

Enhancing Internal Audit with a Privacy Control Framework



The Institute of
Internal Auditors
Chicago

Kristen Rohrer & Luke Pillarella

March 18, 2024

Chicago IIA Annual Seminar

Introduction



Speaker Bio



Kristen Rohrer

Privacy Consulting Manager, CIA & CIMP
Kristen.Rohrer@crowe.com

As a privacy professional of the Crowe Privacy and Data Protection team and background in internal audit, Kristen has lead a variety of privacy projects across clients within the life science, manufacturing, technology and healthcare. She has specialized in assessing privacy programs, building privacy frameworks and working with companies to be in a place to utilize privacy metrics.



Luke Pillarella

Privacy Consulting Senior, cGMP
Luke.Pillarella@crowe.com

As a Privacy, Data Protection, and Compliance Senior Consultant at Crowe, Luke has three years of extensive experience in spearheading privacy program implementations, executing comprehensive assessments, and managing AI risk. Luke's professional portfolio covers an array of industries from pharmaceuticals and biotechnology to manufacturing, cannabis, and banking, providing adaptable and forward-thinking strategies for process enhancements and managed services.



Learning Objectives



Understand the current privacy regulatory landscape.



Gain a thorough understanding of privacy control frameworks and their relevance to Internal Audit.



Develop the skills to effectively integrate privacy controls into Internal Audit processes.



Acquire practical knowledge and best practices through real-world examples.

Agenda

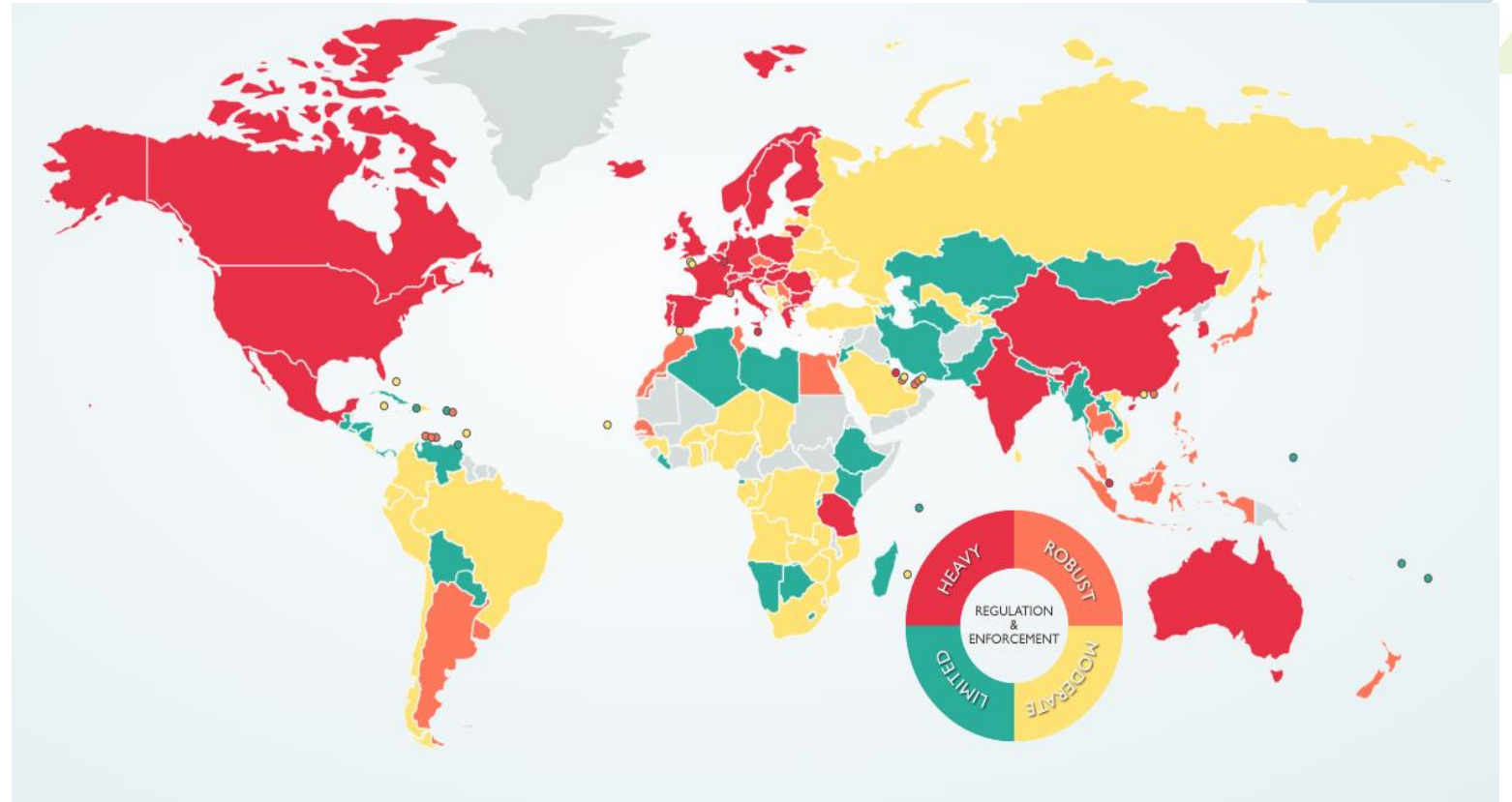
-
1. Introduction
 2. Privacy landscape overview
 3. What is a privacy framework?
 4. NIST privacy framework & others
 5. Customizing frameworks
 6. Why do you need a privacy framework?
 7. How to establish a privacy framework
 8. Internal Audit and Privacy Synergy
 9. Q&A

Privacy Landscape Overview



Global Privacy View

- Rising complexity in global privacy laws demands advanced compliance strategies.
- It is essential for internal audit to grasp the full spectrum of privacy risks for effective risk management.
- Changing privacy laws shape audit scope and goals, requiring agility and alertness.



