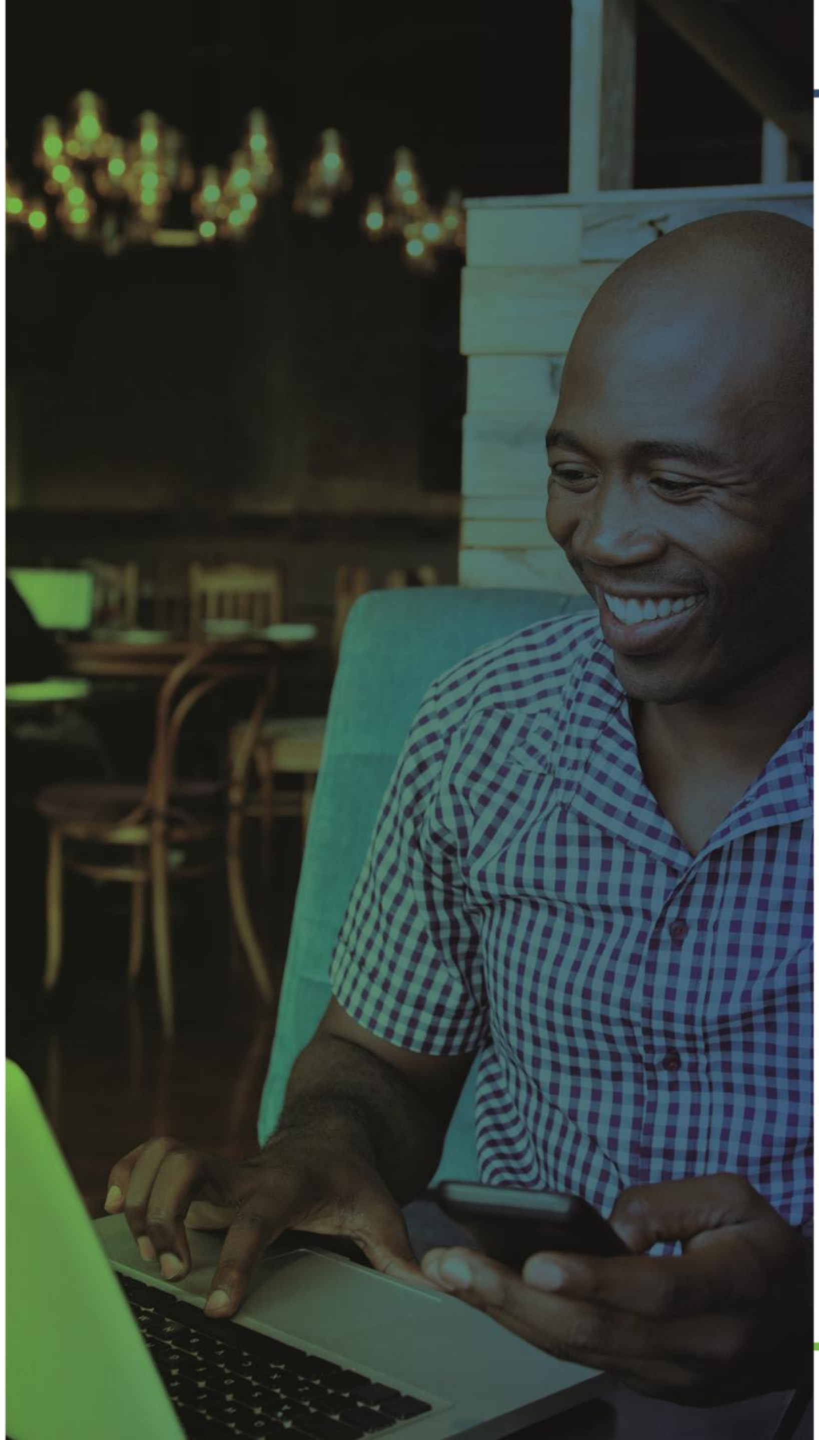


Demystifying Data Mapping: Why It Matters and How to Do It Well

Thursday, 15 February
10:00–11:00 PST
13:00-14:00 EST
19:00–20:00 CET

osano

KPMG

Introductions

Oskar Trpisovsky
MSc ETH, CIPM, CIPP/C, CIPP/US, CIPP/E

Senior Manager, Risk Consulting

KPMG Canada

Rachael Ormiston
CIPP/E, CIPM, CIPP/US, FIP

Head of Privacy

Osano

Agenda

- What is the most important insight from your data map?
- Why data mapping?
- Operationalizing your data map
- The big picture: The value of data mapping
- Questions and answers

What is the most important insight from your data map?

