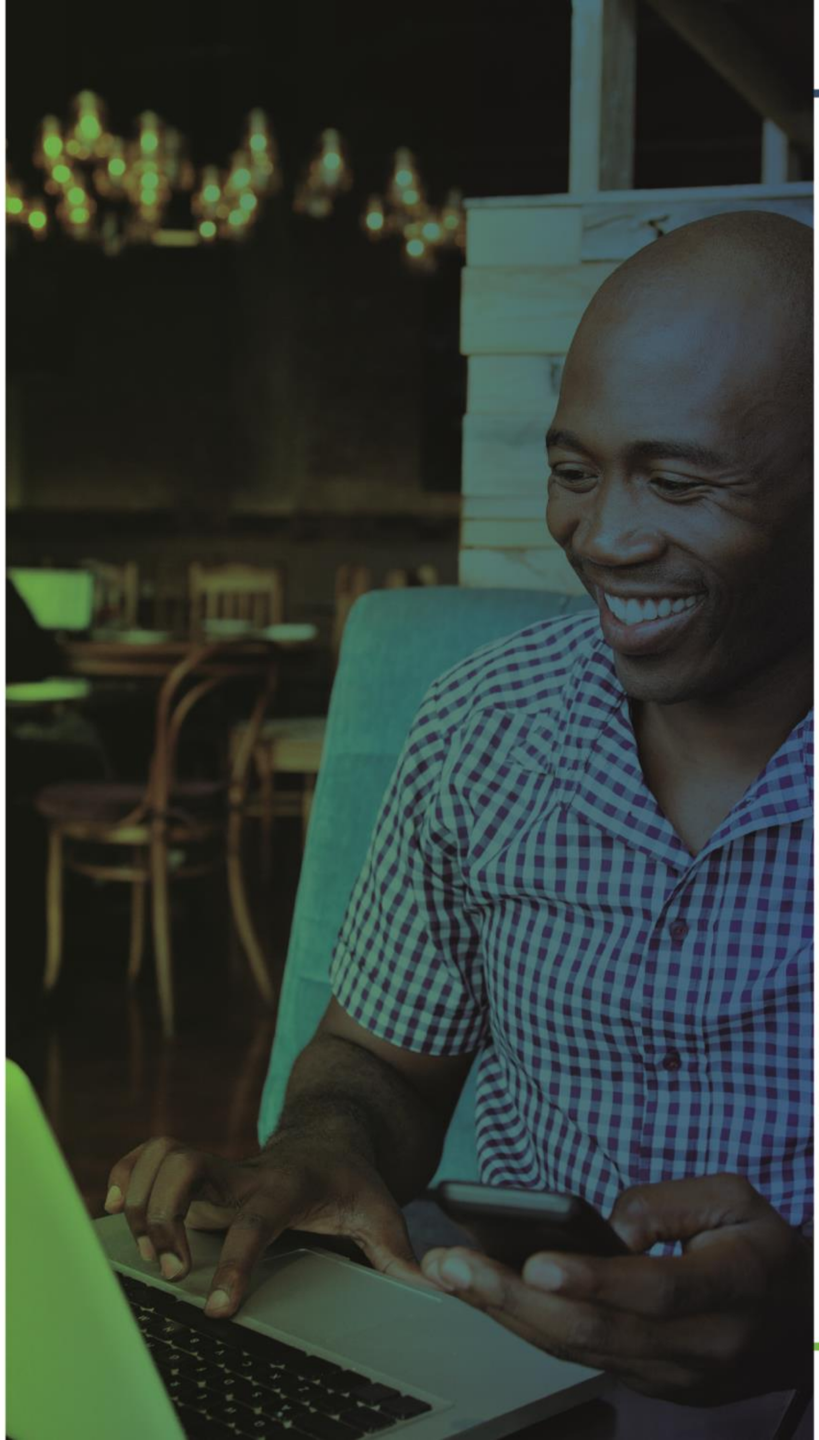
osano



iapp

Why Privacy Is Your Secret Weapon Against Third-Party Risk

Tuesday, 8 October
10:00-11:00 PST
13:00-14:00 EST
19:00-20:00 CET

Meet Your Hosts

Rachael Ormiston

Head of Privacy

Osano

Nicole Howard

Sr. Product Manager

Osano

Today's Agenda

- **Poll**
- **Defining TPRM**
- **Why TPRM Feels Like a Hydra and How Data Privacy Can Be Your Secret Weapon**
- **Practical Tips for Data Privacy-Driven TPRM**
- **How Osano Can Help**
- **Q&A**

Poll

Who owns third-party risk management at your organization?