Source: www.dlapiperdataprotection.com



Monitoring Privacy Law

Staying abreast of changing privacy requirements is essential. Here are a few common sources for monitoring privacy laws and regulations:



Legislation and
Regulations



Government
Agencies



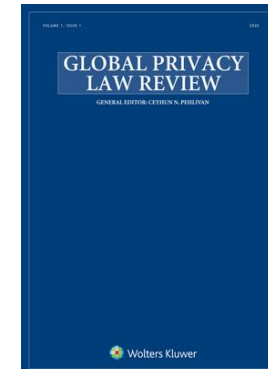
Industry
Associations



Legal Publications



Webinars and
Conferences



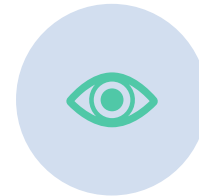
Key Takeaways



Privacy is integral to risk management and organizational integrity.



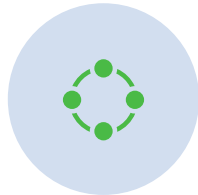
Internal audit shapes and mitigates privacy risks strategically.



Privacy risks are essential in audit planning for thorough oversight.



Auditors must be up-to-date with privacy trends to manage risks effectively.



Cross-functional collaboration ensures privacy is woven into business processes.



Proactive privacy risk management by internal audit enhances trust and confidence.



Polling Question 1

What is your level of involvement with privacy-related audits?

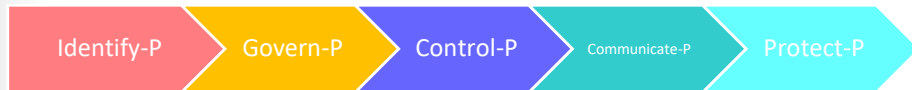
- A. I lead and conduct privacy-related audits.
- B. I participate as a team member in conducting privacy audits.
- C. I provide support or expertise for privacy audits but am not directly involved in auditing.
- D. I have no involvement in privacy-related audits.
- E. My company hasn't started performing privacy related audits.

What is a Privacy Framework?



Defining a Privacy Framework

- A privacy framework serves as the foundational structure for developing and managing a comprehensive program that fulfills privacy obligations and addresses risks while promoting business opportunities.
- By aligning a privacy framework with measurable metrics, organizations can increase their privacy maturity, enabling continuous improvement and clearer visibility into privacy practices.
- Mapping a privacy framework to specific metrics can reveal the convergence between privacy controls and regulatory requirements, streamlining compliance efforts.



NIST



AICPA[®]



ISO 27701



The Institute of
Internal Auditors
Chicago

Benefits of Using a Framework

- ✓ Risk-based approach
- ✓ Proactive vs. Reactive
- ✓ Stable core structure amid regulatory uncertainty
- ✓ Ethical decision-making
- ✓ Resource and budget prioritization
- ✓ Aligning with industry standards
- ✓ Builds customer trust through transparent practices.



Polling Question 2

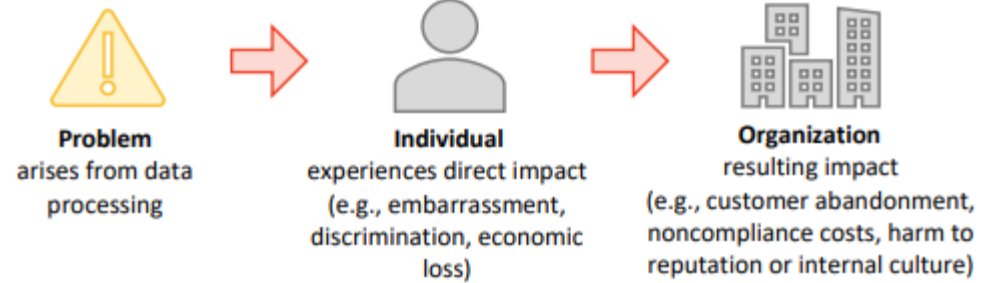
Does your organizations internal audit function review privacy controls?

- A. Yes, regularly as part of our standard audit procedures.
- B. Occasionally, but not as a routine part of our audits.
- C. No, privacy controls are reviewed by a separate compliance function.
- D. Unsure/Not applicable to our organization.

NIST Privacy Framework & Other Types of Frameworks






NIST Overview and IA's relevance



<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>

NIST Privacy Alignment Example

-  Alignment with NIST Privacy Framework v1.0
-  Library of privacy risks
-  Library of privacy controls
-  Library of privacy Key Risk Indicators

Optimized Maturity

NIST Privacy Framework	Risks	Controls	KRIs/KPIs
IDENTIFY	12	18	3/1/35
GOVERN	18	20	53
CONTROL	14	22	40
COMMUNICATE	8	8	25
PROTECT	27	28	90
Totals	79	96	247

**Risks, controls, and KRI's are subject to change as content is refined by Crowe due to regulatory updates, framework updates, or general improvements.*

Example Framework – NIST Privacy Framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>

Metrics mapped to a framework allows you to organize, focus, and align activities:



Other Common Privacy Frameworks

Fair Information Practices (**FIPs**) - provide basic privacy principles central to several modern frameworks, laws, and regulations

- rights of individuals (notice, choice and consent, data subject rights),
- controls on information (information security, information quality),
- information life cycle (collection, use and retention, disclosure, destruction),
- and management (management and administration, monitoring, enforcement)

The Organization for Economic Co-operation and Development (**OECD**) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data are the most widely accepted privacy principles; together with the Council of Europe's Convention 108, they are the basis for the EU Data Protection Directive and GDPR.

