#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PRV-T09**

The Steps to Successfully Baking Privacy into an IAM Implementation

Christine C. Owen

Director
Guidehouse Inc
cowen@guidehousefederal.com

Jamie M. Danker

Senior Director
Venable LLP
JMDanker@Venable.com

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 Venable LLP. This presentation is intended as a summary of the issues presented and is not intended to provide legal advice. It is provided for the general information of the attendees. Legal counsel and advice should be sought for any specific questions and before taking any action in reliance on the information presented.

Agenda

Our Preparation

Our Recipe

Your Journey Towards a More-Secure, Privacy-Enhanced Network

Our Preparation

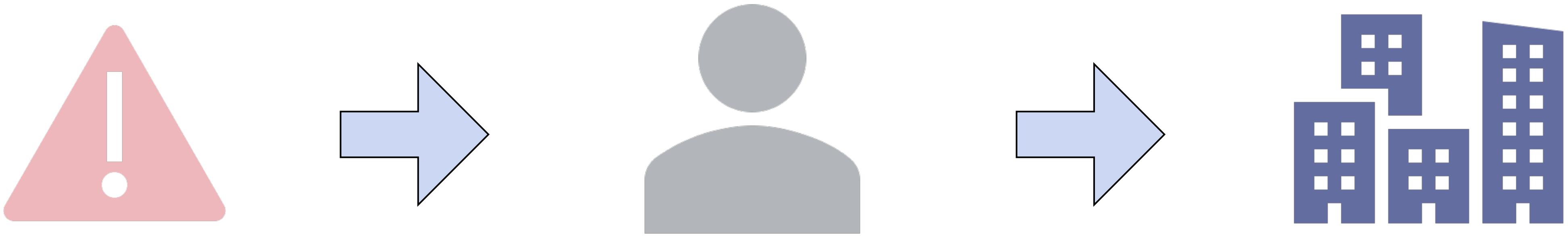
Current Regulatory Landscape

GDPR
CCPA
Privacy Act of 1974
EXECUTIVE ORDER
ON IMPROVING THE NATION'S
CYBERSECURITY

Identity and Privacy Are Key for a Successful Zero Trust Implementation

- The Perimeter Is Identity
- Remote and Biometric Identity Proofing Enhances Identities
- Phishing-resistant MFA and Contextual Authentication Are Critical
- Automated Identity Governance Rules Control Access
- Loss Prevention Protects Data and Privacy

Privacy Risk and Organizational Risk



Problem

Arises from data processing

Individual

Experiences direct impact

(e.g., embarrassment, discrimination, economic loss)