01 Nobody

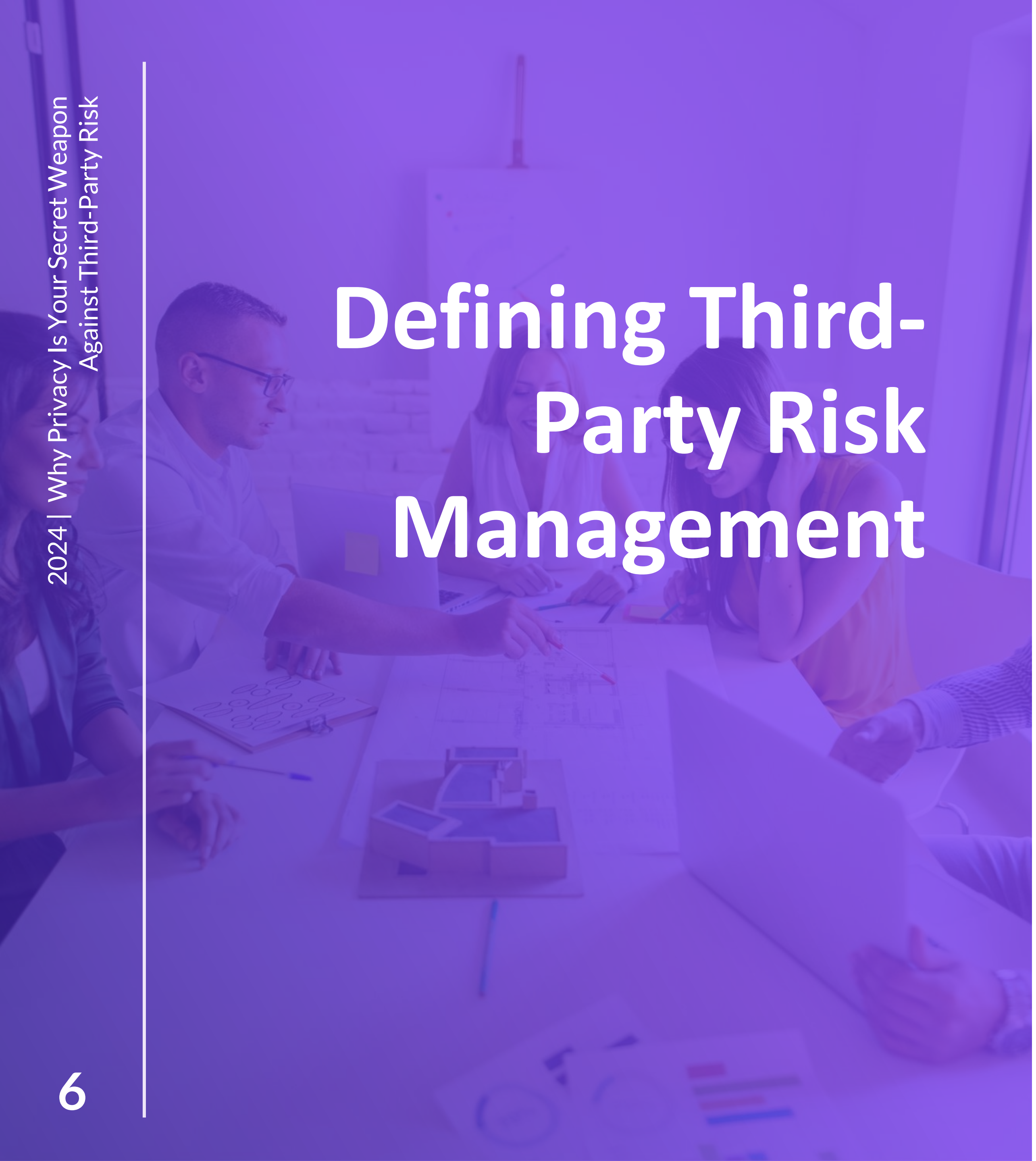
02 Our GRC team

03 Our cybersecurity team

04 Our legal department

05 Our privacy and compliance team

06 A team that handles two or more of these functions



Defining Third-Party Risk Management

- **TPRM:** The practice of identifying, mitigating, and tracking the risks that come from the third parties with whom you do business.
- Modern businesses cannot succeed without relying on external partners.

16

Small businesses maintain 16 3rd-party relationships on average.

170+

Large enterprises maintain over 170 3rd-party relationships on average.

Source: Auditboard, 2023

- You can't dictate third party's operations; you can manage the risk they present.
- There is no universally accepted set of TPRM best practices.

Mitigate One Risk Factor, and Two More Appear

Fighting the Hydra of TPRM

Third-party risk appears in multiple vectors:

Compliance Risk

- E.g.: How does this new third-party relationship impact your ability to comply with regulations?

