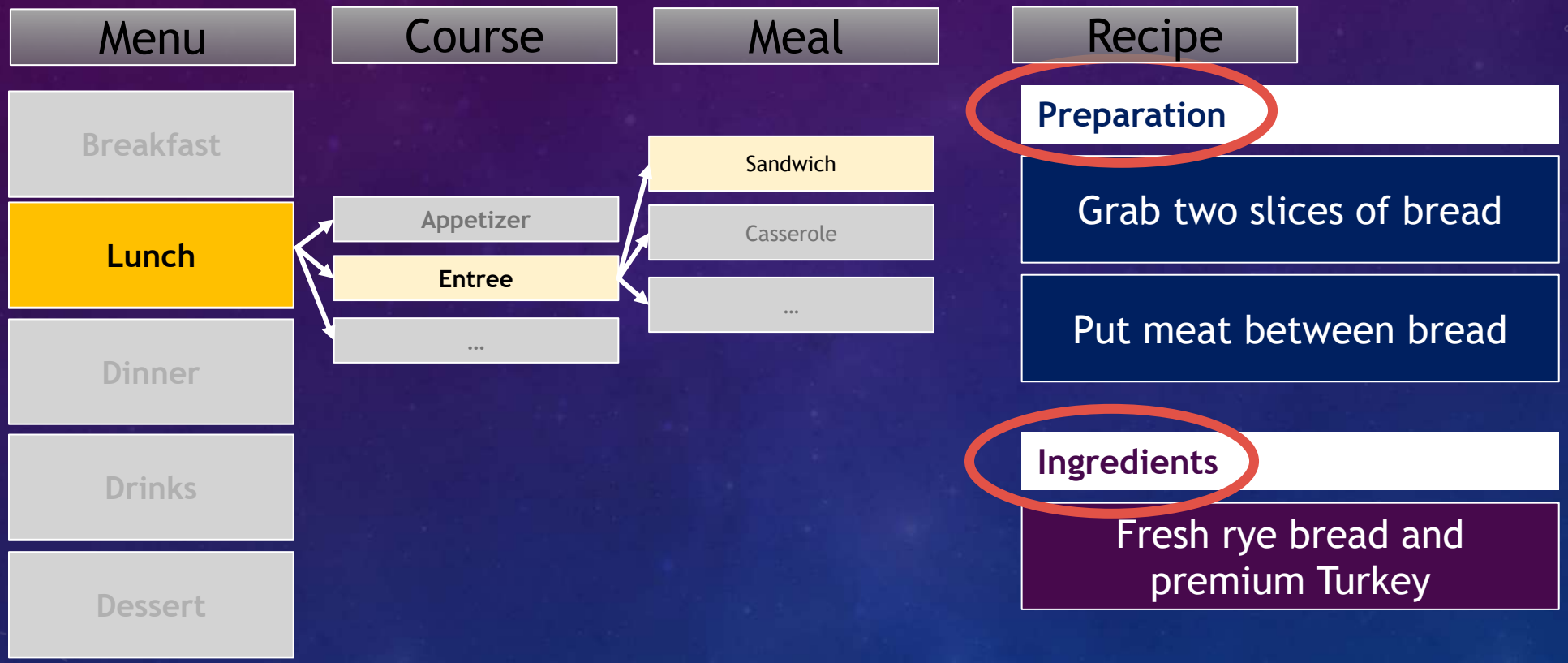
Crosswalk from the Framework for Improving Critical Infrastructure Cybersecurity V1.1 to the NIST Privacy Framework Core

Cybersecurity Framework Core			NIST Privacy Framework Subcategory
Function	Category	Subcategory	
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**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.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
		ID.AM-2: Software platforms and applications within the organization are inventoried	**ID.IM-P1:** Systems/products/services that process data are inventoried. **ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
		ID.AM-3: Organizational communication and data flows are mapped	**ID.IM-P8**: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.
		ID.AM-4: External information systems are catalogued	**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.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**GV.PO-P3**: Roles and responsibilities for the workforce are established with respect to privacy.