- **Data lineage:** Where has my organization's data come from and where is it going?
- **Data purpose:** Why do I have this data? How will my organization use it?
- **Asset overview:** What systems does my organization have? How do these systems accept and transfer data?
- **Risk identification:** If or when something goes wrong, is my organization's risk profile minimal?

KPMG Insights

Why Data Mapping?

You Can’t Do Data Without Privacy…

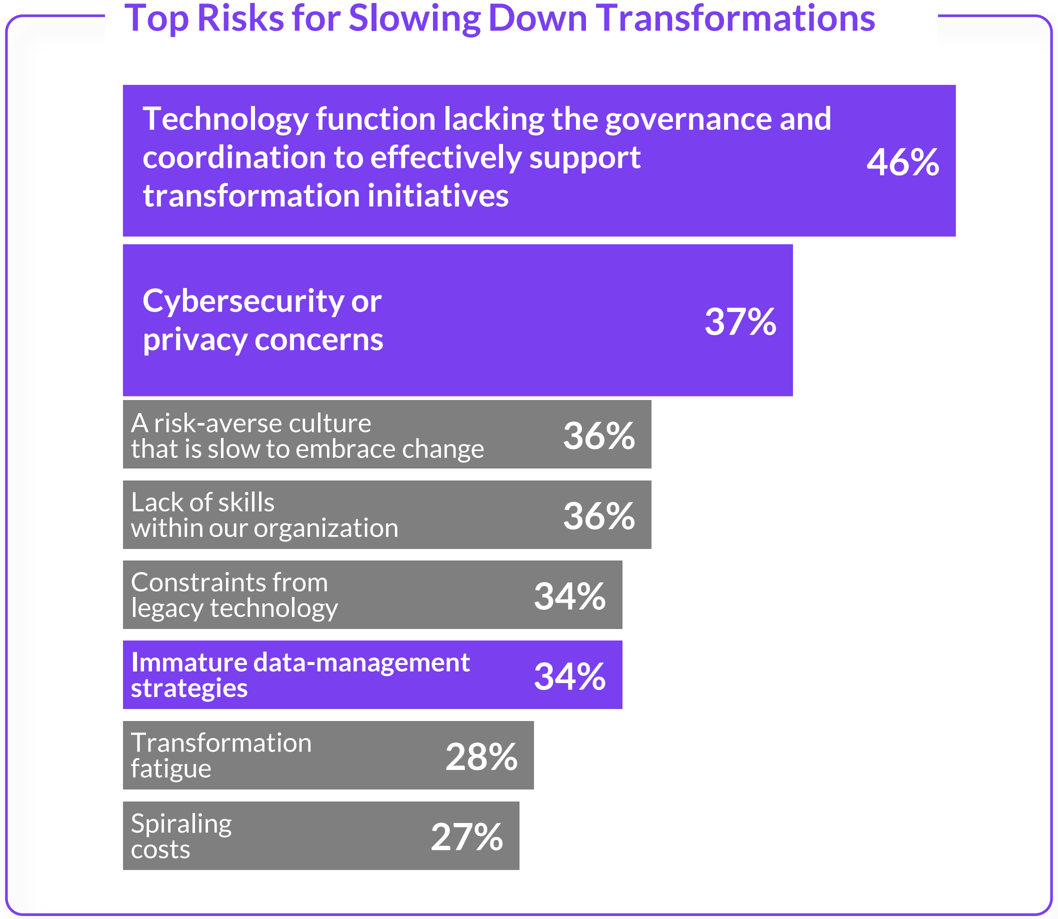
Positive Impact Of Data & Analytics

66% see an improvement in profitability or performance

Privacy & Cybersecurity

#1 Customer/user expectation with the most influence on strategic priorities within digital transformation projects