Operational Risk

- E.g.: If this third party suffers a breach, will it impact my ability to do business?

Cybersecurity Risk

- E.g.: Does this third party integrate with my systems and do they have adequate security?

Reputational Risk

- E.g.: Is this third party conducting business ethically and if not, how does their behavior reflect on me?

Fighting the Hydra of TPRM

How do you prioritize these risks?

Some organizations will prioritize based on:

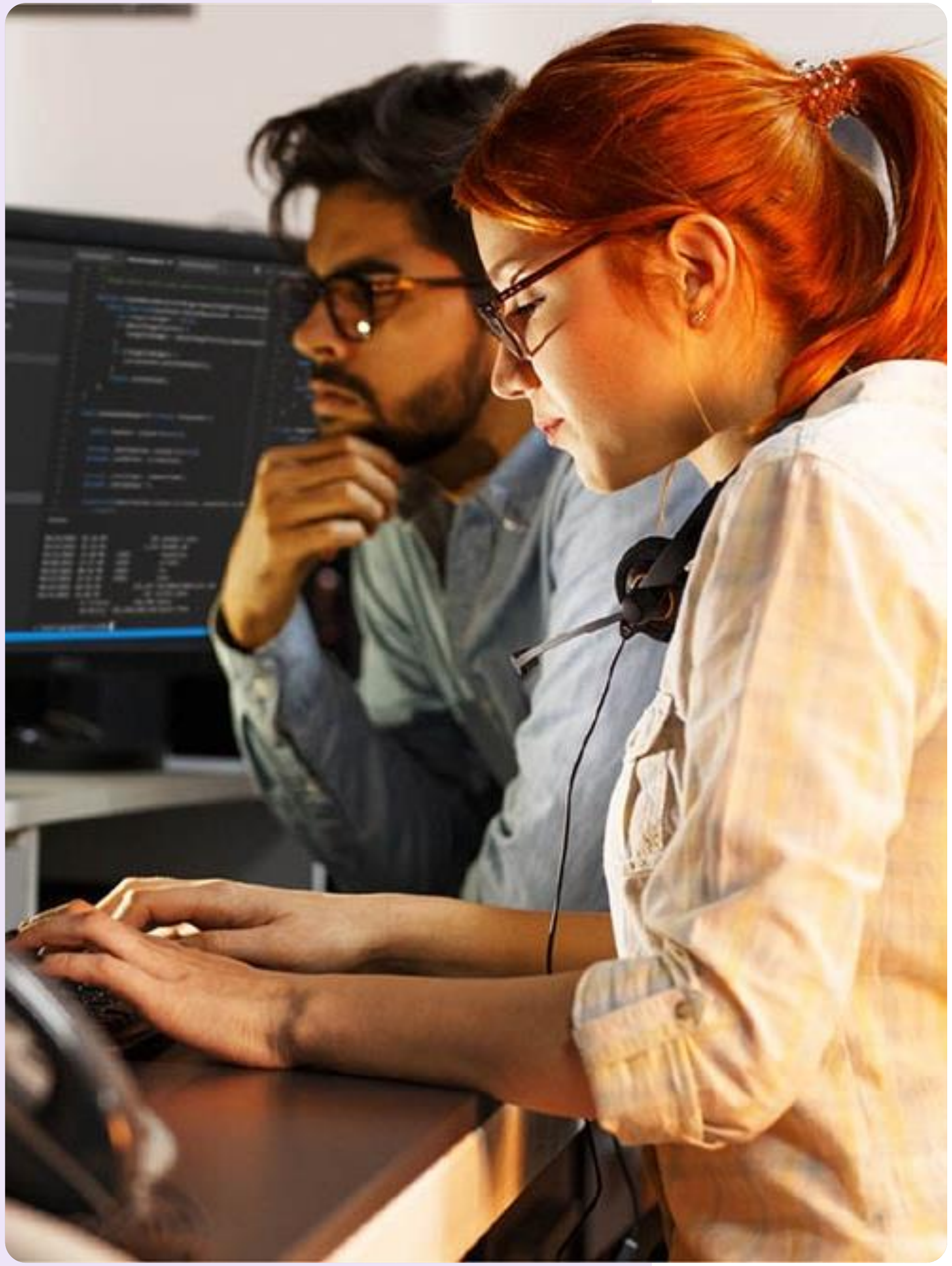
- Regulatory scrutiny
- Whether their services are need-to- or nice-to-have
- Sensitive data processing
- History of breaches

But most will have a blend of priorities or may see them all as equally urgent.

Is it even possible to mitigate them all?

