osano

Certified B Corporation

AICPA SOC

Certified CMP Partner

Users Love Us

Leader WINTER 2025

iapp

Privacy for risk management

Bridge the business, technology & compliance gaps

Wednesday, 18 June
07:00–08:00 PST
10:00–11:00 EST
16:00–17:00 CET

Meet Your Hosts

Ashley Slavik

Chief Privacy &
Information GRC Officer

ADM

Skye McCullough

Chief Customer Officer

osano

Agenda

- What Makes Privacy So Challenging to Prioritize
- Shifting Perspectives on Privacy
- Privacy's Not an Appendix
- Actionable Steps to Take
- Q&A

osano

What Makes Privacy So Challenging to Prioritize

And Why It's Worth Doing Anyways

Poll

What is your biggest challenge when it comes to managing privacy risk?

01 Keeping up with and interpreting privacy law and enforcement

02 Translating regulatory knowledge into privacy operations

03 Delegating privacy operations with confidence

04 Proficiency with a large tech stack and/or interoperability

05 Giving enough attention to privacy when there are other priorities

06 Coordinating across siloed teams

07 All of the above

osano

What GRC & Risk Pros Are Struggling With

Challenges Abound

GRC & Risk professionals are struggling with all of the challenges we identified in the poll to some degree.

Top 3 most commonly reported challenges blocking privacy compliance

(IAPP Privacy Governance Report 2024)

What We've Seen

? Fragmentation in ownership

🖇️ Missing connective tissue

🚨 Privacy and security are perceived as important but only become urgent AFTER something breaks

👶 Privacy is treated as the younger sibling of security

Privacy Is Tough to Prioritize, But It's Worth It

Data Breaches

Poor data privacy practices increase risks associated with data breaches:

- Poor data minimization and retention practices = bigger scope
- The more data involved in a breach, the more ammo malicious actors have
- Regulators may investigate and apply follow-on penalties if a breach was related to poor data privacy practices
- Privacy practices generate the paper trail that enables you to prove what happened