Top Risks for Slowing Down Transformations

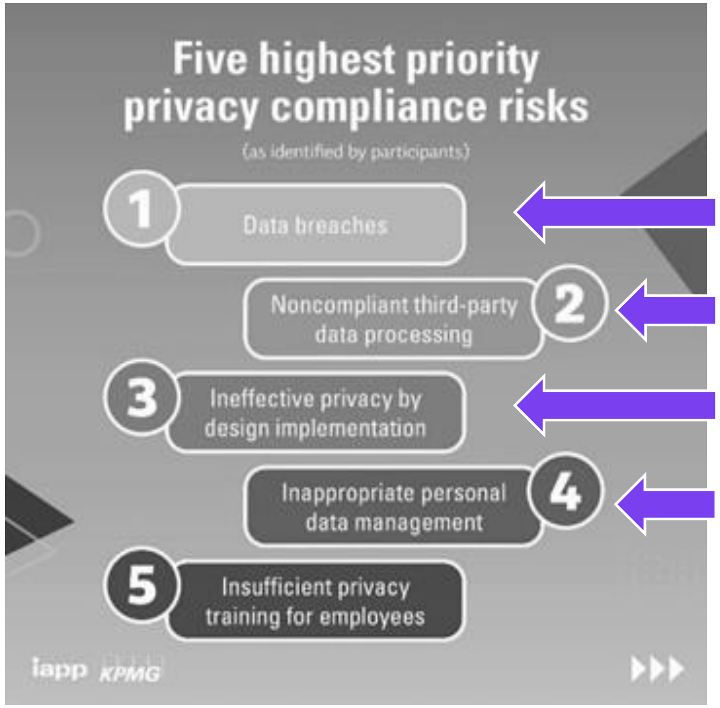


Source: KPMG Global Tech Report 2023

…And You Can't Do Privacy Without Data

iapp KPMG

PR!VACY R!SK STUDY 2023



Five highest priority privacy compliance risks

(as identified by participants)

1 Data breaches

2 Noncompliant third-party data processing

3 Ineffective privacy by design implementation

4 Inappropriate personal data management

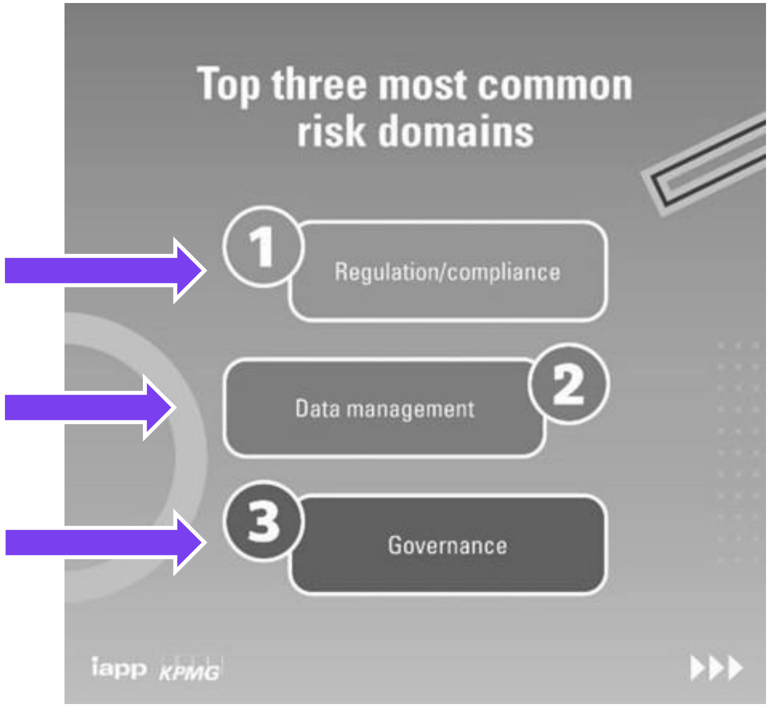
5 Insufficient privacy training for employees