- Risk mitigation is an ongoing activity that's invisible to the organization when done well.
- At the same time, it's difficult to know when you're effectively managing third-party risk—success can be invisible to you, too.
- ~70% of respondents are unsatisfied with their insight into risk across their third parties.

Source: Moody's Analytics, 2023



Data Privacy Can Be Your Secret Weapon

Data Privacy Is Pervasive in Third-Party Risk

- Data privacy impacts:
  - Compliance, through data privacy regulatory compliance and audit-readiness
  - Operations, through data minimization
  - Cybersecurity, through visibility into your data landscape
  - Reputation, by improving the customer experience
- If data privacy is to be found in TPRM no matter where you look, what are the implications for you?

Data Privacy's Implications for TPRM

What Does This Mean?

1. By focusing on data privacy management, you'll improve your TPRM as a byproduct.

2. Once you've developed strong data privacy practices, you'll have a stronger foundation to build broader TPRM practices.

Where Data Privacy and Third-Party Risk Intersect

AT&T

- $13M settlement over a 2023 breach impacting 8.9 million customers.
- AT&T was NOT the source of the breach; their vendor was.
- The exposed data was meant to have been deleted in 2017/2018, but this never occurred.

CrowdStrike

- Data privacy regs require data to be resilient and available—the CrowdStrike bug made data inaccessible
- Understanding requirements around data resiliency could have underscored CrowdStrike’s position as a critical vendor in need of additional scrutiny

Most VPPA Cases

- VPPA cases hinge on illegal transfers of consumer viewing data to third parties
- Understanding the fundamentals of data privacy regs, what constitutes a “sale” of data, and what constitutes consent could have enabled these defendants to dodge VPPA cases.

How Data Privacy Simplifies TPRM

It’s clear that data privacy plays a role in third-party risk; does it actually make TPRM easier?

- **Data minimization** reduces the impact of vendor breaches
- **Data mapping and discovery** uncovers duplicative and/or unnecessary vendor relationships
- **Insight** into what good looks like in vendor data privacy practices
- **Assessments** are required under data privacy law; they can jumpstart your vendor evaluations.

Don’t Reinvent the Wheel

Embed data privacy into your current processes; focus on evolution, not revolution.