The **AICPA/CICA Privacy Task Force**, developed the Generally Accepted Privacy Principles (GAPP) to guide organizations in developing, implementing and managing privacy programs in line with significant privacy laws and best practices.

The **Canadian Standards Association (CSA) Privacy Code** became a national standard in 1996 and formed the basis for the Personal Information Protection and Electronic Documents Act (PIPEDA)

Customizing Frameworks



Crowe Privacy Framework



Polling Question 3

Is your organization using a framework today to help manage your privacy program?

- A. Yes, we are using the NIST Privacy Framework
- B. Yes, we are using ISO 27701
- C. Yes, we are using the OECD Privacy Framework
- D. Yes, we are using the AICPA Privacy Management Framework
- E. Yes, we have developed our own privacy framework.
- F. We are not currently using a framework, or our framework isn't listed

Why Do You Need a Privacy Framework?



Enhancing Audit with a Privacy Framework



A privacy framework helps evaluate the maturity of the privacy program



The components enable systematic evaluation of privacy controls, risk identification, risk mitigation, and consistent audit reporting



Internal audit plays a key role in assessing the effectiveness of the privacy framework, testing controls, and suggesting improvements for enhanced privacy protection.

How Structure Supports Audit Planning

- The privacy framework highlights key risks and prescribes relevant controls for targeted oversight, facilitating a strategic audit focus.
- Audit activities are structured to systematically address key privacy concerns.
- A structured framework broadens the scope of audit coverage, aiming for a complete review that leaves no aspect of privacy overlooked.

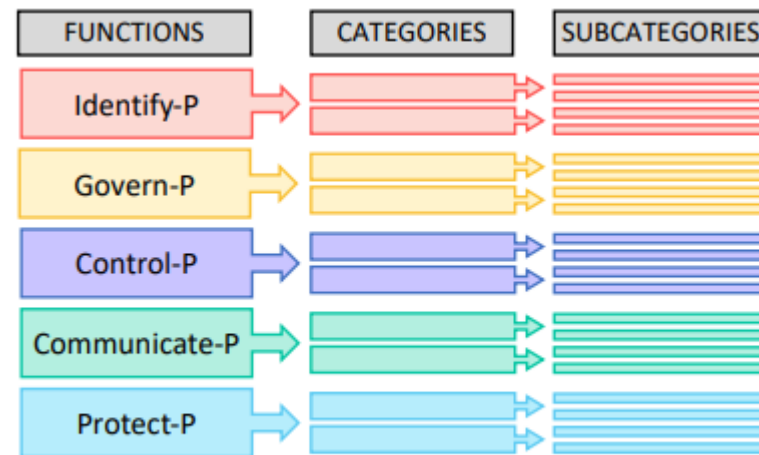


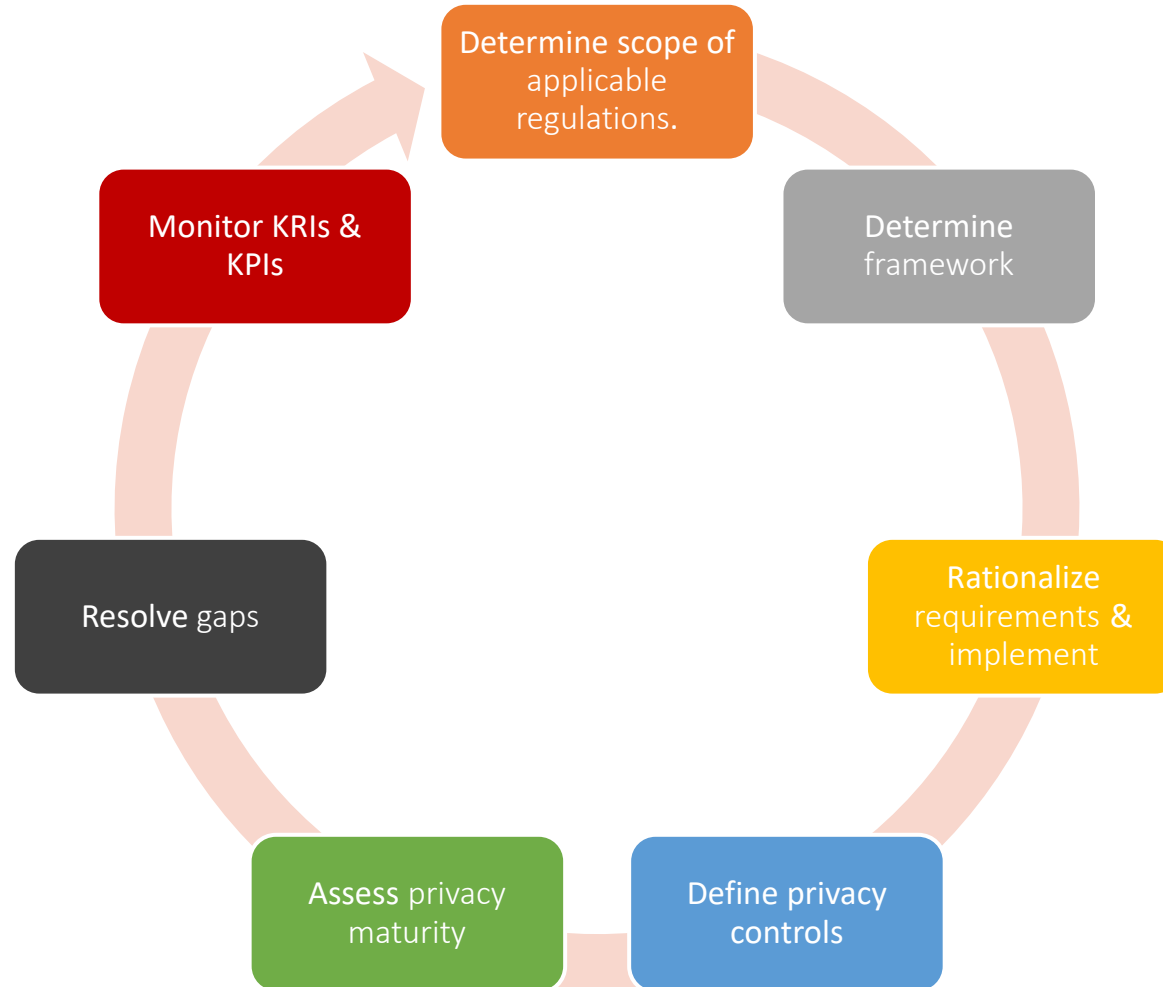
Figure 4: Privacy Framework Core Structure

