onetrust

From compliance to impact: Embedding privacy across the tech lifecycle

Welcomes and Introductions

Brett Tarr is a strategic legal executive with over 20 years of experience building high-impact privacy, AI governance, and information governance programs across Fortune 500s and fast-growing SaaS companies. He specializes in designing scalable systems that reduce risk and increase operational clarity, balancing regulatory and business needs while embedding privacy and ethical AI principles into complex organizations.

Brett has led programs achieving Binding Corporate Rules for Data Processors, delivered ISO 42001 certification for AI systems, and built enterprise-wide privacy and data governance programs for multi-billion-dollar companies.

Brett Tarr

Head of Privacy & AI Governance
OneTrust

From compliance to impact:
Embedding privacy across the tech lifecycle

01. Aligning AI Capabilities to Business Needs & GROWTH

02. Embedding Privacy Across Functions to Scale at the Rate of AI

03. Collaboration that Drives Operational Efficiency

04. Recap & Key Takeaways

Merging Disciplines to Create an Effective and Compliant Data Enablement Strategy

Technology

Advances in machine learning systems have allowed companies to automate and scale in ways never seen before.

Ownership

Across different operating models, Privacy is always at the table as a leading voice to ensure the responsible, ethical, and beneficial use of AI

Adoption

Common considerations driving privacy are even more present when dealing with and evaluating different AI systems.

Operations

Shifting ‘left’ to proactively work across business operations has been a consistent challenge for all risk and compliance teams

Embedding Privacy Across Business Operations to Scale at the Rate of AI

Embedding Privacy Across Functions

1	2	3	4	5
Establish Steering Committee	Identify Privacy Liaisons	Privacy Business Partner Program	Tailored Privacy Trainings	Establish New Product Lifecycle

Embedding Privacy Across Functions

1

Establish Steering Committee

- Risk leaders, Data leaders, and other key stakeholders
- Develop and articulate privacy strategy and policy to business stakeholders
- Discuss new technologies and business processes that may trigger privacy compliance or implications

2

Identify Privacy Liaisons

3

Privacy Business Partner Program

4

Tailored Privacy Trainings

5

Establish New Product Lifecycle

Embedding Privacy Across Functions

1	2	3	4	5
Establish Steering Committee	Identify Privacy Liaisons	Privacy Business Partner Program	Tailored Privacy Trainings	Establish New Product Lifecycle
▪ Risk leaders, Data leaders, and other key stakeholders ▪ Develop and articulate privacy strategy and policy to business stakeholders ▪ Discuss new technologies and business processes that may trigger privacy compliance or implications	▪ Connect with key business partners responsible for updates to how you map data, IT assets, processing activities, and new vendors or applications in use? ▪ Define a cadence to connect and reinforce periodic updates (in additional to automation)			

Embedding Privacy Across Functions

1 Establish Steering Committee

- Risk leaders, Data leaders, and other key stakeholders
- Develop and articulate privacy strategy and policy to business stakeholders
- Discuss new technologies and business processes that may trigger privacy compliance or implications

2 Identify Privacy Liaisons

- Connect with key business partners responsible for updates to how you map data, IT assets, processing activities, and new vendors or applications in use?
- Define a cadence to connect and reinforce periodic updates (in additional to automation)

3 Privacy Business Partner Program

- Reinforce privacy principles at the operational level
- Support early I.D. of new business processing activities
- Support privacy assessments *(LIA, PIA, DPIA)*
- Limits "hind-sight" questionnaire challenges with proactive engagement

4 Tailored Privacy Trainings

5 Establish New Product Lifecycle

onetrust

Does your organization have designated privacy liaisons that are responsible for reporting to privacy?

e.g., identify new data processing activities, new vendors/technologies, or other privacy-centric issues

Embedding Privacy Across Functions

1 Establish Steering Committee

- Risk leaders, Data leaders, and other key stakeholders
- Develop and articulate privacy strategy and policy to business stakeholders
- Discuss new technologies and business processes that may trigger privacy compliance or implications

2 Identify Privacy Liaisons

- Connect with key business partners responsible for updates to how you map data, IT assets, processing activities, and new vendors or applications in use?
- Define a cadence to connect and reinforce periodic updates (in additional to automation)

3 Privacy Business Partner Program

- Reinforce privacy principles at the operational level
- Support early I.D. of new business processing activities
- Support privacy assessments *(LIA, PIA, DPIA)*
- Limits "hind-sight" questionnaire challenges with proactive engagement

4 Tailored Privacy Trainings

- **Obtaining consent** + Ensuring new uses align with original consent
- The importance of privacy assessments *(PIA, LIA, DPIA)*
- **The need-to-know** about your vendors and the business processes you undertake
- **Applicability & shifts** in regulations/privacy laws

