An Agile Approach to PIAs and Privacy by Design

Moderator:
Andrew Clearwater, CIPP/US Director of Privacy, OneTrust

Panelists:
Chad Quayle, CIPT, Senior Privacy Manager, Cox Communications
Cynthia Van Ort, CIPM, CIPP/C, CIPP/US, CPO North America, Citigroup, Inc.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Foundational Knowledge</td>
</tr>
<tr>
<td>2</td>
<td>Train a Privacy Champion</td>
</tr>
<tr>
<td>3</td>
<td>Create a Threshold Step</td>
</tr>
<tr>
<td>4</td>
<td>Create Specific Questionnaires</td>
</tr>
<tr>
<td>5</td>
<td>Hook Into the SDLC</td>
</tr>
<tr>
<td>6</td>
<td>Deliver the PIA Using a User Friendly Tool</td>
</tr>
<tr>
<td>7</td>
<td>Track results in development systems</td>
</tr>
<tr>
<td>8</td>
<td>Aim for Constant Improvement</td>
</tr>
</tbody>
</table>

**OnetTrust**

**Foundational Knowledge**
The Value of PIAs

They solicit all necessary information up front, to inform risk assessment.

They identify considerations which may drive project development.

They standardize an approach to facilitate auditable and consistent responses to the same scenario.

They enable proactive builds of privacy in the design (Privacy by Design).

Traditional PIAs

Privacy impact assessments (PIAs) are a tool to identify and reduce privacy risks.

3 Components of a PIA

1. Plan the Intake Questions
2. Gather Responses & Take Action
3. Review and Report Outcomes
What is Agile?

Team Collaboration

Short Feedback Loop

Iterative and Evolutionary

OneTrust

Why the Traditional PIA Approach Doesn’t Work

Traditional PIAs:
- One and Done Approach
- Typically Extensive
- Time-consuming
- Administered by Privacy Professionals

What is Needed:
- Continuous Assessment
- Immediate identification of risks
- Rapid Advice

OneTrust
Why We Need Agile

We are in a rapidly evolving information age
- Big Data, Mobile and the Internet of Things are rapidly transforming how information is collected, processed, used and shared.

Our industry is in a digital transformation
- Mobile finance, alternative lending, digital payments and currency and a host of other rapidly emerging information platforms are re-shaping financial services.

New framework is emerging
- Information-related global laws and regulations are adapting to new technologies and new data uses, requiring a new approach to managing information-related risks.

What is Privacy By Design?

Privacy by Design Principles
- Proactive not reactive; Preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric
Train a Privacy Champion

Training and Awareness

- Establishing Privacy champions embeds privacy/security eyes and ears throughout the organization.
- Identified individuals with the title “Privacy Champions” or “Business Privacy Officers” puts accountability for privacy in the business or with individuals.
- Training them could be at various levels, from “how you protect yourself from identity theft” to IAPP level training and training in between.
Create A Threshold Step

Use Threshold Assessments

- Traditional assessments review the entire project at the beginning
- Traditional assessments do not have touchpoints at iterations
- Traditional assessments do not have an understanding of the technology
- Traditional assessments are standardized and may not fit the product
Create Specific Questionnaires

Communication – Create Specific Questionnaires

- Create and publish general guidance/guardrails for an initial build
- Create a standardized library of scenarios and decisions trees
- Consider creating focused PIAs for different sprints
- Automate, where possible, controls and reporting

OneTrust
Hook into the SDLC

Process – Hook into the SDLC

- Avoid Redundancies
- Streamline the Response activity
- Demonstrate Value
- Build metrics into the PIA tool

OneTrust
Deliver the PIA Using a User Friendly Tool

- Get The Right Information
- At the Right Time
- In the Right Way
- To the Right Person

OneTrust
Track results in development systems (ie. JIRA)
Aim for Constant Improvement

Seek incremental improvement over time by focusing on:

- Feedback
- Efficiency
- Evolution

OneTrust
OneTrust Tool Launch for IAPP
IT Application Development

Lead
Tim Wilson (External)

Reviewer
Tim Wilson (External)

Started
8/22/2016 11:36:23 PM

Completed
8/22/2016 11:37:25 PM

APPROVAL NOTES

Approval contingent upon identification of data hosting parties. Full Privacy Impact Assessment not required.

RISKS

Risk 1: Low
Data hosted by third parties requires an vendor agreement in place.

Recommendation: 
Mitigation:

Determine where data is hosted.

OneTrust
Data Privacy Software

Thank You