



# Privacy by Design

**Brendon Lynch, Microsoft**  
**Trevor Hughes, IAPP**

Session ID: ASEC-304  
Session Classification:

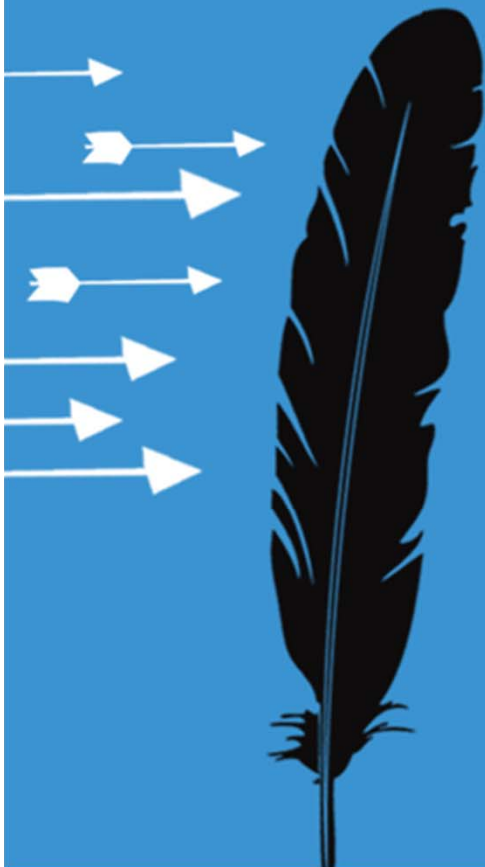
**RSACONFERENCE2012**

# Privacy by Design

- What is it? Why now?
- Building it. Microsoft Example
- Getting Support.
- Where to Focus.
- Getting Help.
- Education.
- Running, Measuring, and Managing it.



# What is Privacy by Design?



# Privacy by Design

- A broad collection of ideas.
- Championed by Ann Cavoukian, Privacy Commissioner of Ontario
- Basically, build privacy into technology and business processes before launch, not after.





# Why now?

**RSA**CONFERENCE2012

# Privacy by Design

- As public policy efforts have struggled to respond to privacy concerns, attention has turned to operational solutions
- EU Directive, Framework Review
- FTC
- APEC
- Commerce White Paper