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>

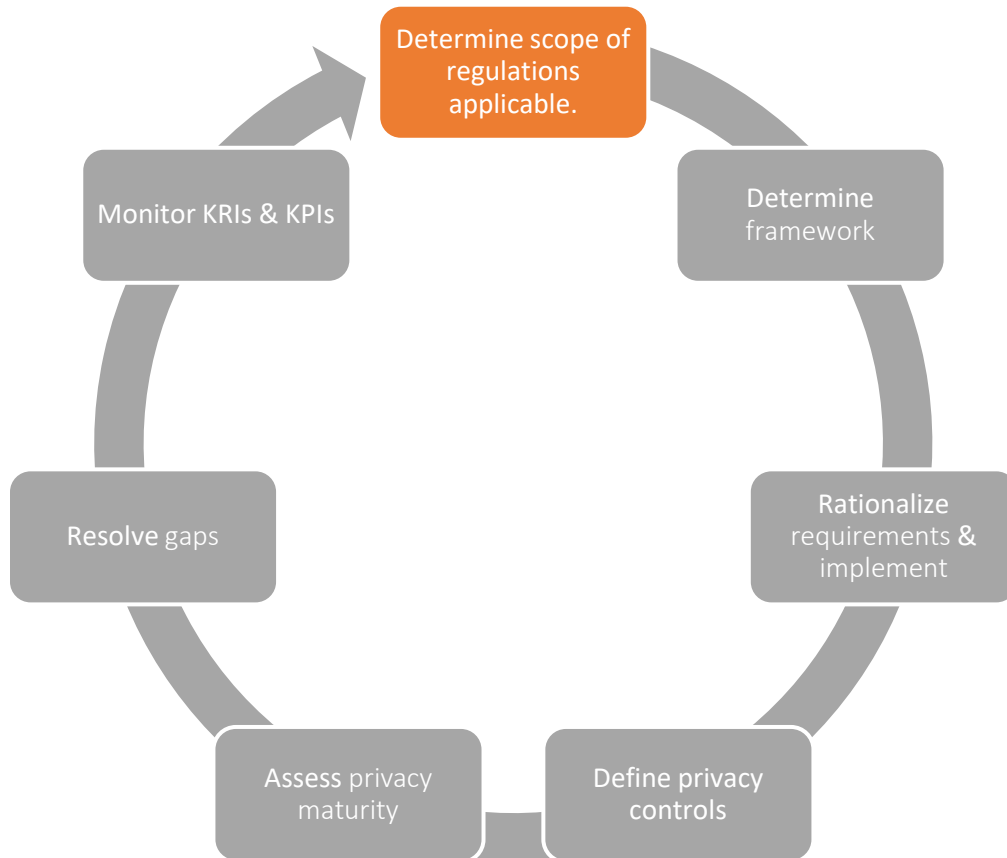
How to Establish a Privacy Framework?