5 Establish New Product Lifecycle

Embedding Privacy Across Functions

1 Establish Steering Committee

- Risk leaders, Data leaders, and other key stakeholders
- Develop and articulate privacy strategy and policy to business stakeholders
- Discuss new technologies and business processes that may trigger privacy compliance or implications

2 Identify Privacy Liaisons

- Connect with key business partners responsible for updates to how you map data, IT assets, processing activities, and new vendors or applications in use?
- Define a cadence to connect and reinforce periodic updates (in additional to automation)

3 Privacy Business Partner Program

- Reinforce privacy principles at the operational level
- Support early I.D. of new business processing activities
- Support privacy assessments *(LIA, PIA, DPIA)*
- Limits "hind-sight" questionnaire challenges with proactive engagement

4 Tailored Privacy Trainings

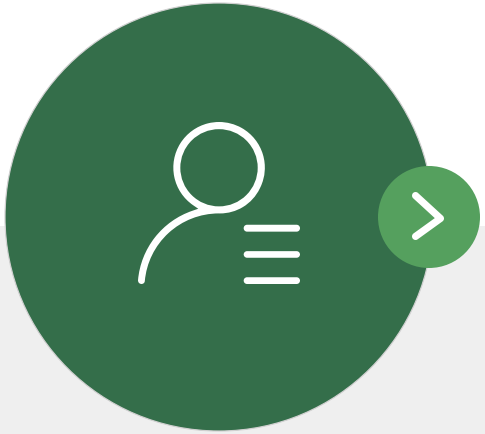
- **Obtaining consent** + Ensuring new uses align with original consent
- The importance of privacy assessments *(PIA, LIA, DPIA)*
- **The need-to-know** about your vendors and the business processes you undertake
- **Applicability & shifts** in regulations/privacy laws

5 Establish New Product Lifecycle

- Installing privacy-by-design into product development
- Allows for early review at the ideation stage to flag for potential privacy issues
- Develops a more linear pathway rather than create-review-revise iterations

Benchmarking for now, building for later

Benchmarking for now, building for later

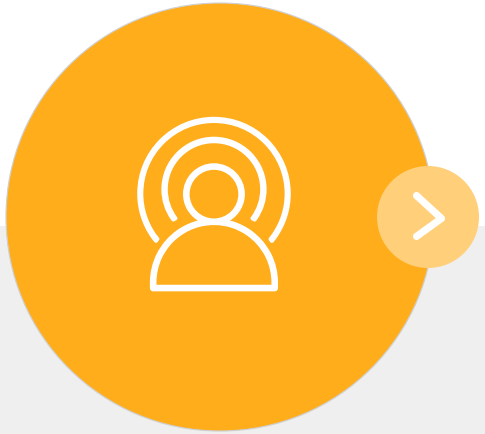


Developing Metrics

Track the progress and optimization of Privacy teams and how they add value to the larger organization

Privacy-led initiatives

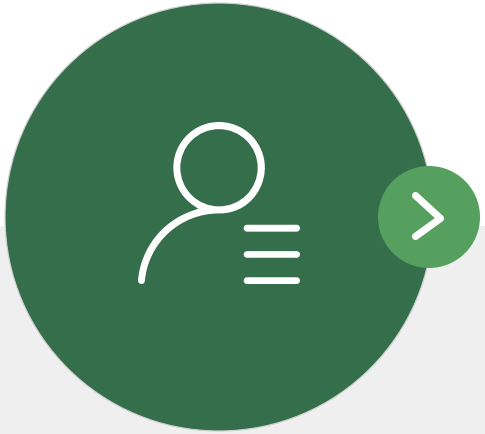
Leverage embedded privacy program to identify at-risk processes



Regulatory horizon scanning

Monitoring regulatory developments at Sectoral, US State, Federal, International regions and country-specific levels

Benchmarking for now, building for later



Developing Metrics

Track the progress and optimization of Privacy teams and how they add value to the larger organization

Sample Privacy Metrics

- Number of assessments & time to completion
- Number of vendors vetted & throughput time to onboarding
- Number of new AI use cases approved
- Number of incidents and whether reporting was required
- Training conducted (enterprise level and team level)

Benchmarking for now, building for later

Privacy-led initiatives

Leverage embedded privacy program to identify at-risk processes

- Departing Employee Program
- Data Retention Policy and Schedules
- Enterprise Privacy Training/Education
- AI Tool Selection and Deployment with Associated Policy and SOP Documentation
- Privacy Steering Committee
- Coordinated enterprise training (consolidating Privacy, Security, Compliance, Ethics) to develop a single calendar and reduce business burden
- Procurement and Vendor Process consolidation
- AI Governance Steering Committee

onetrust

How does your organization manage regulatory compliance and horizon scanning?