iapp KPMG

✓ ✓ ✓ ✓

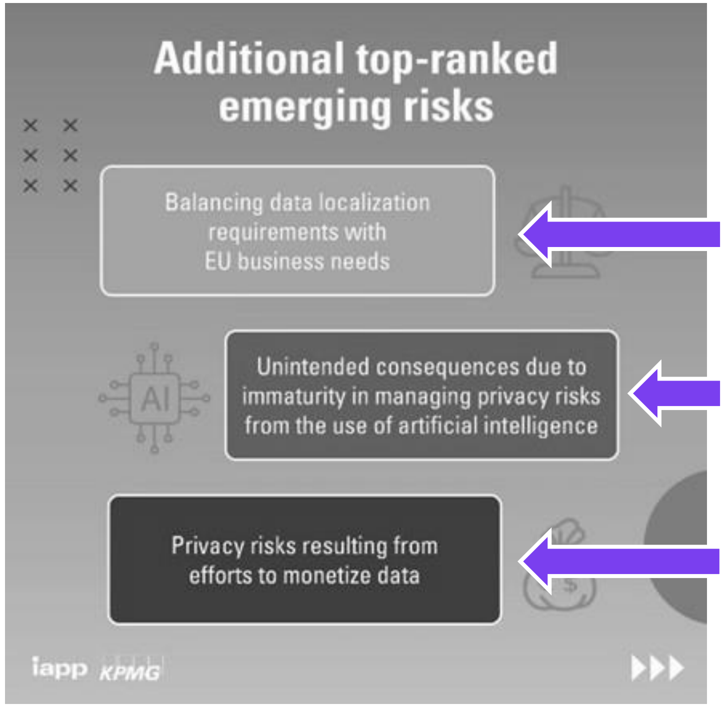
Data Mapping!

…And You Can’t Do Privacy Without Data



Top three most common risk domains

- ✓ 1 Regulation/compliance
- ✓ 2 Data management
- ✓ 3 Governance



Additional top-ranked emerging risks

- Balancing data localization requirements with EU business needs ✓
- Unintended consequences due to immaturity in managing privacy risks from the use of artificial intelligence ✓
- Privacy risks resulting from efforts to monetize data ✓

AI
iapp KPMG

Data Mapping!

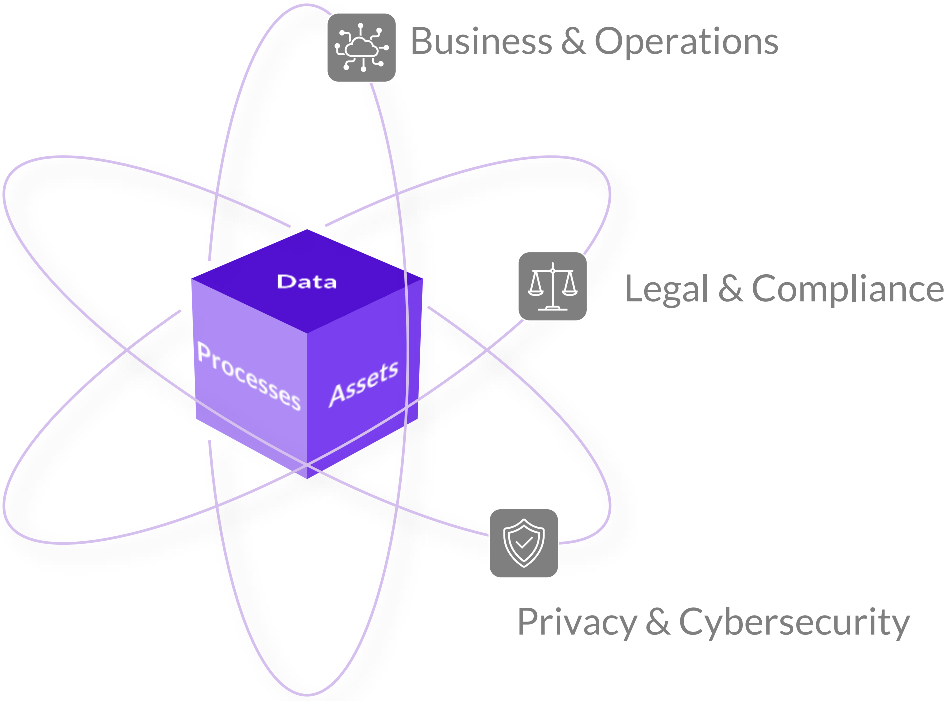
(Data Map)^3—Discover. Describe. Demystify.

A proper data map establishes the fundamental baseline of organizational transparency and satisfies the needs of the business & operations, risk & compliance, and privacy & cybersecurity stakeholders.

Data-Centric | Characteristics
Capture all descriptive attributes and information of your (personal) data.

Process-Centric | Use & Purpose
Explain the actual use of (personal) data down to an appropriate level of granularity.

Asset-Centric | Origin & Source
List the assets and their managing parties containing (personal) data and establish data provenance.