Organization

Resulting impact

(e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

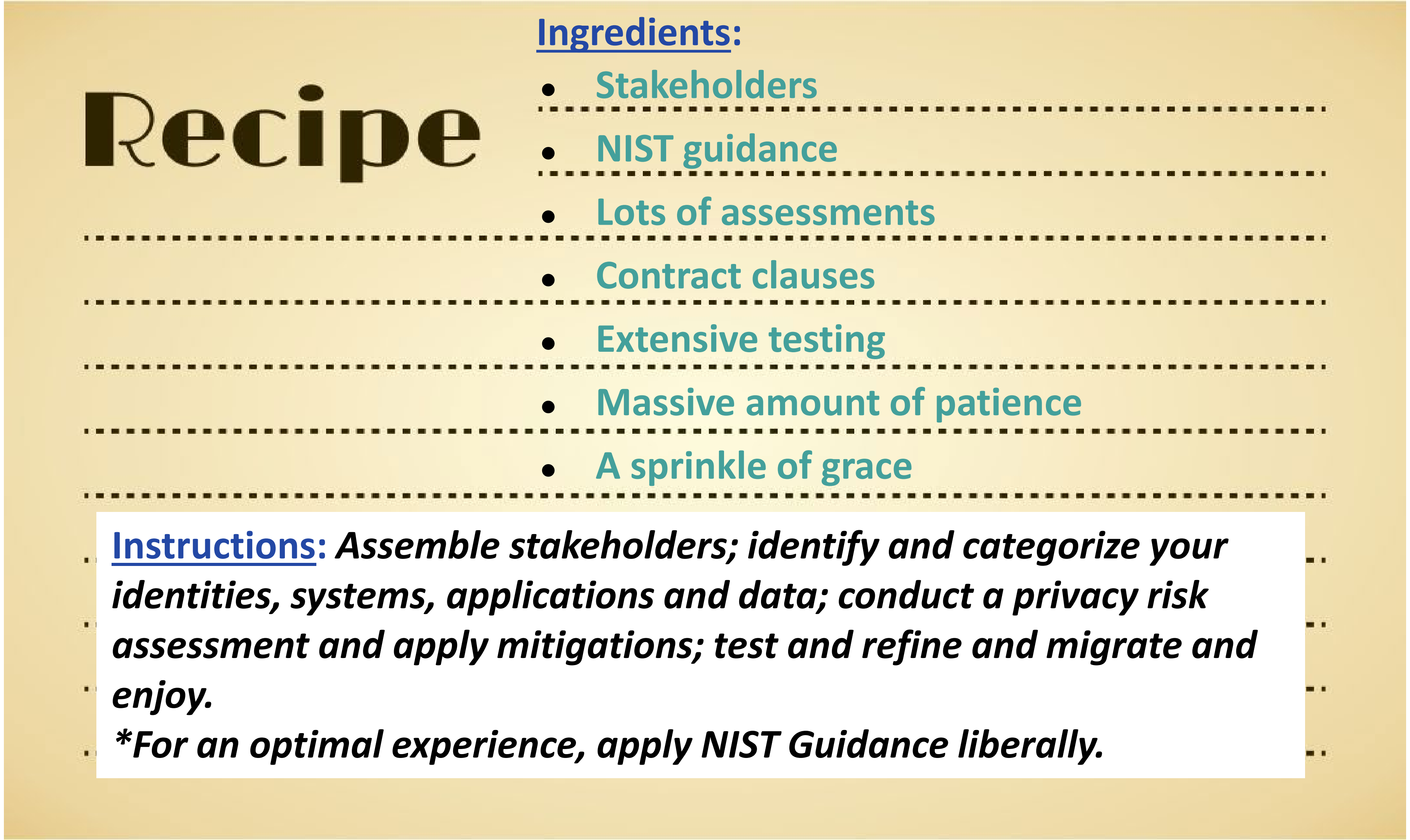
Source: NIST