Privacy Framework Lifecycle



Determine scope of applicable regulations

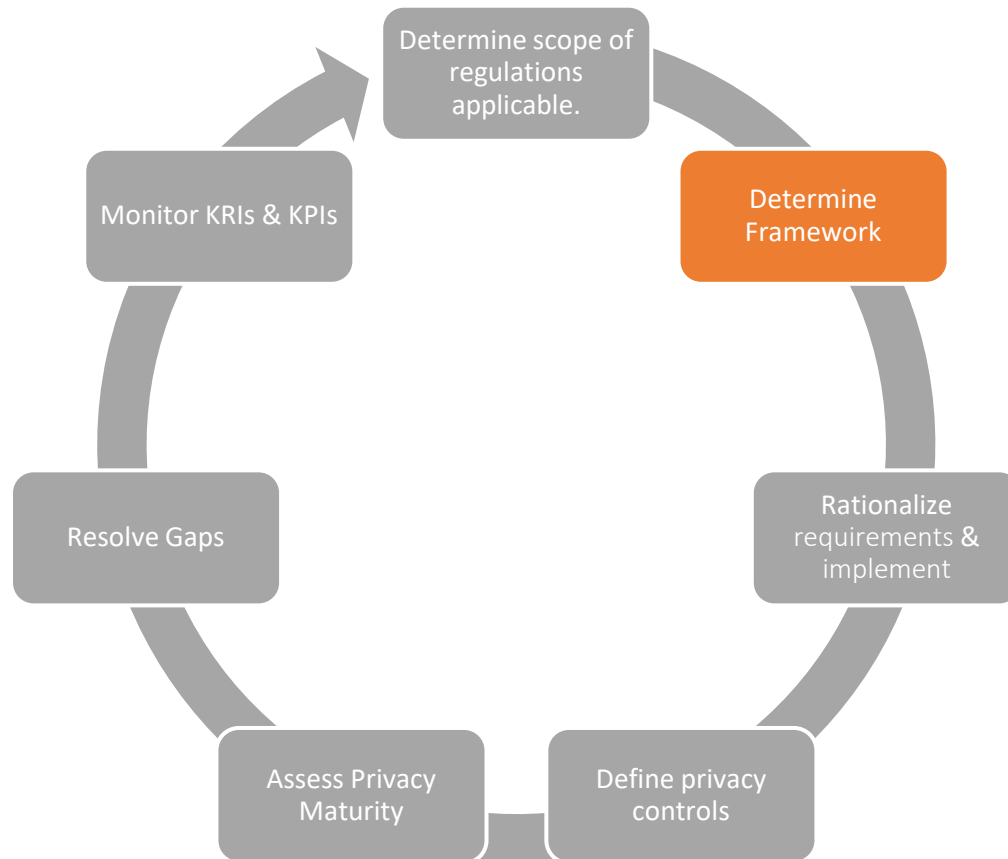


Determine scope of applicable regulations:

Consider the types of data you handle, the revenue thresholds that trigger specific legal obligations, and the volume of data processed to determine which regulations are applicable to your organization.



Determine Framework



Determine Framework:

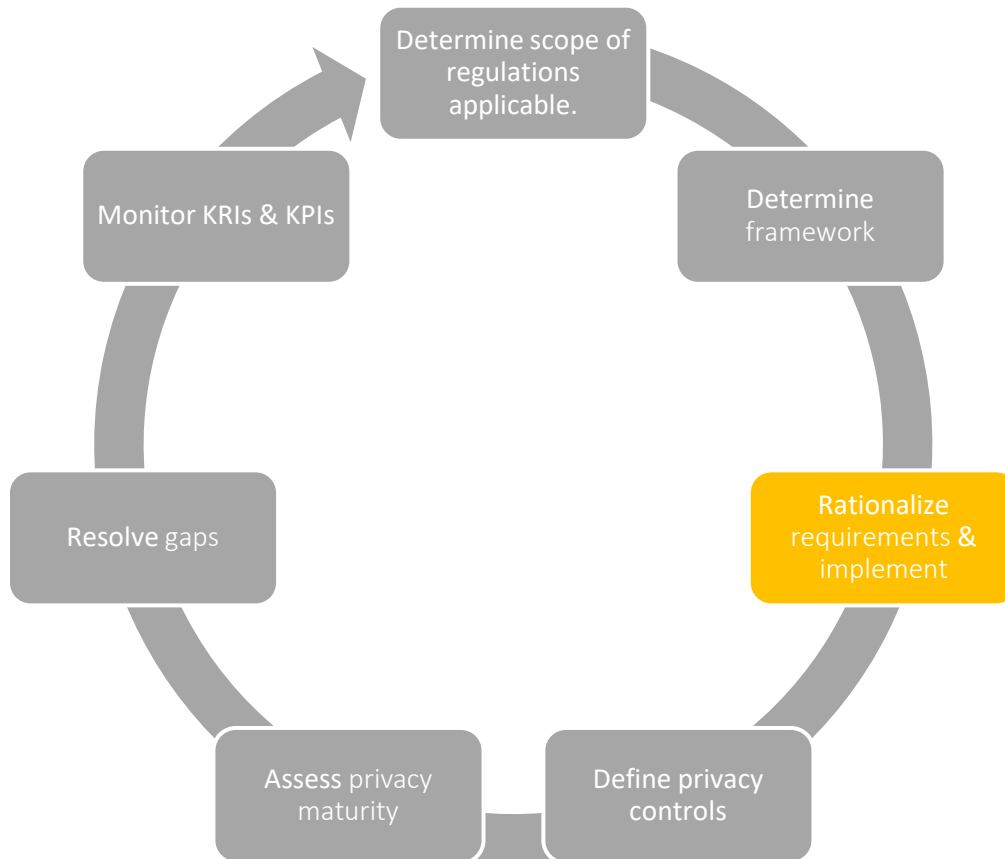
The International Association of Privacy Professionals (IAPP) categorizes privacy frameworks into two distinct types:

(1) Principles and Standards-based frameworks, which are designed around a set of core privacy principles and industry best practices

(2) Legal and Regulatory frameworks, which are grounded in specific laws, regulations, and compliance programs.