Practical Tips for Data Privacy-Driven TPRM

01 Understand your privacy drivers

02 Map your data

03 Establish a vendor onboarding & evaluation process

04 Establish a vendor monitoring process

Privacy-Driven TPRM Tips

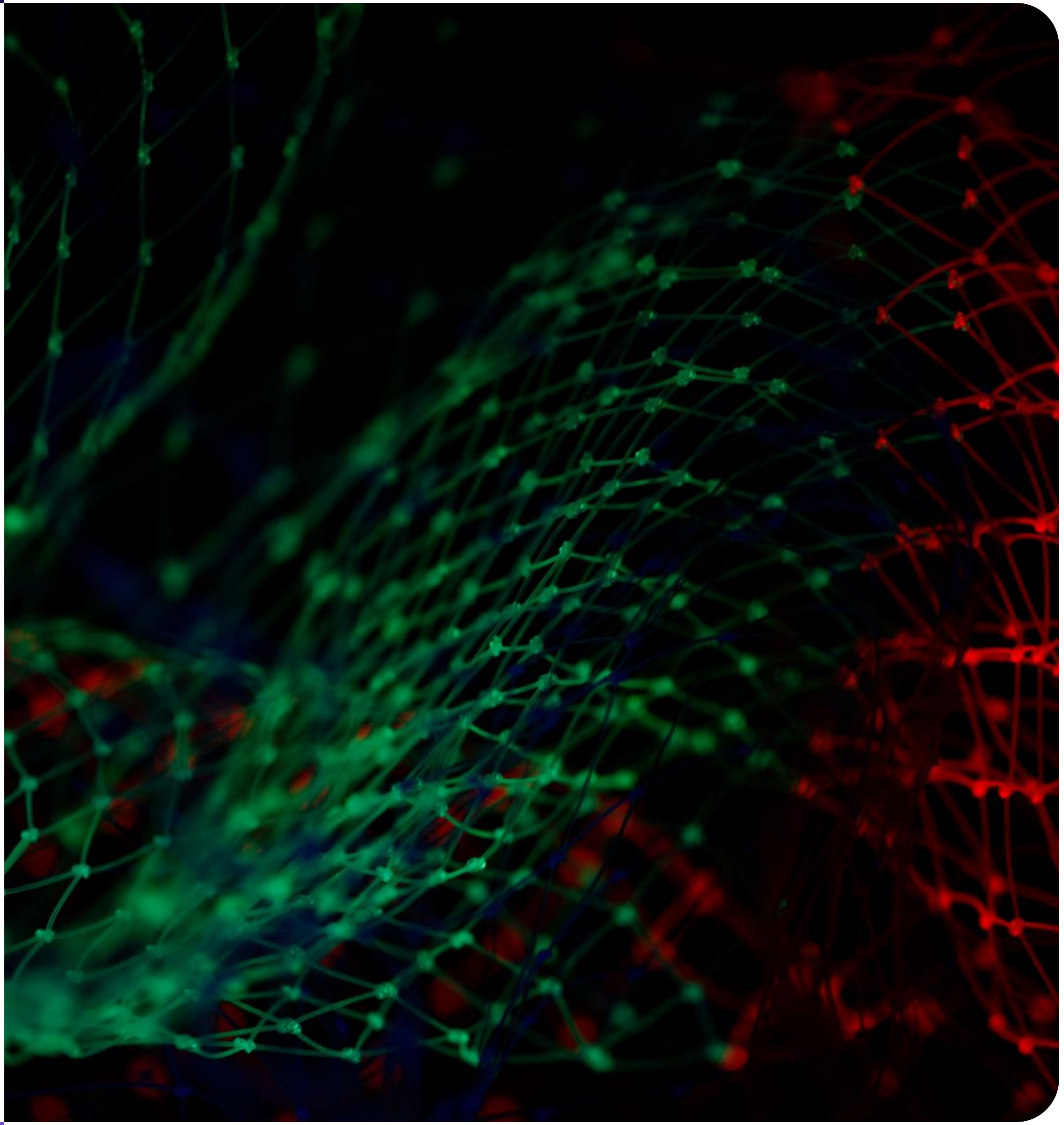
Understanding Privacy Drivers

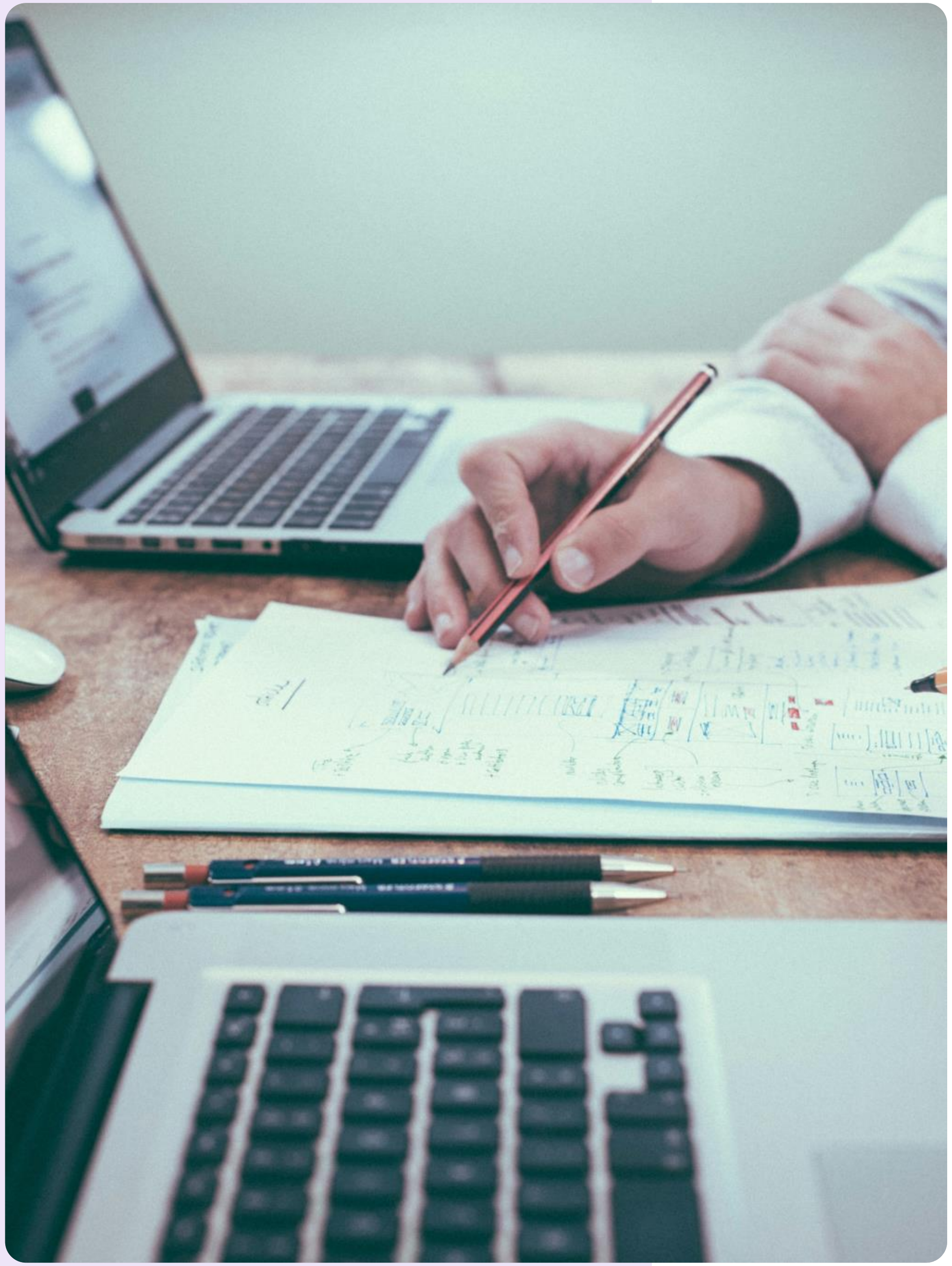
- What regulations are you subject to?
- What requirements or priorities are at play in your organization?
- When looking at privacy regulations, keep an eye out for language around:
  - Assessments (e.g. PIAs, DPIAs)
  - Contractual requirements (e.g. data privacy addendums, standard contractual clauses)
  - Data minimization
  - Subject rights requests
  - Vendor liability (are you on the hook for your vendors' noncompliance?)