Stakeholder Management

RSA®Conference2022

Our Recipe

Privacy Preserving IAM/ZTA Implementation Recipe



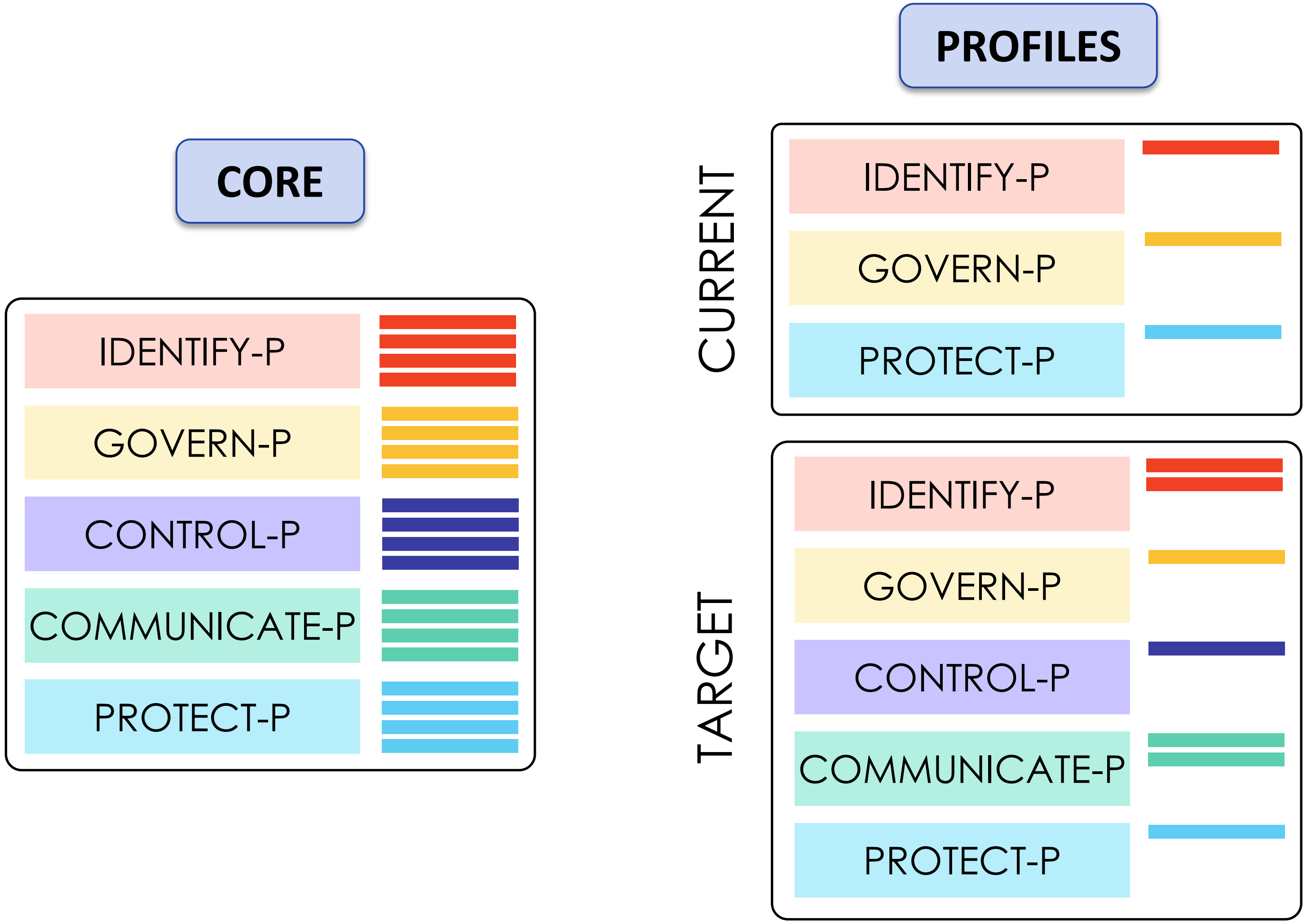
Ingredients:

- Stakeholders
- NIST guidance
- Lots of assessments
- Contract clauses
- Extensive testing
- Massive amount of patience
- A sprinkle of grace

Instructions: ***Assemble stakeholders; identify and categorize your identities, systems, applications and data; conduct a privacy risk assessment and apply mitigations; test and refine and migrate and enjoy.***

****For an optimal experience, apply NIST Guidance liberally.***

Our Best Kept Secret Recipe: The NIST Privacy Framework



CORE

IDENTIFY-P

GOVERN-P

CONTROL-P

COMMUNICATE-P

PROTECT-P

PROFILES

CURRENT

IDENTIFY-P

GOVERN-P

PROTECT-P

TARGET

IDENTIFY-P

GOVERN-P

CONTROL-P

COMMUNICATE-P

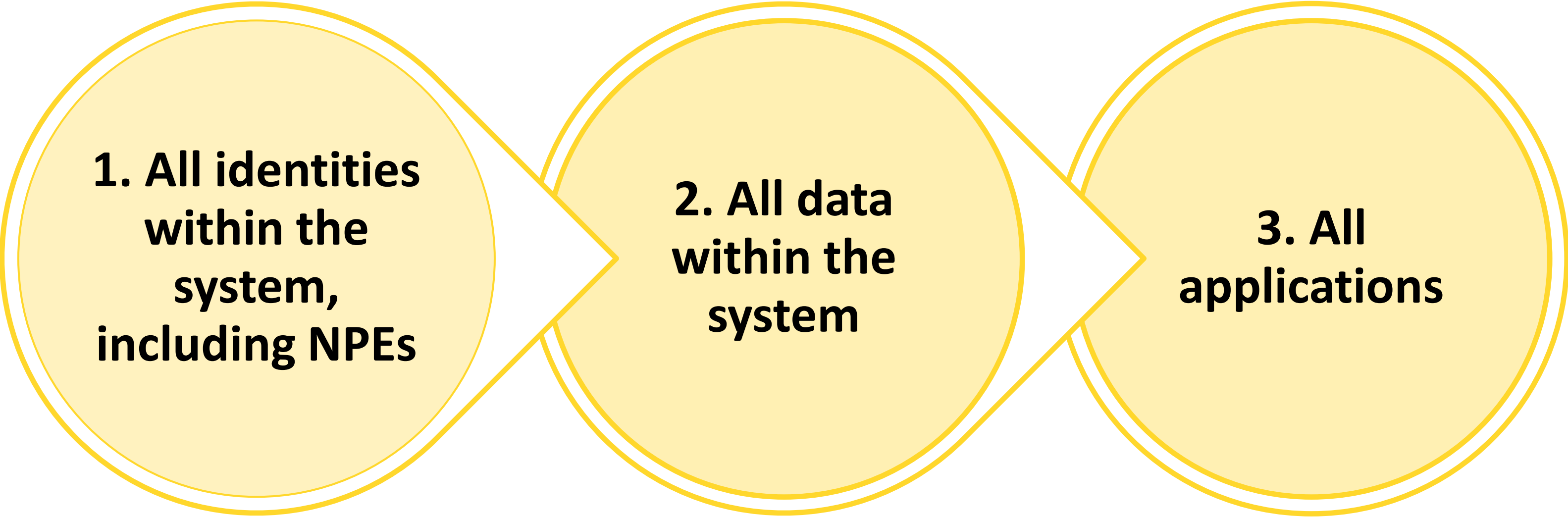
PROTECT-P

***Consider:**

- Organizational goals
- Role(s) in the data processing ecosystem or industry sector
- Legal/regulatory requirements & industry best practices
- Organization’s risk management priorities
- Privacy needs of individuals

Source: NIST

Identify & Categorize



1. All identities within the system, including NPEs

2. All data within the system

3. All applications

***Privacy Pro tip:** Leverage the NIST Privacy Framework's Inventory and Mapping Category

Privacy Pro’s Favorite Categories for IAM: Mini Profile

ID-P

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, other risk management priorities

ID-P

Inventory and Mapping (ID.IM-P)

Data processing by systems, products, or services is understood and informs the management of privacy risk.

CT-P

Disassociated Processing (CT.DM-P)

Data processing solutions increase dissociability consistent with the organization’s risk strategy to protect individuals’ privacy and enable implementation of privacy principles (e.g., minimization).

CM-P

Data Processing Awareness (CM.AW-P)

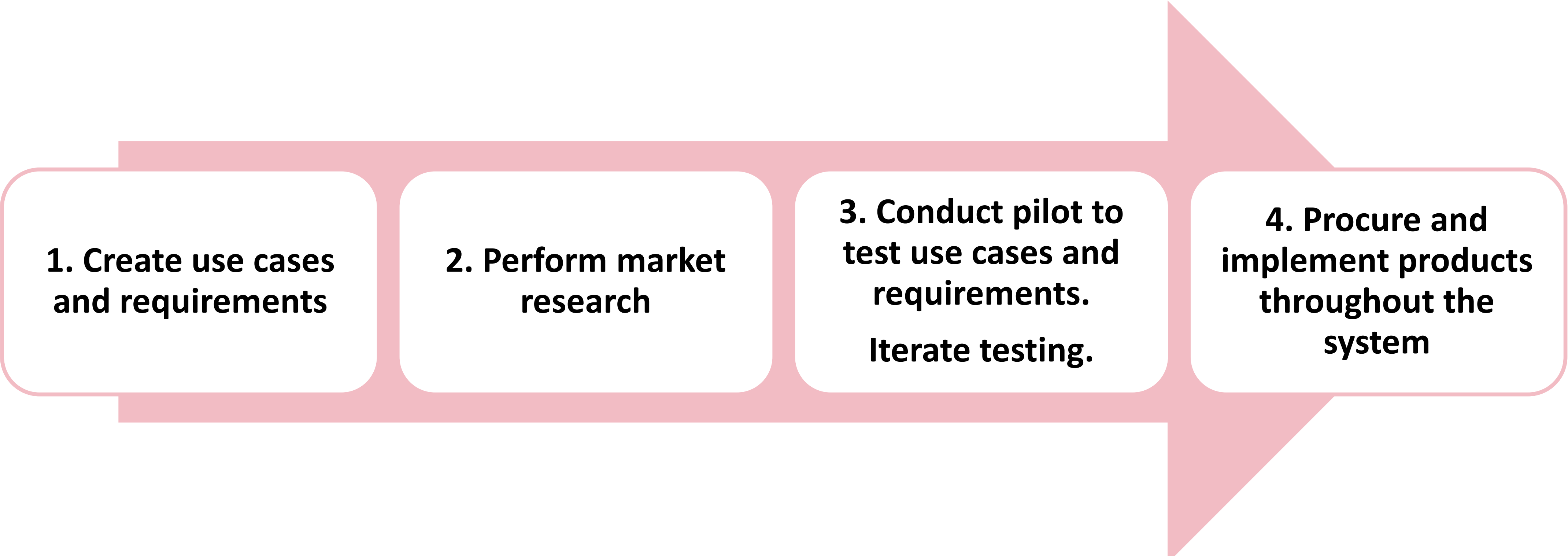
Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization’s risk strategy to protect individuals’ privacy.