Rationalize Requirements

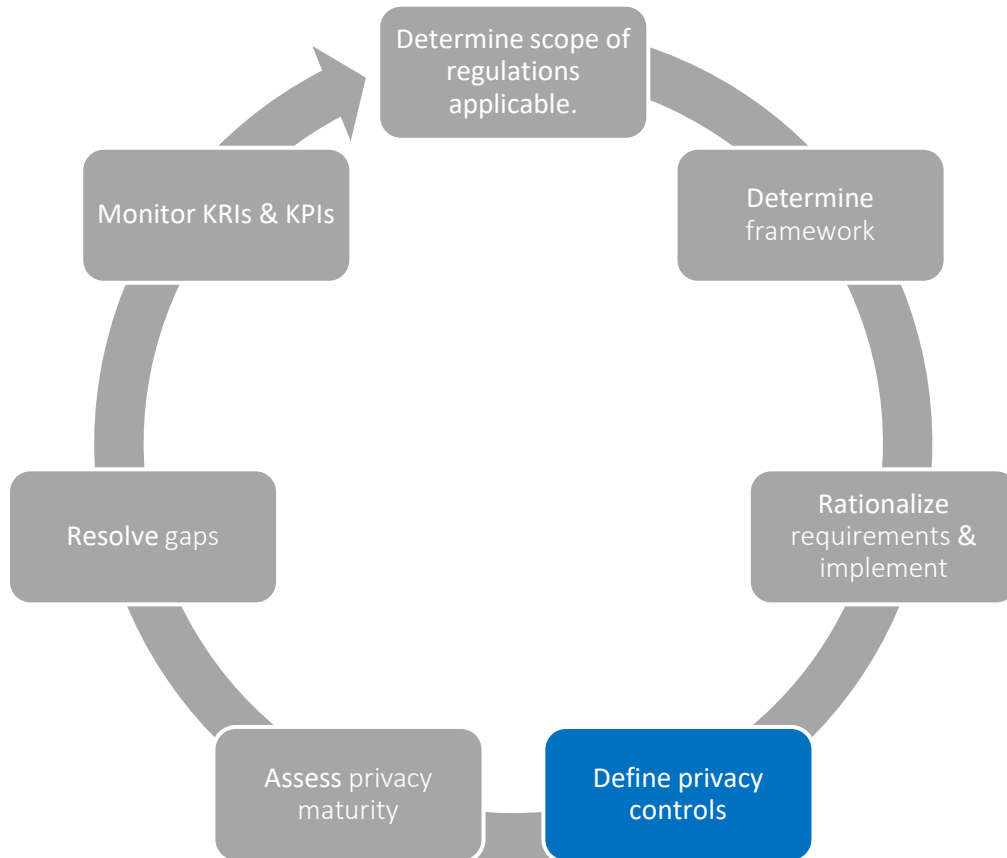


Rationalize requirements & implement:

Implement solutions that materially addresses requirements. For example, rationalizing the common legal obligation of providing individuals with a right of access to their personal information.



Define privacy controls

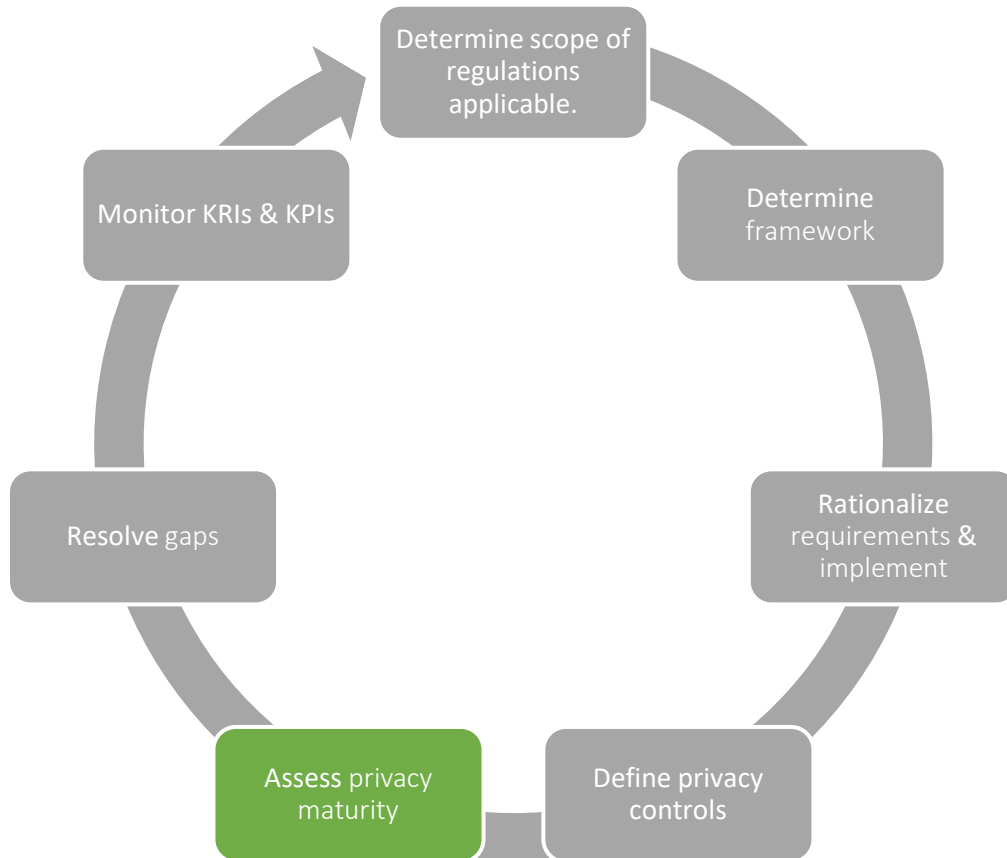


Define privacy controls:

Define privacy controls by establishing tailored measures that address your organization's unique data protection needs and risk profile.