Privacy-Driven TPRM Tips

Data Mapping

- Privacy-focused data mapping helps you understand the flow of data into, out of, and throughout your organization.
- Uncovers:
  - Duplicate or inactive vendors
  - Vendors who are due for assessment
  - Vendors who handle especially sensitive personal information
  - Vendors who receive more data than necessary
  - Parties that need to be notified of SRRs
  - Other unknown unknowns





Privacy-Driven TPRM Tips

Vendor Eval & Onboarding Process

- Privacy assessments can serve as the foundation for overall vendor risk evals.
    - Businesses with poor data privacy practices are twice as likely to suffer a breach; those with the worst practices are 80% more likely.
- Osano's database of vendor privacy scores can help you quickly develop a vendor shortlist (more on this later).

Privacy-Driven TPRM Tips

Vendor Monitoring

- Monitor your vendors:
  - Litigation
  - Privacy policy changes
  - Data breaches
- Conduct regular, ongoing assessments
- Important: Act on assessment results!
  - Connect with vendors who's privacy/security posture is slipping
  - Consider new vendors if necessary

How Osano Can Help

Putting Data Privacy & TPRM into Practice

How Osano Can Help

Operationalizing Data Maps

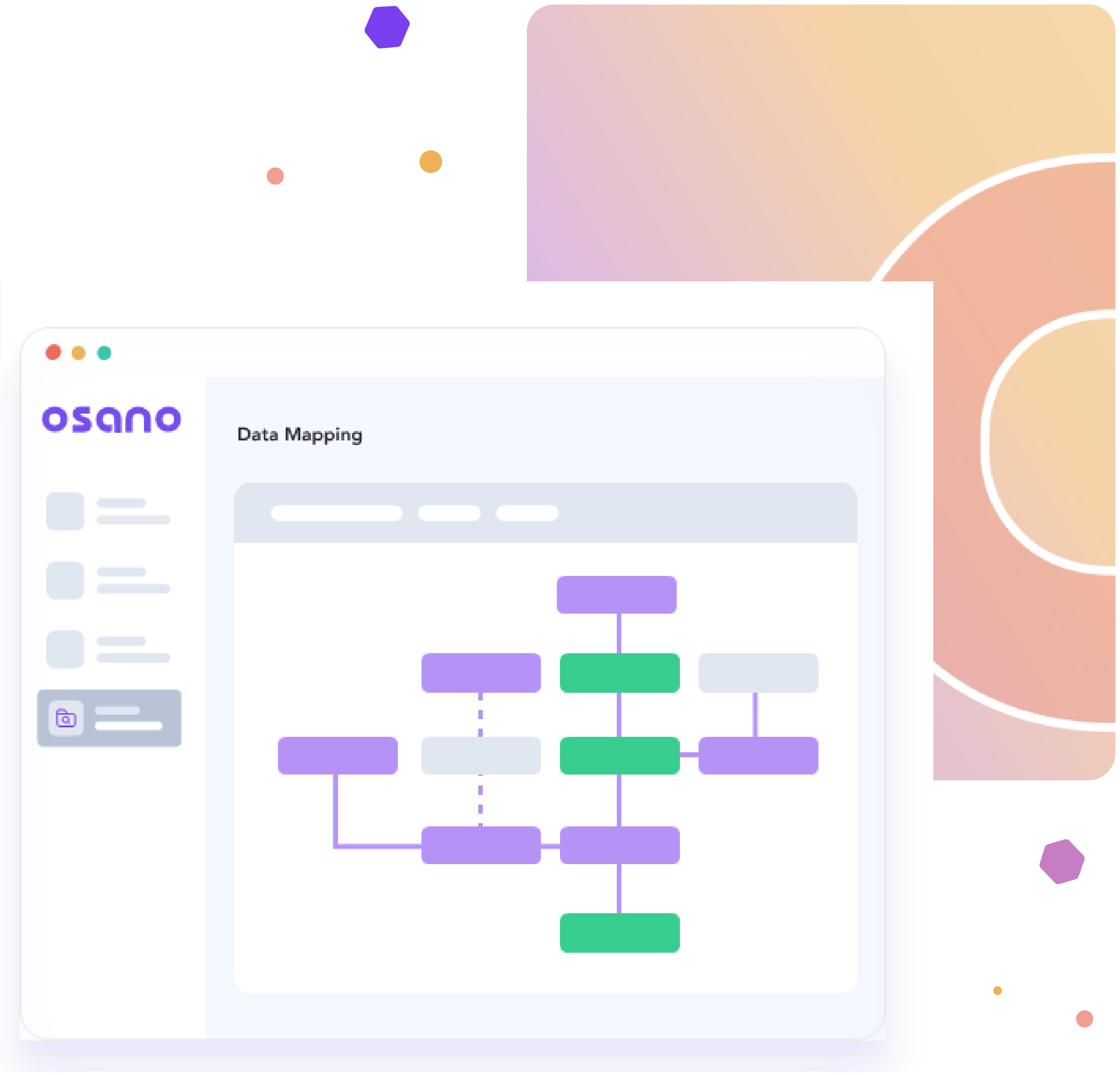
Avoid spreadsheets and non-privacy-focused data mapping solutions. Solutions like Osano:

Automatically Discover Data Stores

Osano integrates with “umbrella sources” to list out all connected systems and track data flows in an automated and refreshable manner.

Streamline Manual Workflows

Managed application discovery surveys discover and upload unintegrated, niche, or shadow IT systems into your data map



How Osano Can Help

Tracking Vendor Characteristics

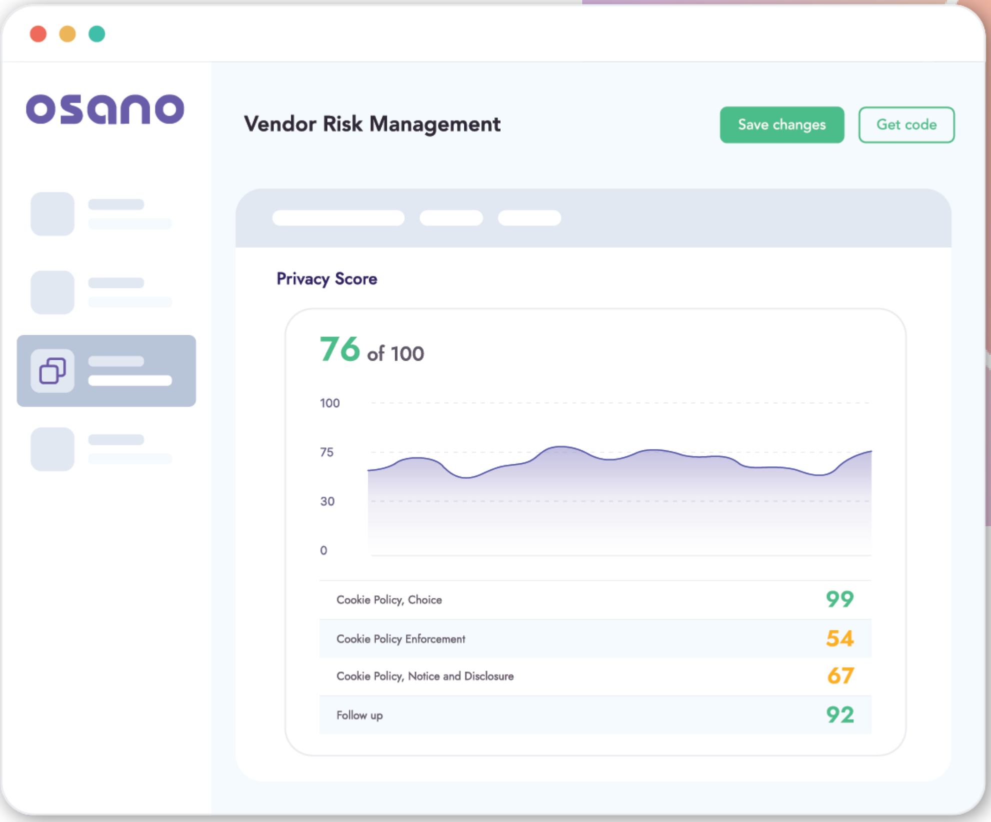
Vendor monitoring is a core task of TPRM; use a solution like Osano to automate it.