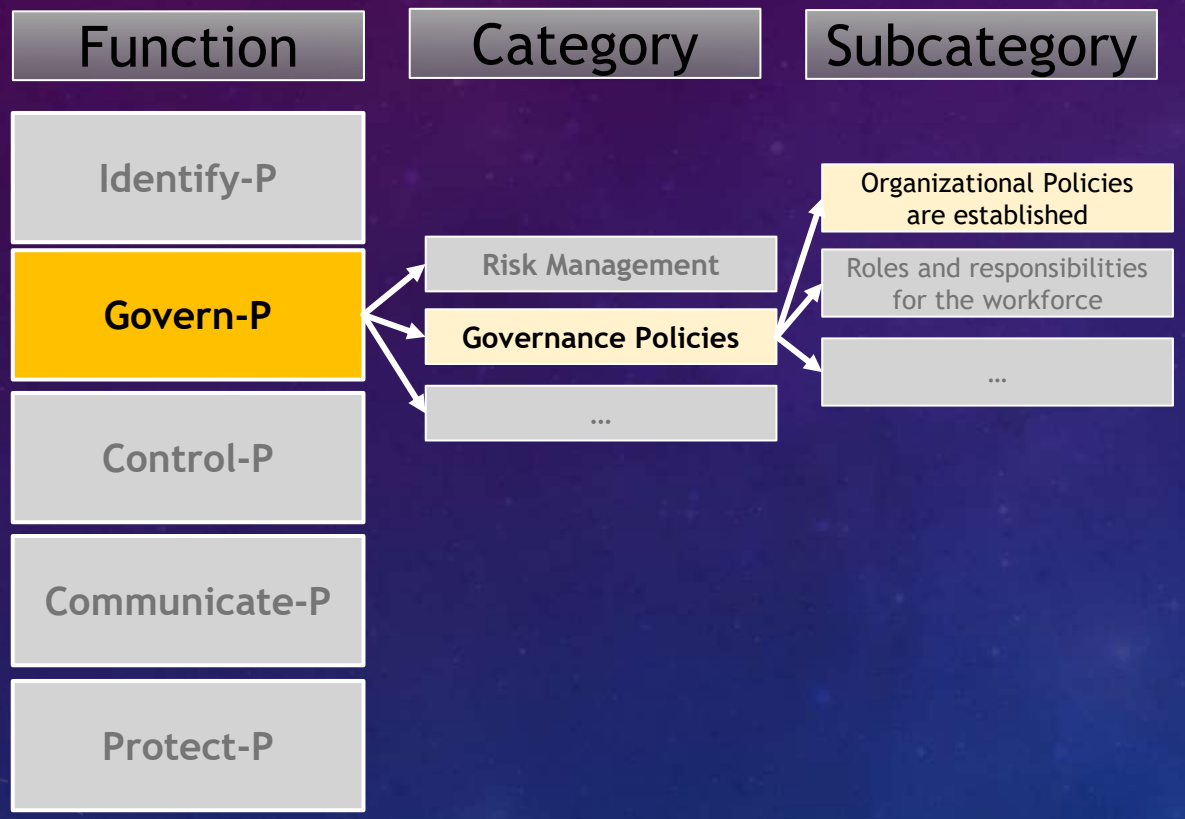
PRIVACY FRAMEWORK - CORE



PRIVACY FRAMEWORK - PROFILES



PRIVACY FRAMEWORK - PROFILES



Procedural / Tasks

Policies are available on the corporate intranet

Policies are reviewed and approved by executives

Substantive

We do not monetize data

PRIVACY FRAMEWORK - PROFILES

CURRENT PROFILE

Subcategory

Organizational Policies are established

TARGET PROFILE

Procedural / Tasks

Policies are available on the corporate intranet

Policies are reviewed and approved by executives

Substantive

We do not monetize data

able on the
tranet

n stakeholders

Hold stakeholder roundtable and seek input and review

adership team
licies

We do not monetize data

We do not send unsolicited communications

PRIVACY FRAMEWORK - IMPLEMENTATION TIERS

- Partial
- Risk Informed
- Repeatable
- Adaptive

TARGET PROFILE

Policies are available on the corporate intranet

Identify organization stakeholders

Hold stakeholder roundtable and seek input and review

Have executive leadership team approve policies

We do not monetize data

We do not send unsolicited communications

PRIVACY FRAMEWORK - IMPLEMENTATION TIERS

Partial

Myth: **Tiers = maturity model**

Tiers are about determining capabilities
Maturity is about operational effectiveness of your capabilities