What A (Privacy) Data Map Could Look Like

Categories of PI

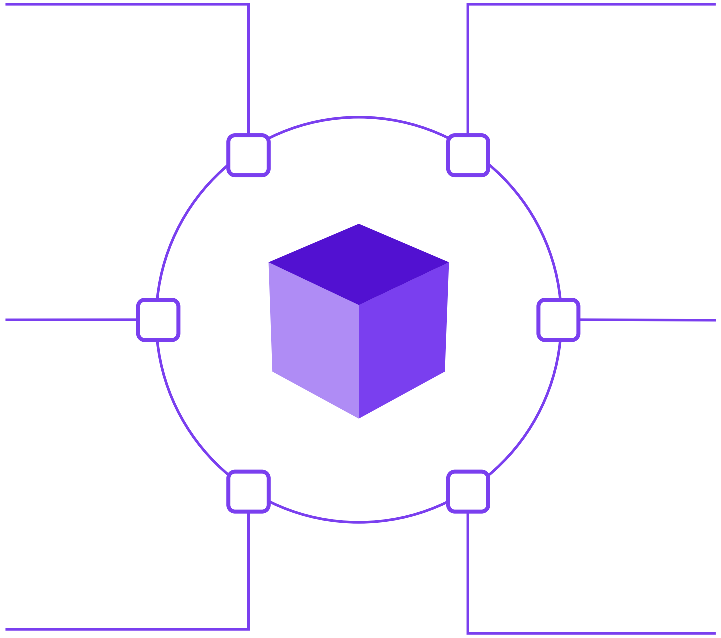
Inventory of personal information processed by the organization incl. categories showing sensitivity and volume as basis for privacy risk

Inherent Risk Description

Initial inherent risk register of threshold questions triggering privacy impact assessments

Third Parties

Data map showing exchanges, flows, and residency of personal information



Purpose & Use

Transparency regarding collection, purpose, and use of personal information established for confirming appropriate lawful processing

Ownership & Stewardship

Accountability for personal information handling and lifecycle management

IT Assets

Register of IT assets handling personal information
and their safeguards

What Do You Need To Consider Specifically?

Categories of PI

- Discover both *structured* and *unstructured* data.
- Identify certain types of sensitive personal information, e.g. financial information, health information, government ID information (e.g. citizenship, SIN, SSN, etc.), employment information, etc.

Inherent Risk

- Ability to apply an inherent risk assessment to categories of PI vs. systems/assets
- Identify and classify personal information according to a customers' data classification scheme
  - Ability to override exceptions to the data classification scheme
- Identify the volume of personal information retained in systems/assets

Third Parties

- Capture and manage the personal information that is collected, used, and retained by third parties
- Capture and manage the personal information that is disclosed to third parties

Purpose & Use

- Capture and manage considerations such as:
  - Provenance of the personal information, including whether it is collected directly or indirectly from the data subject—and the ability to map back to consent
  - Business processes that collect and/or use the personal information