Assess Privacy Maturity

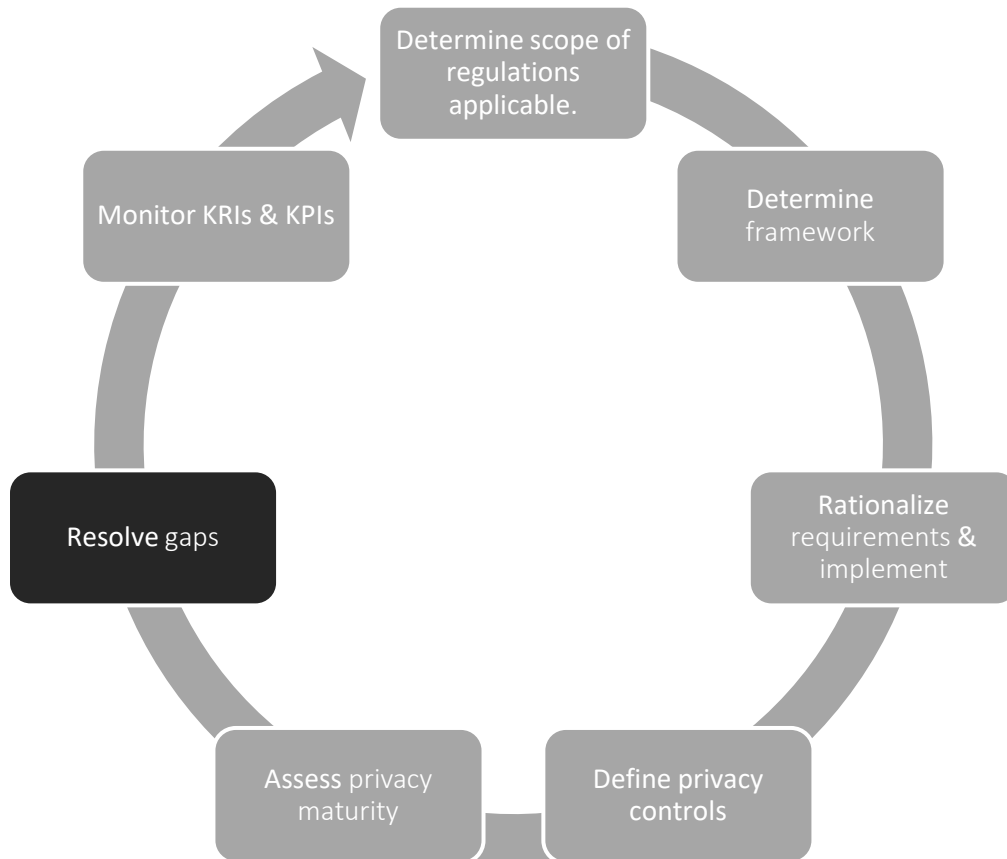


Assess Privacy Maturity:

Evaluate your company's privacy maturity level by measuring the implementation and effectiveness of the identified framework and corresponding set of controls against established benchmarks.



Resolve Gaps

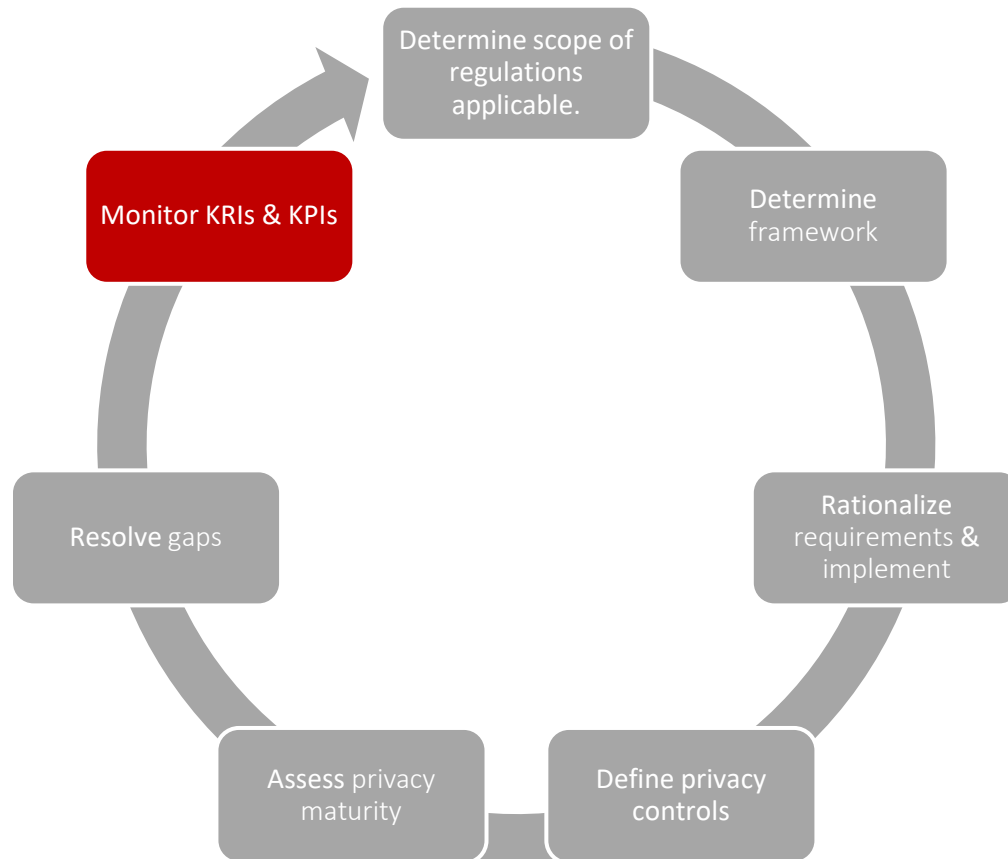


Resolve Gaps:

Address and remediate gaps highlighted by the assessment to enhance the maturity of your organization's privacy program.



Monitor KRIs and KPIs



Monitor KRIs and KPIs:

Track and analyze key performance indicators (KPIs) and key risk indicators (KRIs) to gauge the effectiveness and risk profile of your privacy controls.