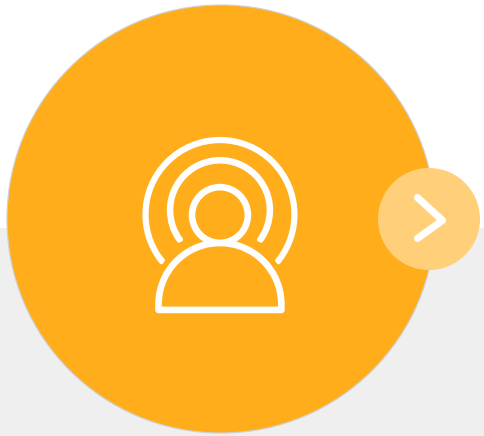
Internal teams responsible for keeping up to date
Outside counsel
Third party services and newsfeeds
Other.

Benchmarking for now, building for later

What does the law say,

What are the regulators doing,

What enforcement actions are you seeing?



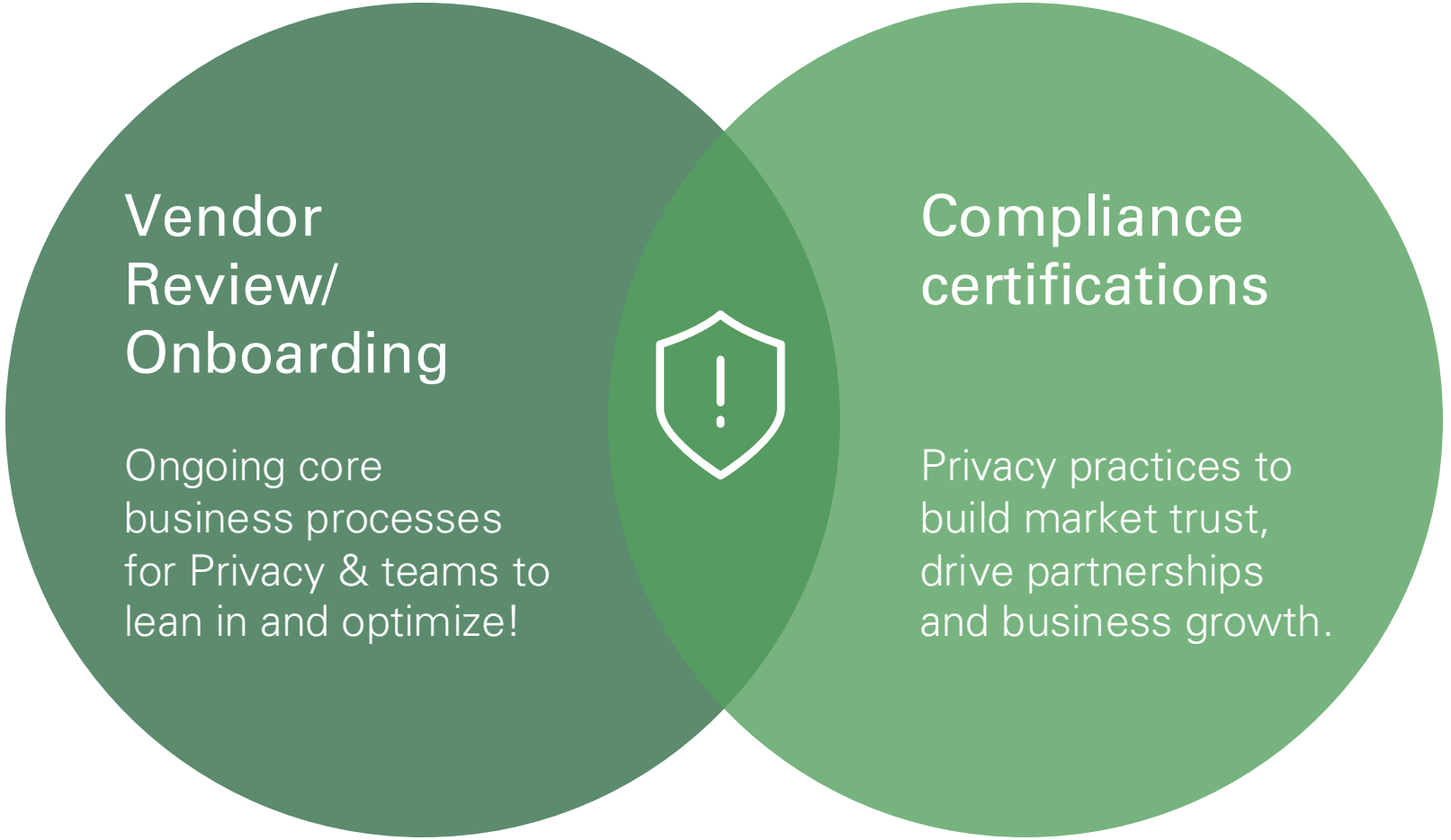
Regulatory horizon scanning

Monitoring regulatory developments at Sectoral, US State, Federal, International regions and country-specific levels