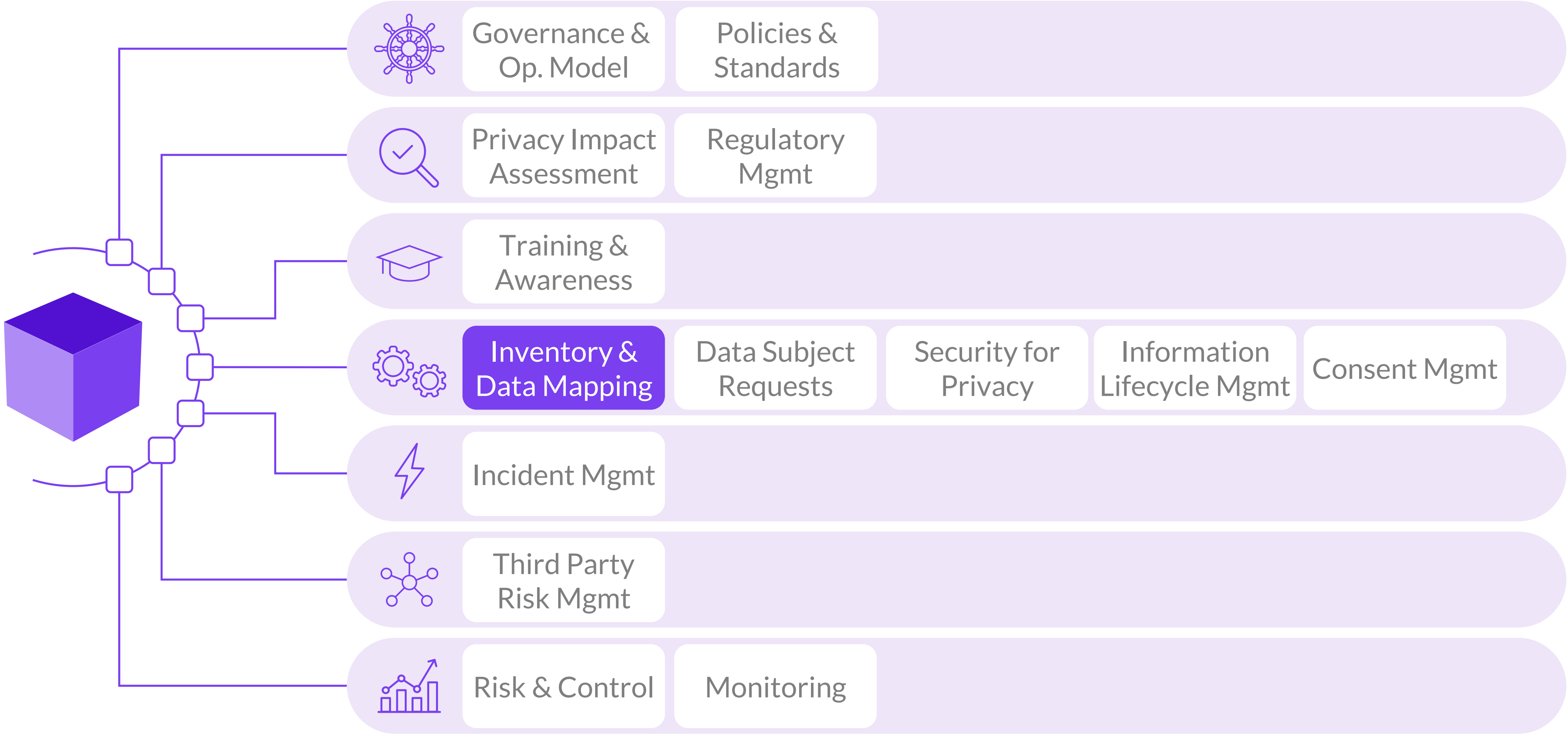
Ownership

- Capture and manage key governance considerations such as:
  - System/asset ownership (incl. **non-IT assets**)
  - Data stewardship
  - Evergreen maintenance and updates to the PI inventory and data maps (scheduled/routine updates, triggers)

IT Assets

- Capture systems that contain personal information (including routine verification scans for updates)
- Trigger notices or warnings changes to the scope of PI used, or other systems accessing the PI

The Engine Of Your Privacy Program



Governance & Op. Model

Policies & Standards

Privacy Impact Assessment

Regulatory Mgmt

Training & Awareness

Inventory & Data Mapping

Data Subject Requests

Security for Privacy

Information Lifecycle Mgmt

Consent Mgmt

Incident Mgmt

Third Party Risk Mgmt

Risk & Control

Monitoring

Osano Insights

Operationalizing Your Data Map

- How to generate a data map
- Associated challenges and solutions
- Putting your data map into action

Challenges

Who Does the Data Mapping?

- Do you have a dedicated privacy professional on staff?
- Can your privacy professional map your data using the chosen approach?
- What priority is data mapping for the responsible person?
- Does your privacy professional have the skillsets?

Discovering What You Don't Know

- No matter what, some personal data stores and flows will not be discoverable.
- With a fully manual approach, you'll need to manually discover even integrated data stores.
- Data mapping tools can automatically discover data stores integrated with your SSO provider BUT unconnected data stores will remain.
- Determining scope.

Bandwidth

- Data mapping requires, at minimum, time and attention that could be spent elsewhere.
- How do you prioritize?

Maintaining Your Data Map

- Data mapping should not be one-and-done exercise.
- Operationalizing maintenance to sustain your data map requires buy-in.

How to Generate Your Data Map

Broadly, there are three approaches to generating a data map:

Fully Manual

+

- Cheap
- Easy to get started immediately
- Reveals requirements, challenges, etc.