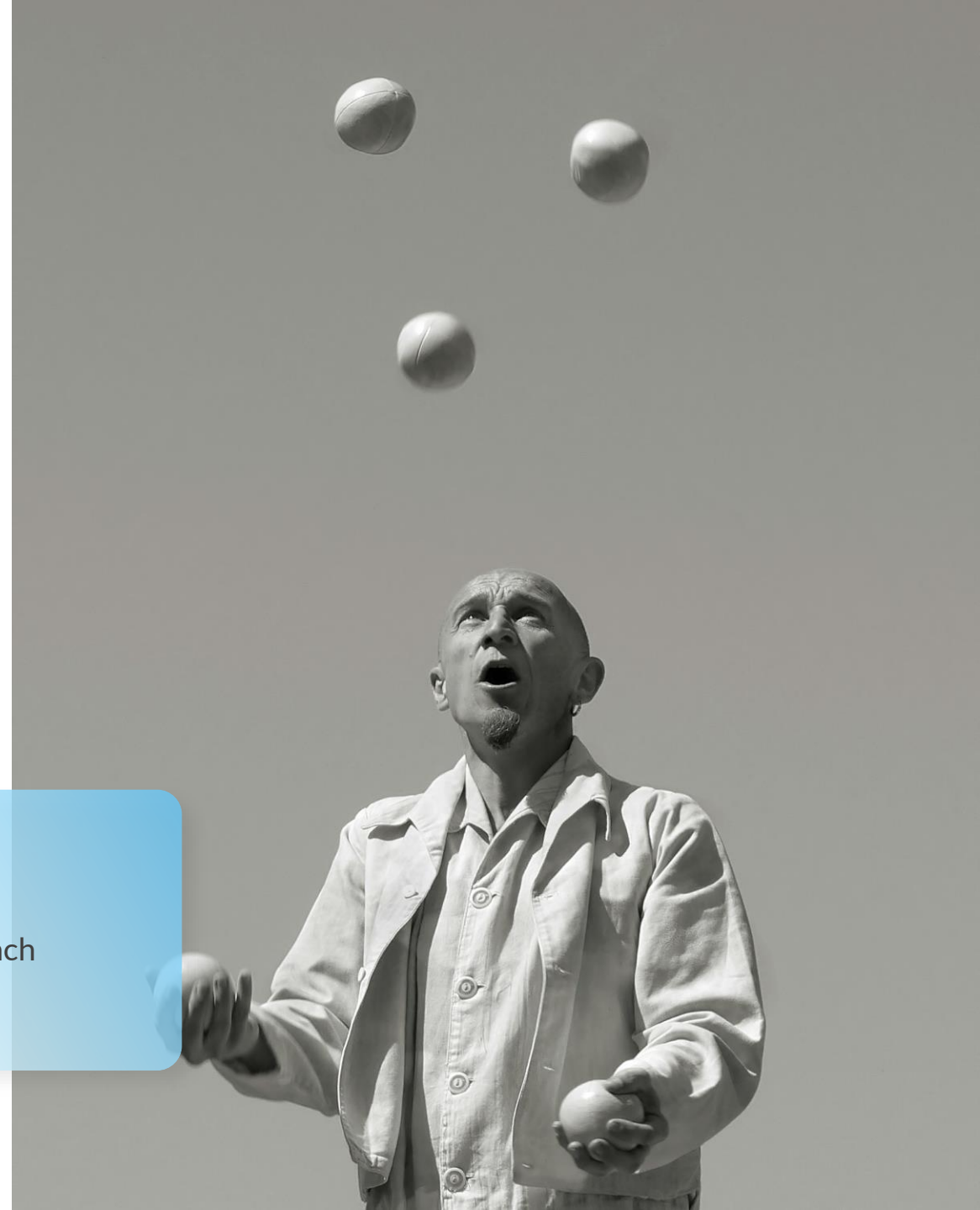
1 out of 3

Organizations that suffered a data breach also had to pay fines*

$4.88 M

Average cost of a data breach in 2025*

*IBM, Cost of a Data Breach Report, 2024



Privacy Is Tough to Prioritize, But It's Worth It

Downstream Risk Management

Managing privacy risk is foundational—it bleeds into more targeted downstream risk sources.

AI is a great example of how privacy practices can reduce further risk.

- If you develop an AI system, do you have appropriate legal basis for training data?
- If you use AI systems, have you evaluated your vendors' privacy practices? Have you conducted a PIA or DPIA to determine risks posed to users?
- If you use AI for automated decision-making, are you managing consent and subject rights appropriately for different data privacy laws?

Privacy Is Tough to Prioritize, But It's Worth It

Market Expectations

Privacy is becoming table stakes

- Cyberinsurers look for privacy risk management
- Business partners, M&A partners, etc. look for privacy risk management in due diligence or as part of ISO 27001 and SOC 2.
- Customers expect it too and will take their business elsewhere.

"We are seeing more data privacy breach claims in the U.S. where there is a growing trend for class action litigation against large U.S. and international corporations related to privacy violations, such as around consent and data usage,"

— Business insurer Allianz Commercial in their Cyber Risk Trends 2024 Report

85%

of customers say that they will not do business with a company if they are worried about its data practices.

PWC, Protect.me report

osano

Shifting Perspectives

Building the Bridge Between Business, Technology, and Compliance

Change the Organization’s Perspective on Privacy

More Than a Legal Obligation

Privacy is a strategic risk category tied to reputation, operational resilience, and trust.

Reframe GRC

Reframe GRC (including privacy and AI) as a trust and brand enabler to differentiate your organization, increase efficiency, and drive innovation.

Embed Privacy Into Existing Processes

Embedding privacy into risk registers, incident response, and audits helps unify legal and business accountability.

Tailor the Message

Tailor Your Message to Ensure Buy-in and Adherence

Create a shared language across functions

alignment instead of silos:

- Business/Marketing hears improved customer experience and responsible data use.
- IT/Security hears strengthened controls, architecture, and incident response.
- Compliance hears pragmatic policies in line with legal requirements and best practices.

Make Time for Training and Education

- Privacy can’t happen in a vacuum
- Support your training and education efforts with solutions with built-in guardrails.
- Compliance software that puts the onus on you to research compliance best practices is a red flag.