- Understanding the practical implications of regulatory changes:
  - *What should you start doing?*
  - *What should you stop doing?*
  - *What should you do differently?*
- Regulatory change doesn't necessarily mean obligations change
  - *Some regulatory change simply shifts responsibility for governance/enforcement/compliance*
  - *EU AI Act/Executive Order on AI examples*
    - *Shifting responsibility from AI developers to the companies that are using the AI to ensure customer trust*

Collaboration that Drives Operational Efficiency

Identify business use-cases that have clear ROI



Develop a holistic approach to third party risk management

01

Cross-functional Alignment

Delegate specific steps across privacy, security, risk, Legal, AI governance, IT, as well as procurement and finance

02

Workflow & process review

Create parallel workflows where possible rather than serial workflows, to reduce dependencies that can slow the process

03

Repeatable accountability

Establish SLAs for each step in the process

04

Develop metrics

Track process throughput, & bottlenecks for periodic to drive continuous improvement process

05

Tailored Intake Forms

Identify risk, data categories, access considerations, and controls for each vendor or business unit

06

Cascade deeper work

Identify when to trigger privacy assessments (LIA, PIA, DPIA, AI) based on vendor questionnaires

onetrust

How well-integrated do you feel your privacy teams are in the vendor onboarding process?

Cross-functionally alongside security, legal, compliance, risk, IT, finance, and procurement

Fast-tracking Integrated Compliance

01

Cross-functional Alignment

Partnership between privacy, security, risk, and audit teams

02

Prioritize to business drivers

Identify the certifications most likely to drive business value

03

Applicability & accountability

Map out the controls and delegate responsibility across partner teams with SLAs to complete

04

Milestone-based execution

Breaking certification process into stages helps the task feel less overwhelming

05

Documentation !!!

- Say what you do, Do what you say
- Labeling & version control
- Continuous review and revision process

06

Audit Calendar optimization

Audit cadence, build it into your business calendar

Aligning AI Capabilities to Business Needs & Growth

onetrust

Does your organization have an AI governance committee that meets regularly and sets the enterprise strategy around AI use and governance?

Building a Cohesive AI Governance Strategy

Benchmarking & Metrics

AI enablement requires a robust system of measurement of historical processes and quantifiable improvements through introduction of AI

Buy vs Build vs Shadow AI

Identify your core set of AI tools, ensure that you have proper contractual and procedural protections in place

Strategic Alignment

Importance of having a clear strategy, where all initiatives, processes, and resources align towards these goals

Identify AI Use Cases

Identify dependencies, bottlenecks, and manual processes that can benefit from automation, introduction of agentic AI

Human-in-the-loop

Ensuring human oversight/QC to avoid bias, drift, hallucinations

Labeling AI interactions and outputs

Increasing regulation around disclosure of AI interaction, content labeling, deepfakes

Recap & Key Takeaways

01

Insight into how organizations embed privacy into the technology lifecycle and day-to-day operations

02

Programmatic best practices for scaling privacy programs, improving consistency, and driving operational excellence

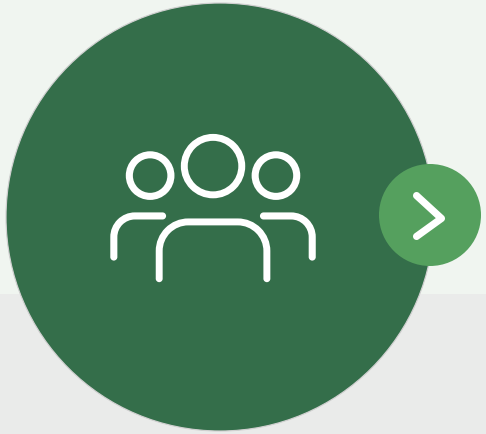
03

Practical approaches to collaborating with executive stakeholders and increasing visibility into privacy risk and performance

04

Perspective on the regulatory horizon and how upcoming changes are influencing privacy strategy

From compliance to impact: Your next steps



AI Governance RACI Matrix

A visual that shows how to structure your AI committee, define ownership for activities.

Understanding the data privacy maturity model ebook

A guide to understand your privacy maturity level and the steps to advance it.

Privacy readiness self-assessment

An interactive assessment that gives you an instant snapshot of where your program stands.

Questions?

Brett Tarr

Head of Privacy & AI Governance
OneTrust

onetrust

Thank you!

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://iappwf.questionpro.com/t/AbBPvZ7vIh

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 AIGP, 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 prior to the live webinar will automatically receive credit. After the broadcast date, individuals may submit for credit by completing 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 please contact: livewebconteam@iapp.org