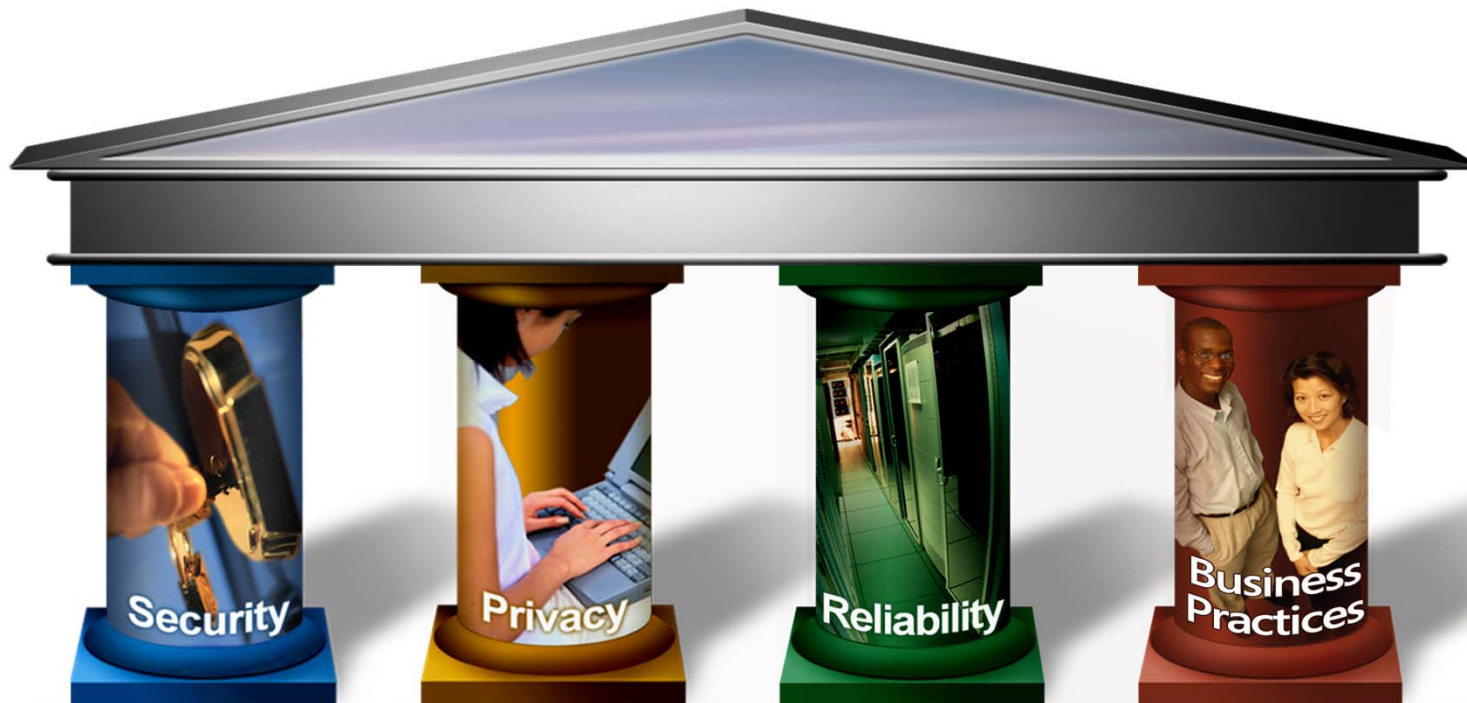




# Building it. Microsoft example.

RSA CONFERENCE 2012

# Trustworthy Computing



- Secure against attacks
- Protects confidentiality, integrity and availability of data and systems
- Manageable

- Protects from unwanted communication