Over 14K Vendors

Scored on a 1-100 scale based on quantifiable data privacy practices.

Alerts You to Vendor Developments

Draws from multiple sources to alert you to privacy policy changes, lawsuits, and data breaches.



76 of 100

Cookie Policy, Choice	99
Cookie Policy Enforcement	54
Cookie Policy, Notice and Disclosure	67
Follow up	92

How Osano Can Help

Facilitate Assessments

Vendors can forget to complete assessments, you can forget to assign assessments on a regular cadence, and assessments can become lost.

Industry-Standard Templates

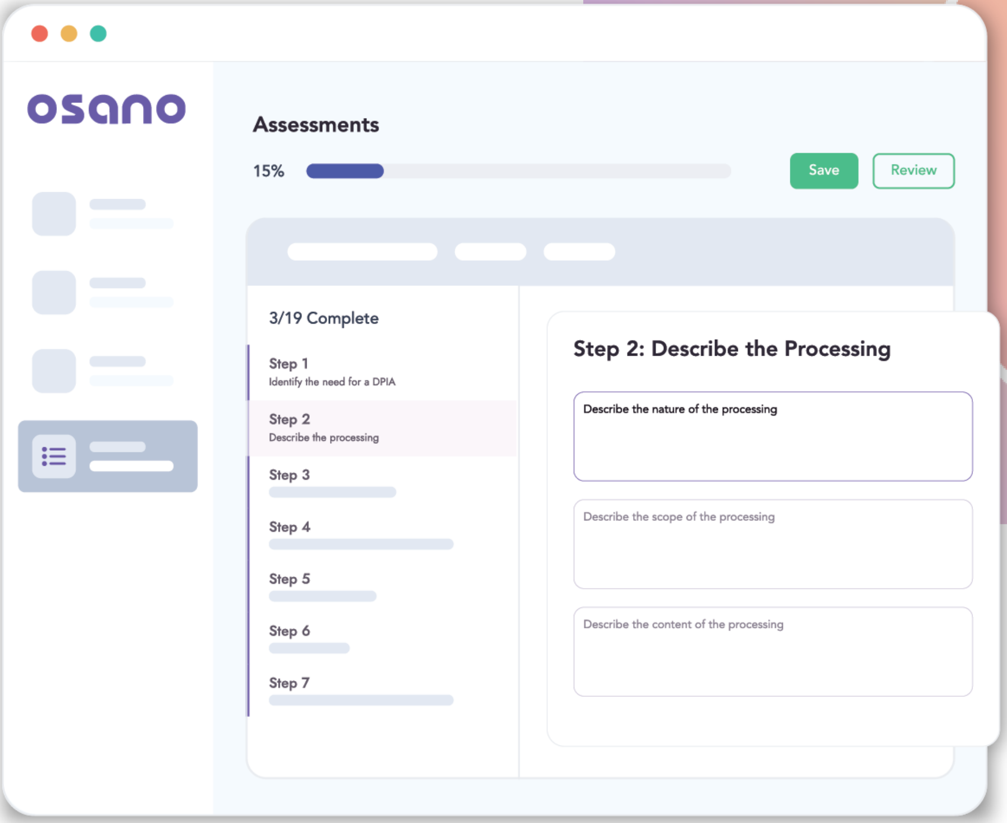
E.g., PIAs and vendor privacy assessments based on the NIST Privacy Framework

Custom Assessments

Incorporate risk evaluation criteria unique to your organization.

Workflow Management

Automatically distribute regular assessments and notify stakeholders of upcoming deadlines



Assessments

15%

3/19 Complete

Step 1
Identify the need for a DPIA

Step 2
Describe the processing

Step 3

Step 4

Step 5

Step 6

Step 7

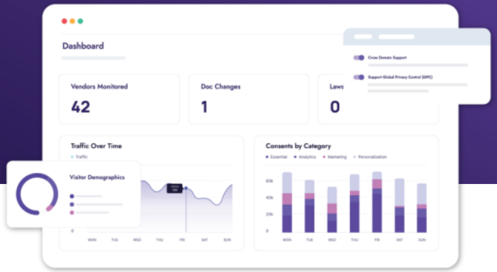
Step 2: Describe the Processing

Describe the nature of the processing

Describe the scope of the processing

Describe the content of the processing

Stay In Touch and Learn More!



Schedule a Demo

Check out the Osano Blog

Q&A

Ask your most pressing data privacy and TPRM 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/ACtQeZ37Rc

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!

osano