osano

Privacy’s Not an Appendix

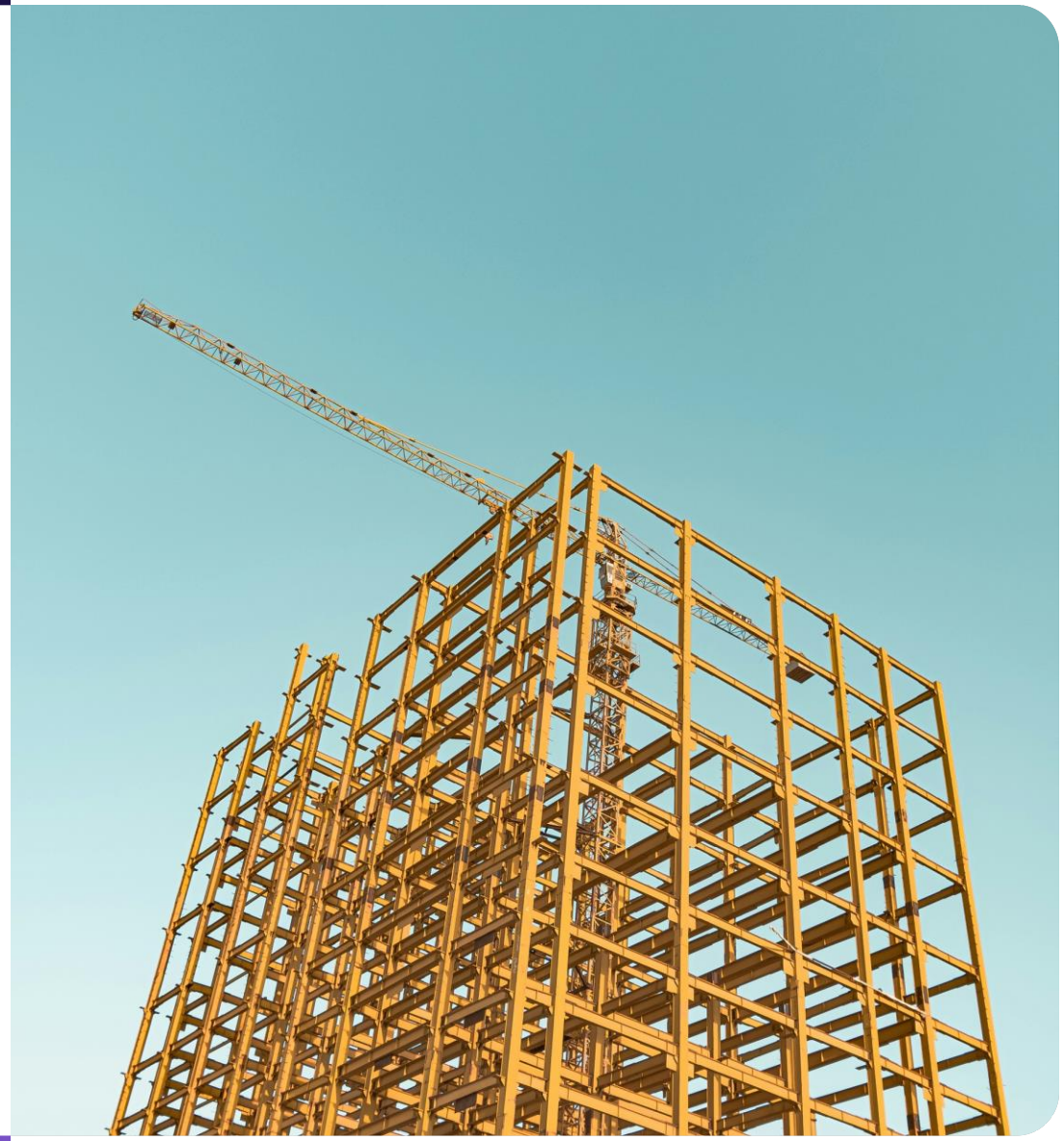
Integrating Privacy in Your Processes

Integrate Privacy into GRC/Risk Frameworks

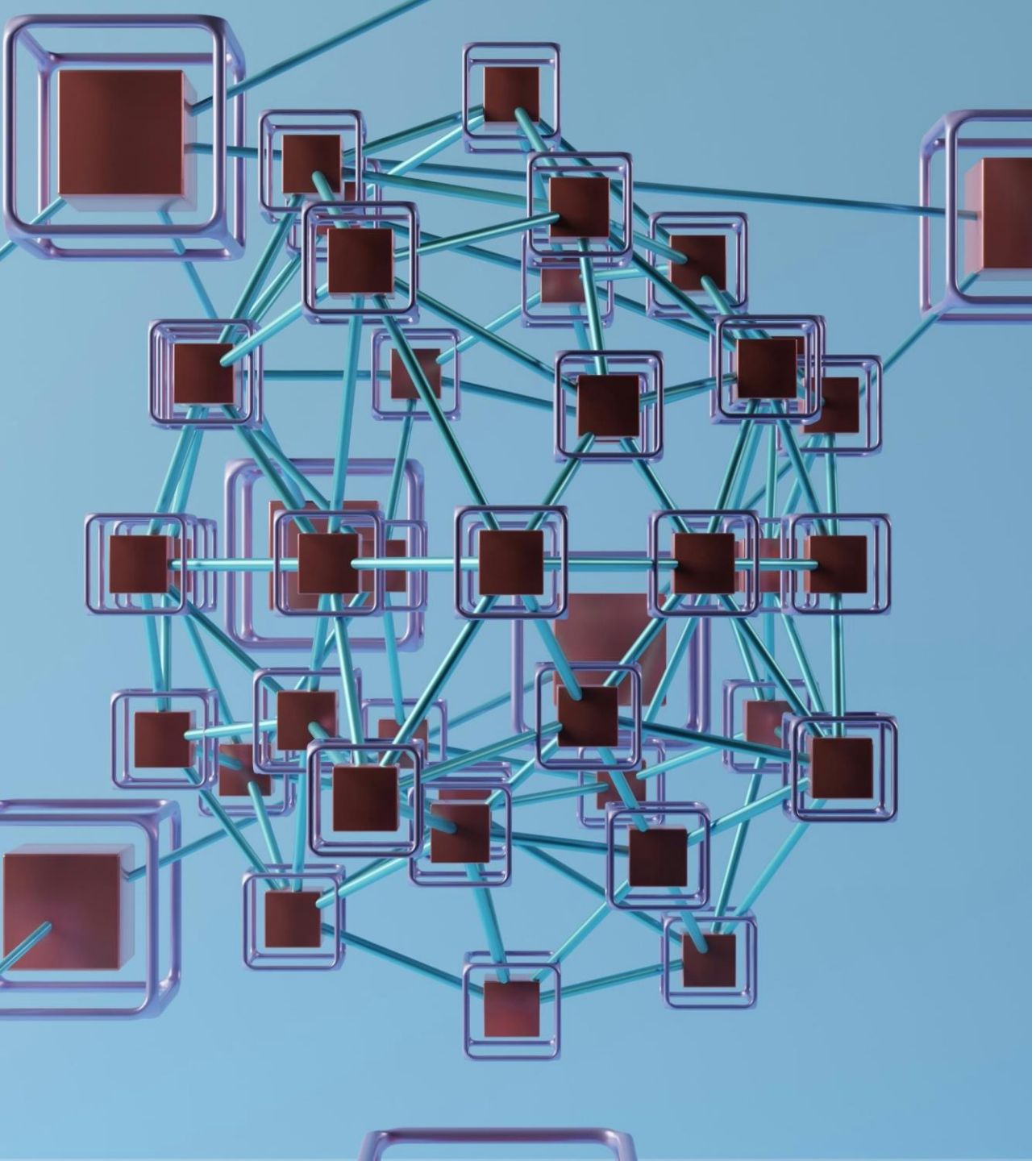
- Unmapped data flows leads to risk of unauthorized access.
- Shadow IT means risk of unmonitored data transfers
- Lack of vendor oversight exposes company data

Connect enterprise risk appetite and privacy controls across the data lifecycle. Build processes for:

- Data transfers
- Data Protection Impact Assessments (DPIAs)
- Data mapping as risk tools within existing frameworks



osano



Metrics, Metrics, Metrics

If you don't measure it, it doesn't exist.

- Define KPIs that reflect privacy maturity and risk posture, such as:
  - % of systems with valid data maps
  - Time to fulfill data subject requests
  - Number of vendors with current privacy terms
- Use these metrics in risk dashboards and quarterly reviews to shift from reactive to proactive privacy management.
- Risk-based frameworks help prioritize where to focus in a global organization
  - E.g. privacy and info sec heat maps

osano

Actionable Steps to Take

What to Prioritize in Privacy Management

What Recent Enforcement Is Telling Us

- Enforcement in the US is ramping up
  - 5 CCPA actions (+ investigative sweep of location data industry)
  - 1 TDPSA action
- You need to have some regular review of regulatory authorities' guidance
  - e.g. the Honda enforcement under the CCPA
  - Osano can help with this via our regulatory guidance and privacy team consultation.
- Regulators aren't auditing companies at random; they start with externally facing privacy mechanisms.
- Prioritize:
  - Consent management
  - Subject rights workflows
  - Policy management
- Data mapping and assessments matter too
  - Identify additional risk sources (privacy and otherwise)
  - A second target after major external-facing mechanisms

Evaluation Is Key

Don’t cut corners when evaluating solutions. The right solution can be a game-changer; the wrong solution just shuffles work around.

Red Flags

- **Few integrations OR 1,000s**—Does it integrate with the tools you actually use? How much maintenance will it require? Have you integrated your way into increased risk?
- **Complicated implementations**—Is there a community of 3rd-party consultants solely there to get you up and running?
- **Ultra flexible**—Some specific organizations will want to be able to do anything and everything with their solutions; most will want a solution that prevents accidental non-compliance.

Green Flags

- **Easy to implement & maintain**—a solution is only as useful as it is usable
- **Designed and maintained by privacy experts**—If you’re expected to research and operationalize current best practices, your solution won’t save you much time
- **Designed for all levels of expertise**—You’ll want to be able to delegate compliance tasks without worrying over non-compliant execution

Q&A

Schedule a Demo

osano

Thank You!

osano

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/ACtQeZ6Mnf

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