- Controls for informational privacy
- Products, online services adhere to fair information principles

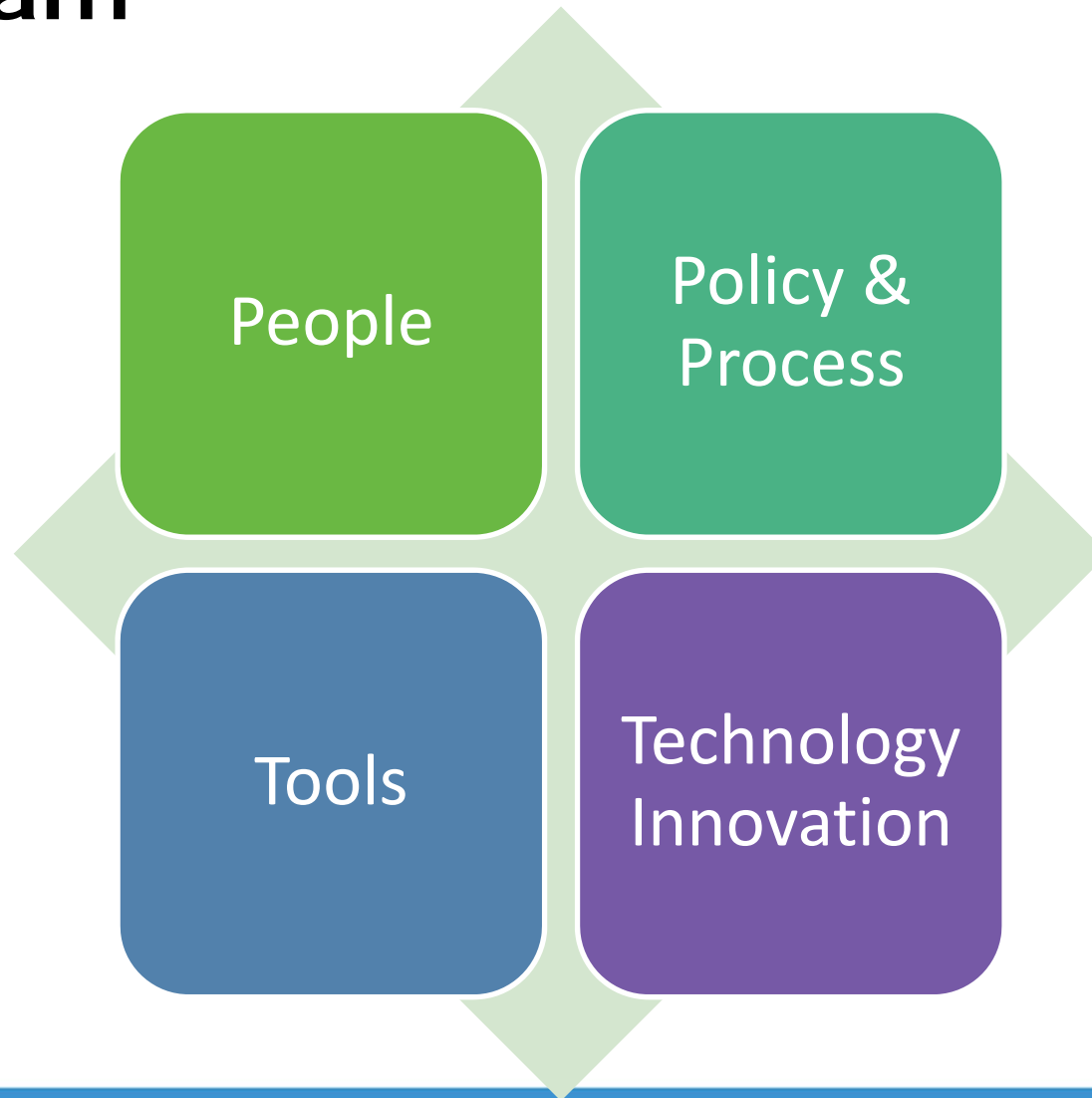
- Dependable, Available
- Predictable, consistent, responsive service
- Maintainable
- Resilient
- Recoverable, easily restored
- Proven, ready