TIERS vs MATURITY

Limited incorporation of risk

Tiers

Maturity

Ad-hoc	Unwritten policy to have secure facilities			
Repeatable	Official corporate policy to secure facilities			
Defined	Policy distributed to all facilities: “We put alarms on all our doors”			
Managed	Facilities managers trained on policy. Attestation they are following policies.			
Optimized	Doors audited, tested. Alarms upgraded.			

Risk assessment can cover multiple situations

Review of risk literature informs policy

Dynamic risk analysis done results in changes to written policies

RISK BASED

Risks to Individuals

- Tangible Harms
  - Financial, physical, emotional
- Moral Harms
  - Violations of Rights and Freedoms
  - Privacy Violations

Risk Arising from the Data Processing Ecosystem

KEY FEATURES OF NIST PRIVACY FRAMEWORK

- It is a framework
  - Every restaurant needs menus, courses, meals
  - But the framework doesn't tell you what to cook or how to cook
  - NOT a prescriptive checklist ☑

- Risk based *(no specific risk model)*
  - Personal not organizational

1. NIST PRAM (Privacy Risk Assessment Methodology)
2. FAIR-Privacy (Factors Analysis of Information Risk for Privacy)

- **Ecosystem** risks not just supply chain risks
  (holistic view of how the organization is affecting privacy in society)

RESOURCES

- NIST Privacy Framework
- NIST Privacy Engineering Collaboration Space
  - NIST Privacy Risk Assessment Method
  - FAIR for Privacy Risk Assessment Method
- Book: Strategic Privacy by Design, 2nd Edition
- Summary Infographic

2 Day Training Intensive
December 2022
privacybydesign.training/nist

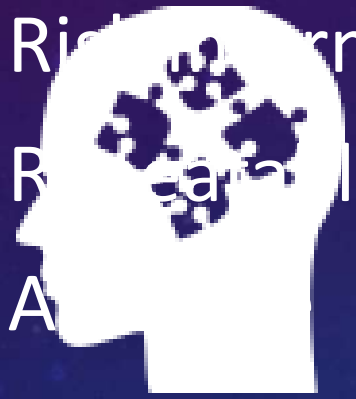
PRIVACY FRAMEWORK - IMPLEMENTATION TIERS

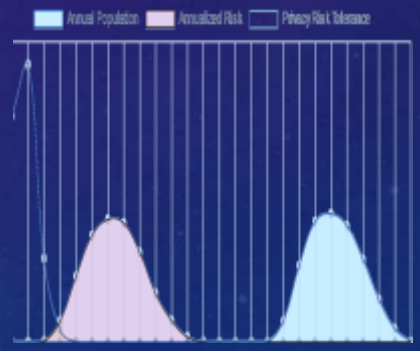
Partial

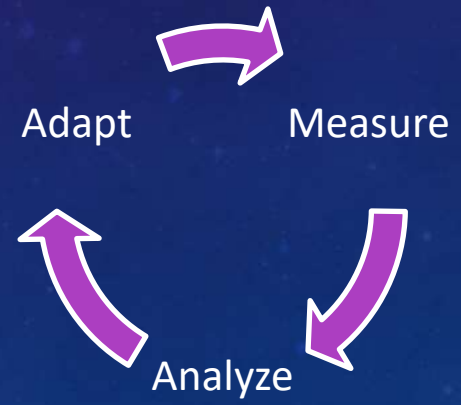
Ri[illegible]rmed

R[illegible]le

A[illegible]







Implementation tiers are levels of inclusion of risk considerations in setting target