PR-P

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.

Research & Prepare



1. Create use cases and requirements

2. Perform market research

3. Conduct pilot to test use cases and requirements.

Iterate testing.

4. Procure and implement products throughout the system

***Implementation Pro tip:** To learn where the weaknesses are, develop, test, and iterate steps 2 & 3 to find breakage within the system and develop solutions.

What Could Possibly Go Wrong?

Migrate Users & Apps – Enjoy!

RSA® Conference2022

Your Journey Towards a More-Secure, Privacy-Enhanced Network

Where to Begin

Immediately

Schedule a privacy/security meetup next week to discuss the privacy requirements for your IAM and Zero Trust integrations

Short Term

Assess your current IAM posture

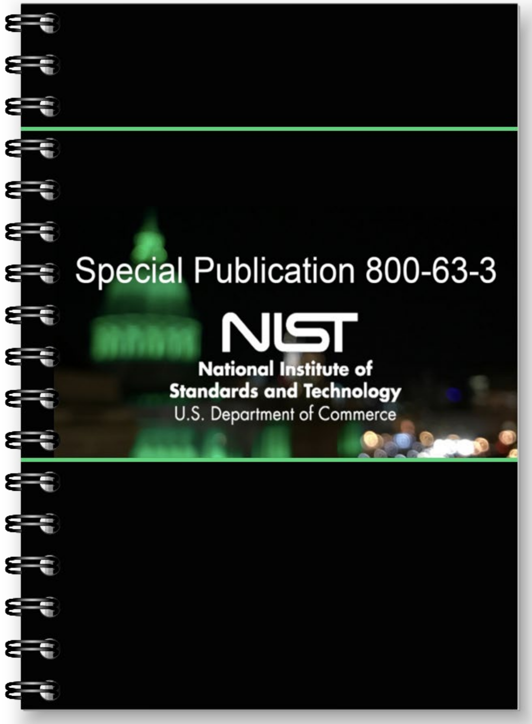
Implement phishing resistant MFA

Long Term

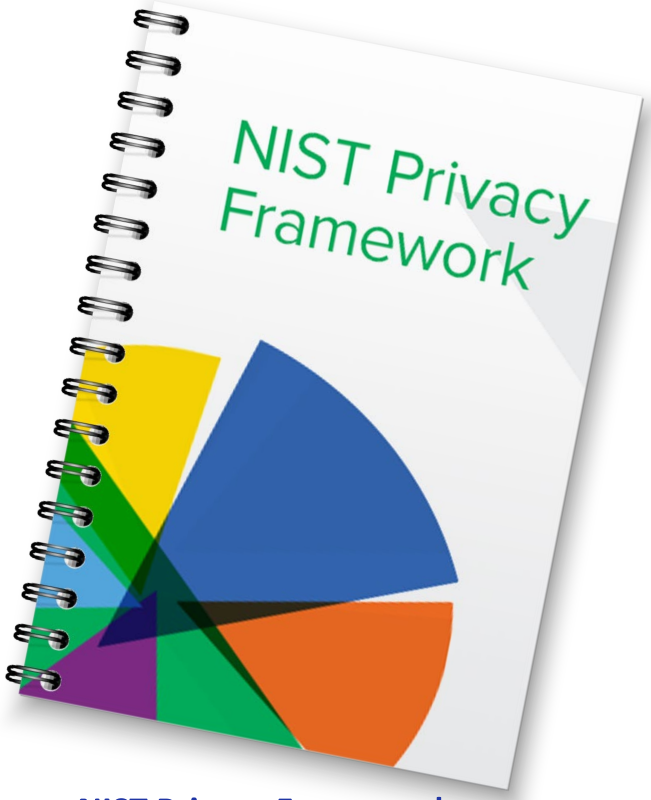
Apply the recipe and make note of your own variations; document success and recipe fails and share with others!

Recipe Book Recommendations

NIST SP 800-207



NIST SP 800-63-3



NIST Privacy Framework

Thank you!

Questions?