- Commitment to customer-centric interoperability
- Recognized industry leader, world-class partner
- Open, transparent





# Microsoft's Privacy Governance Program





# People

RSA CONFERENCE 2012

# People

- The Team
  - ~40 full-time privacy professionals
  - ~400 part-time privacy managers and leads
- Expertise
  - Legal
  - Scientists
  - IT Policy and Management
  - Software Engineers
  - Marketing
  - Business



Legal and  
Corporate  
Affairs  
Privacy  
Team

TwC Privacy Team

Privacy Manager

Privacy Lead

Privacy Champ

**iapp**

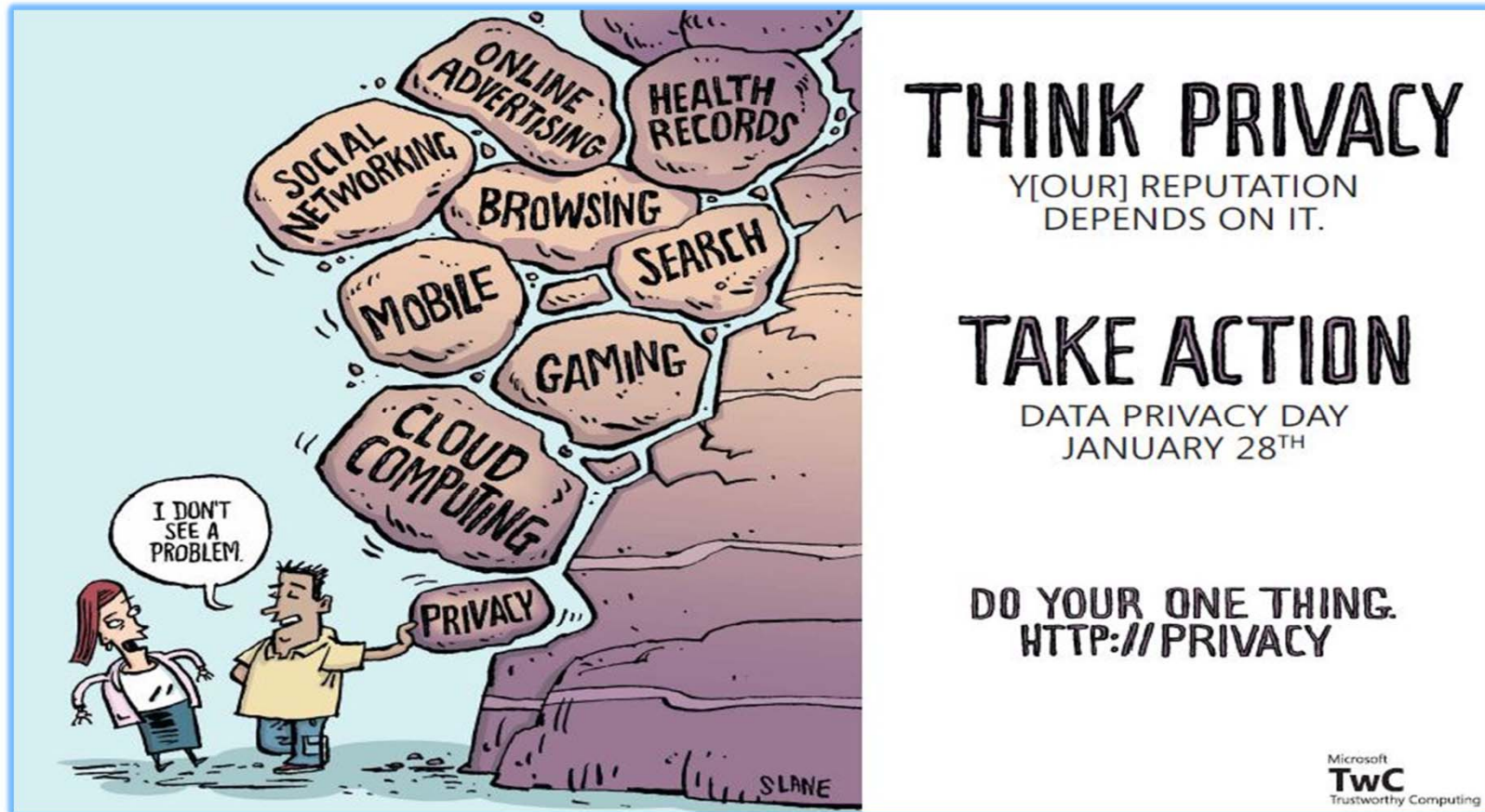
international association  
of privacy professionals