Polling Question 4

Are you familiar with integrating a structured privacy framework into audit activities?

- A. Very familiar – I actively integrate it into audits.
- B. Somewhat familiar – I have some experience with it.
- C. Not familiar – I have not used it in audits yet.
- D. Unaware – I don't know about the NIST Privacy Framework.






Internal Audit and Privacy Synergy



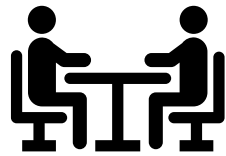
Role of IA in implementation

Internal audit plays a critical role, verifying that the strategy is practical, effective, and aligned with risk profiles. By adopting a suitable privacy framework, internal audit guides the creation of a comprehensive privacy program that:

-  Facilitates material compliance with relevant privacy laws and regulations, as verified through regular internal audits.
-  Acts as a competitive differentiator by demonstrating the organization's commitment to personal information protection, a factor that internal audit can help quantify and communicate.
-  Reinforces the organization's dedication to privacy, which internal audit can validate and report to stakeholders, customers, partners, and vendors, thereby enhancing trust and supporting business objectives.

**Internal audit's involvement is critical in the timing, development, and implementation of the privacy framework, which may differ across organizations based on specific needs and maturity levels.*

Bridging the Gaps



Internal audit can align language and priorities between privacy professionals and senior leadership, addressing common perspective differences.

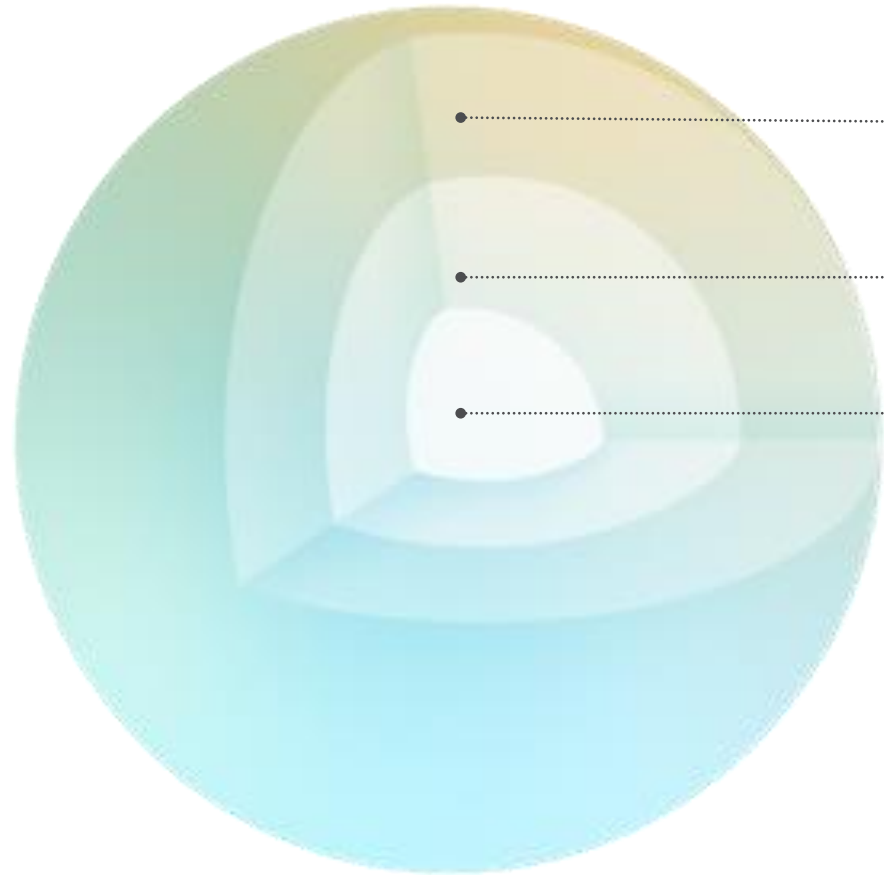
	Privacy Professionals	Senior Leadership
Technical vs. Business Language	Often use technical and legal terms when discussing privacy and data protection principles, practices, and compliance.	Generally, prefer more business-oriented language focused on risks, opportunities, and strategic decision-making.
Compliance vs. Strategic Focus	Tend to focus on compliance with privacy laws and regulations, ensuring data protection, and mitigating risks.	Often may prioritize strategic goals, revenue generation, and overall business objectives.
Detail-Oriented vs. High-Level	Often delve into the details of privacy policies, data processing activities, and legal requirements.	May prefer high-level summaries and overviews that highlight the key implications and business impact of privacy initiatives.
Legal vs. Practical	Generally, emphasize legal requirements and the need for strict compliance.	Can be more concerned with practical implementation, cost-effectiveness, and finding a balance between privacy and business needs.
Risk-Averse vs. Risk-Tolerant	Are necessarily risk-averse, focusing on minimizing privacy risks and ensuring compliance.	Could be more willing to accept certain risks in pursuit of business opportunities.



Strengthening IA Through Privacy Frameworks

- Provides a structured, standardized approach for consistent privacy evaluations
- Enables proactive risk identification and regulatory compliance alignment
- Demonstrates commitment to data stewardship, bolstering stakeholder trust.

Synergy Promotes Business Growth



General public and public relations

Stakeholders and investors

Data subjects
(such as employees, consumers)

Trust matters everywhere. It shapes your brand, your mission, and your reputation. Establishing trust with your data subjects promotes business growth.



Questions & Answers



Thank you.

Questions? Email



The Institute of
Internal Auditors
Chicago