−

- Point in time—hard to sustain
- Not scalable
- Labor intensive
- Lacks automation

Homegrown

+

- Customizable
- Can be automated
- Utilizes your existing techstack

−

- Labor intensive
- Often lacks privacy-specific focus
- Takes the most time to get started
- Can be bottlenecked by internal resources

With a Dedicated Privacy Tool

+

- Automated and robust
- Specific to privacy
- Supports scale + sustainability
- Integrates with other solutions
- Empowers privacy but leaves systems of record undisturbed

−

- Higher upfront cost and implementation time

How to Generate Your Data Map

	Fully Manual	Homegrown	With a Dedicated Tool
Level of Effort	- High	- High	- Low to medium, depending on selected tool.
Level of Risk	- High	- Medium	- Low to medium, depending on selected tool.
Steps Involved	- Taking inventory of data trackers from both internal stakeholders and external vendors. - Interviewing data store owners. - Cataloging findings in spreadsheet. - Using a visual collaboation tool	- Combining a variety of business tools; e.g., Power BI, eDiscovery software, Tableau, etc. - Collaboration with data scientists/analysts. - Follow-up interviews driven by privacy pro to ensure full coverage.	- Evaluating and implementing the right data privacy platform or privacy-focused mapping tool. - Integrating with desired systems (e.g. ServiceNow)
When to Use	- Can be a useful one-time exercise to understand requirements—otherwise, this process is too static and/or time-consuming.	- Useful when there are highly specific, niche requirements that necessitate a custom solution. - Compliance needs are minimal OR data privacy takes priority over other initiatives.	- At any stage—typically strikes a balance between ease of implementation, compliance readiness, repeatability, scalability, etc.

How to Use Your Data Map

Response Readiness

- **Cyber readiness:** Identify data pathways to detect potential data sharing, system connections, data classifications in repos etc.
- **Notification readiness:** Evaluate scope of any breach to support notifications

Visualize Risk

- **TPRM:** Evaluate whether and how much data you send to untrustworthy third parties, or those with a reputation that does not align to your goals.
- **See, not say:** By having a visual representation of risk, it is easier to remove emotion and discuss objective risks.

Facilitate Downstream Compliance

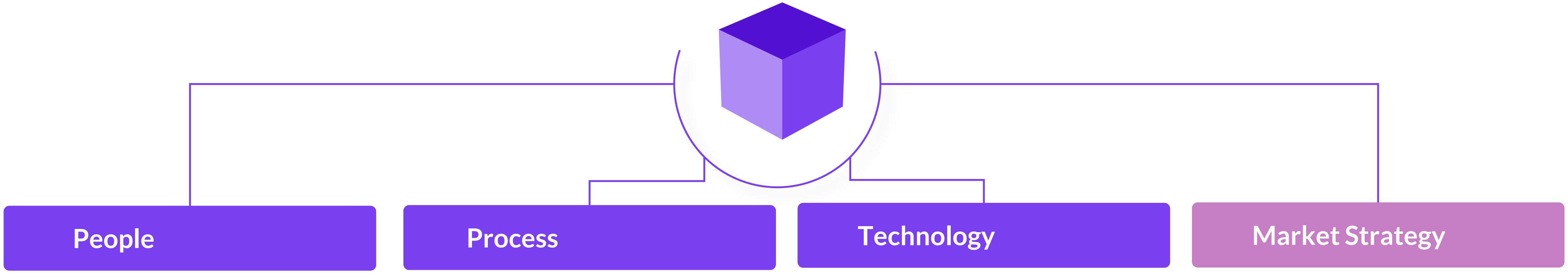
- **Support operationalization:** Data maps aren’t required by regulation, but they make compliance easier.
- **Move quickly:** Execute on DSARs, DPAs faster
- **Proactively identify risks:** Sensitive data stores and apply required protections
- **Streamline assessment:** PIAs, RoPAs, vendor surveys, and more.

Digital Optimization

- **Mange costs:** Identify duplicative vendors, contracts, and processes.
- **Minimize data:** Detect no-longer-needed repos/siloes.
- **Streamline workflow:** Enhance efficiencies that enable digital transformation.
- **Gain awareness:** Manage critical data resources—help support resilience and recovery planning.

Data Mapping Across Domains

Generating a data map has an impact on:



People

- Insight into who needs what data
- Understand who needs to be protected
- Stronger protections for customers and clients

Process

- Understanding of compliance needs for both data privacy regs (e.g., GDPR, CPRA) and other corporate regs (e.g., AI Act, DMA, GLBA)
- Improved ability to execute on compliance tasks (e.g., DSARs, sensitive information protection)
- Better data governance
- Understand where there is heightened risk