RSACONFERENCE2012



# Developing Capability

- Onboarding, Mentoring, & Continuing Education



**iapp**

international association  
of privacy professionals

RSACONFERENCE2012





# Policy & Process

RSA CONFERENCE 2012

# Microsoft Privacy Standard

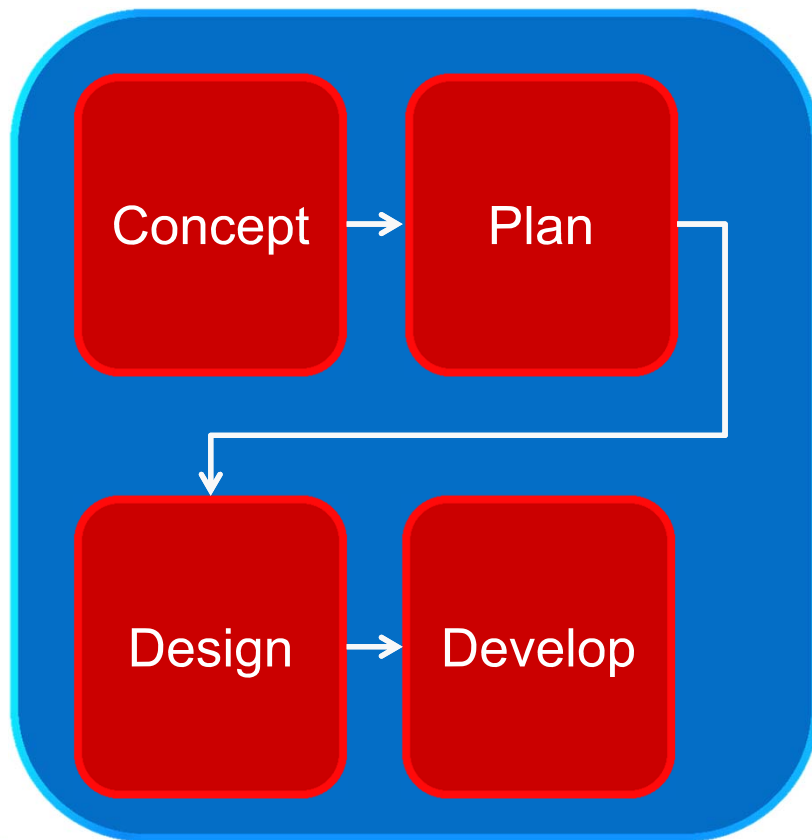


- Software/services development
- Sales and Marketing
- Online Advertising
- Cloud Services
- Location Based Services
- Collection of information from children

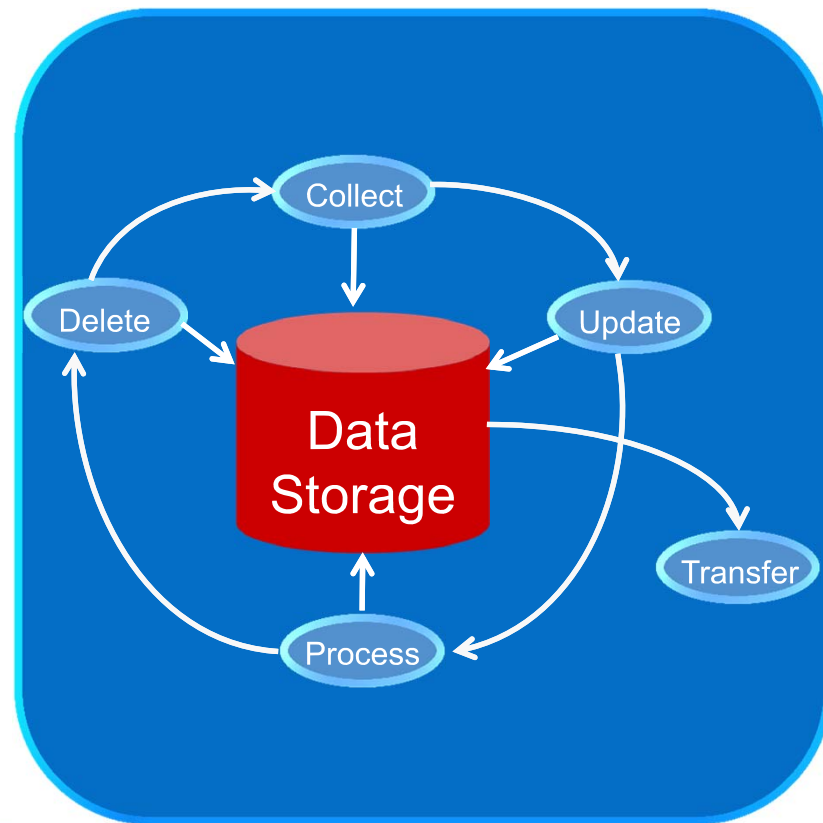


# Privacy in Products, Services and Other Instances

## Development Lifecycle

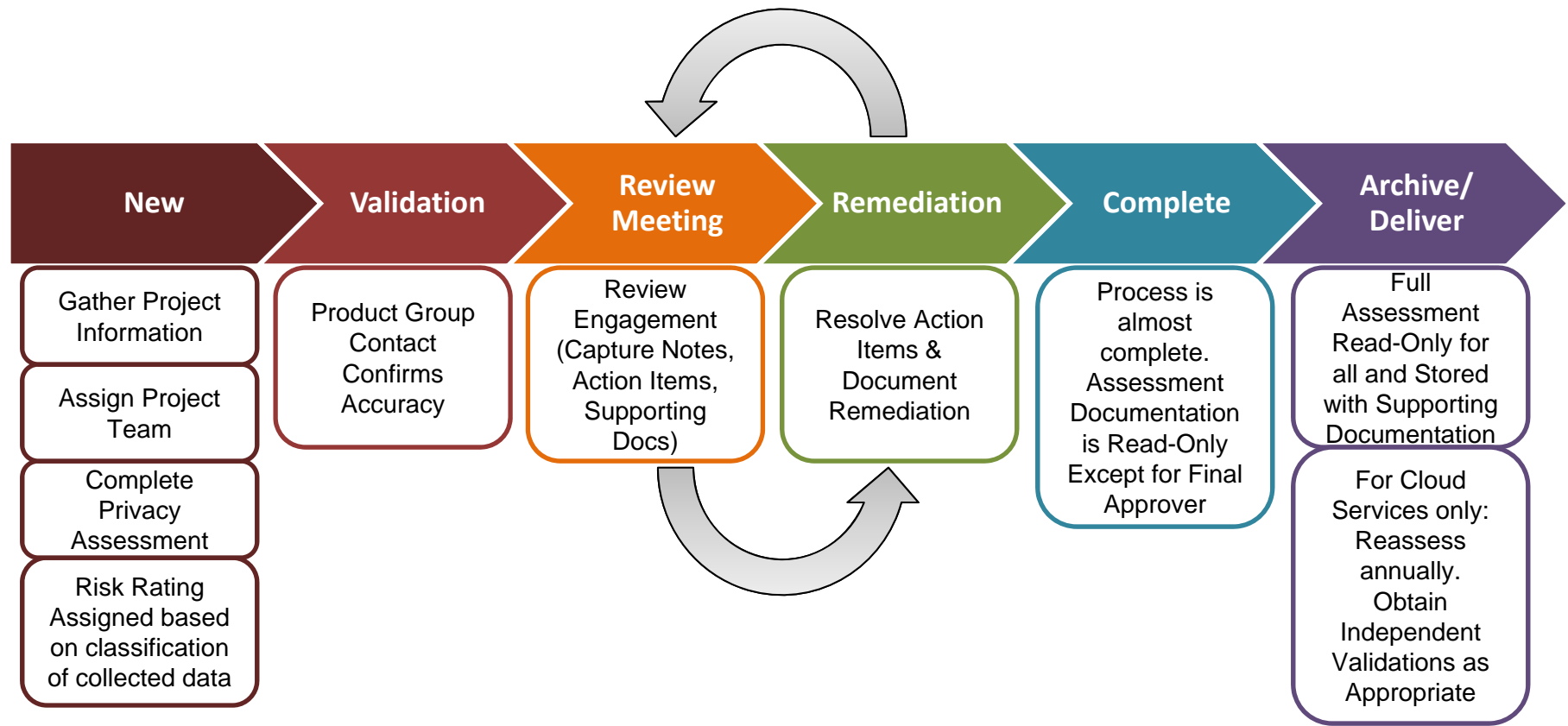


## Information Lifecycle





# Privacy Review Process



# Privacy Reviews



## Players

- Involve those that can answer questions about the planned project/product/service
- Ensure the team understands what they need to provide

## Objective

- Understand data collection, data use, user experience – ensure compliance with policy/standards

## Documentation Requirements

- Privacy Approval Manager Complete
- User experience screenshots or demo (as applicable)
- Marketing materials (websites, emails, etc.)
- Previewed by Privacy Champ or Lead





# Tools

# Policy Approval Manager

PAM Home
Trustworthy Computing
PAM
Policy Approval Manager

Friday 19 August, 2011
Welcome, Rob Roberts
b Roberts

Assessment
Assessment Template

Assessment
Create Assessment
Create Master Assessment
Search/View Assessment
Clone Assessment