Technology

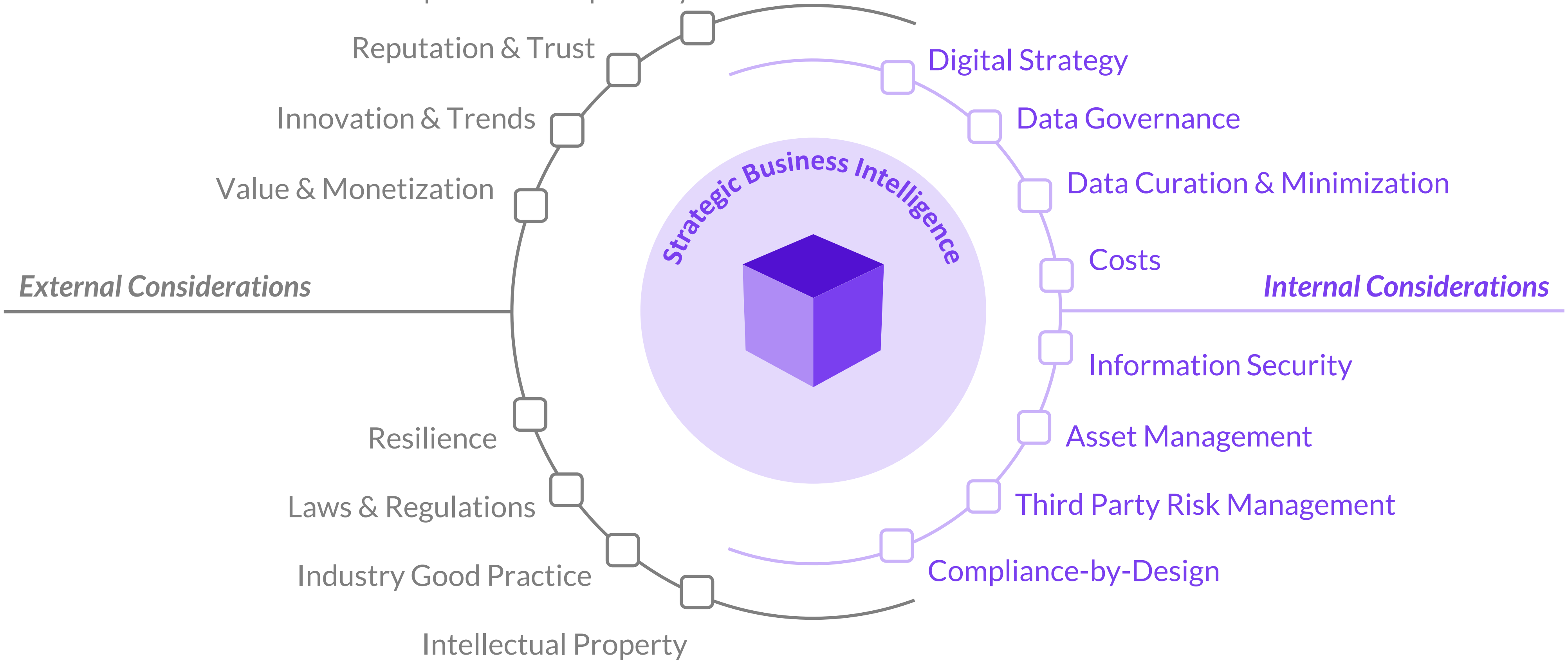
- Understanding of where data flows
- Insight into whether systems are drawing on appropriate and necessary data, including AI systems.
- Identification of duplicative or unnecessary systems

Market Strategy

- The ability to assess whether or not data flows are necessary, prohibitively costly, or prohibitively risky
- Help you gain trust internally and externally—the more you know, the more transparent you can be.
- Can tie to other company goals (ESG, DEI)

The Big Picture:
The Value of Data Mapping

It Helps You Navigate The Entire Risk Landscape



External Considerations

Purpose & Transparency

Reputation & Trust

Innovation & Trends

Value & Monetization

Resilience

Laws & Regulations

Industry Good Practice

Intellectual Property

Strategic Business Intelligence

Internal Considerations

Digital Strategy

Data Governance

Data Curation & Minimization

Costs

Information Security

Asset Management

Third Party Risk Management

Compliance-by-Design

Stay In Touch and Learn More!

Oskar Trpisovsky

Rachael Ormiston

Osano Blog: Data Mapping 101

Q&A

Ask your most pressing data mapping questions.

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iapp.questionpro.com/t/AOhP6Z1FP6

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.

For questions on this or other
IAPP Web Conferences or recordings
or to obtain a copy of the slide presentation please
contact:

livewebconteam@iapp.org

Thank You!