Review Presentation
Review Templates
Glossary & Training

Find PAM ID:
Go

Modify Assessment
Project Name: IAPP Demo
PAM ID: 3600

General Information
Assessment Criteria
Assessment
Summary

Show Responses
Discipline
Assessment Status
Rating

Privacy
Validation
P1
Export To Excel
Create Document

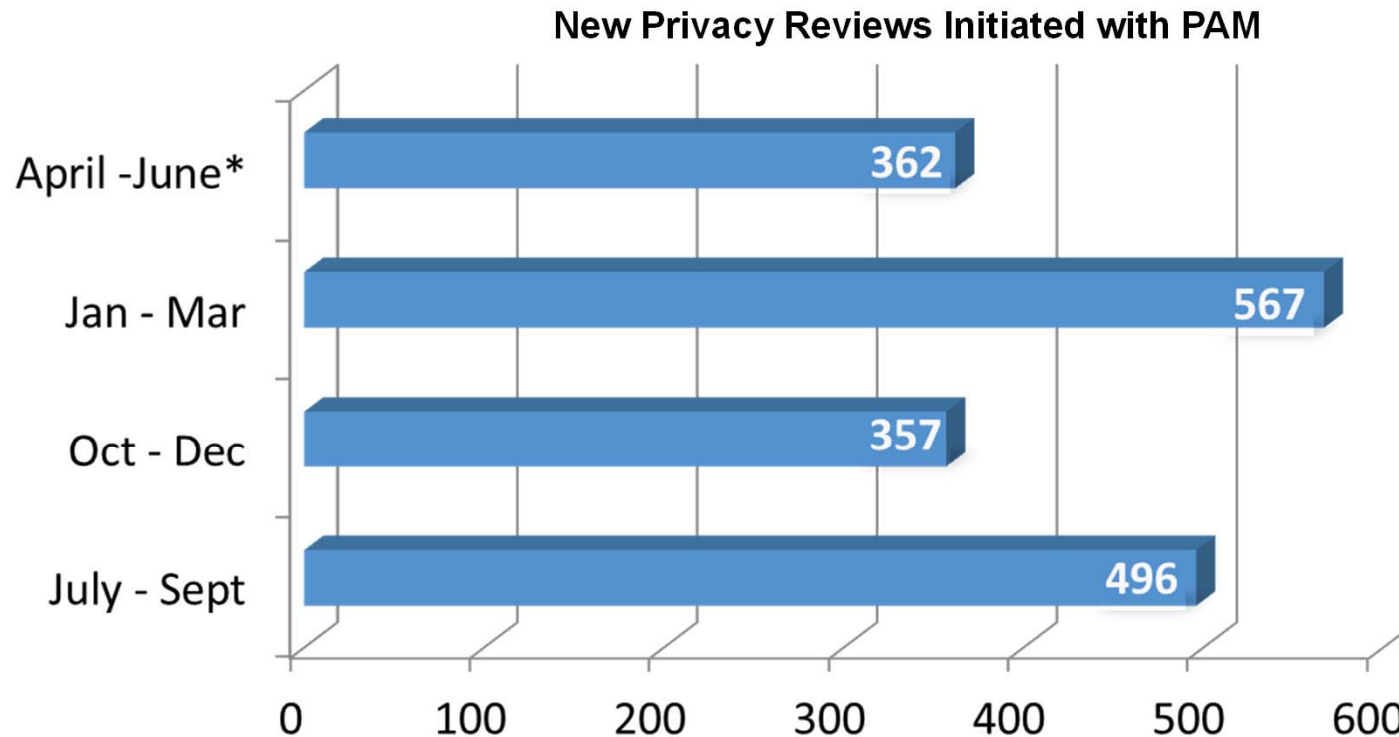
Web Site, Web Aware, or Online Services
Clear Filters

QuestionID	Question	Response
1	What types of data will be collected, transferred, or used? (check all that apply)	PII
1.1	Would you like to complete the detailed questions at this time?	Yes
1.1.1	List all the data types being collected and a brief statement of the purpose of their collection. Please Note: The remaining questions in this section will ask additional details about the types of data collected and their use	First Name, Last Name, Email Address
1.1.2	If any PII data (name, phone, email, physical address) is collected or stored as part of this project, will it be used for promotional purposes?	No
1.1.3	If any PII data (name, phone, email, physical address) is collected or stored as part of this project, please describe any transaction details that are recorded as part of the PII collection (e.g. timestamp, etc.)	Timestamp, Last log on
1.1.4	Are you collecting credit card numbers?	No
1.1.5	Will you be collecting information regarding user interactions (i.e. click tracking, site analytics, etc.)	No
1.1.6	Will this data be associated with any previously collected customer data? If so, please describe.	
1.1.7	What methods will be used to collect the data?	Standard Web logging
1.1.7.2	Will standard web logging be used?	No
1.1.8	Are you displaying content from a third party domain and/or using iframes?	No
1.1.11	Does the website contain or expose employee performance data?	No
1.1.12	Are you transferring and storing the data using a Security approved method (e.g., https://)?	No
1.1.13	Is there a data retention plan in place?	No
2	Is data being stored on the user device using one or more of the following mechanisms? If so, please check all that apply:	Flash Objects or other Local Shared Objects
2.1	Does the project use Flash or Silverlight local shared objects (e.g., "Flash Cookies")?	No
3	Does your service allow users to store data in the cloud including email, photos, back-up data, etc..?	No
4	Is this experience targeted to or attractive to children?	No
5	If this project is targeted at a business or entity will the users be enabled to collect or store PII of their employees or customers?	No

ENCE2012



# Privacy Risk Mitigation in Practice: The PAM Tool



*\*Thru June 9, 2011*

Since deploying the PAM Tool in July 2010, business groups across Microsoft have used the tool to initiate more than 1,700 privacy reviews

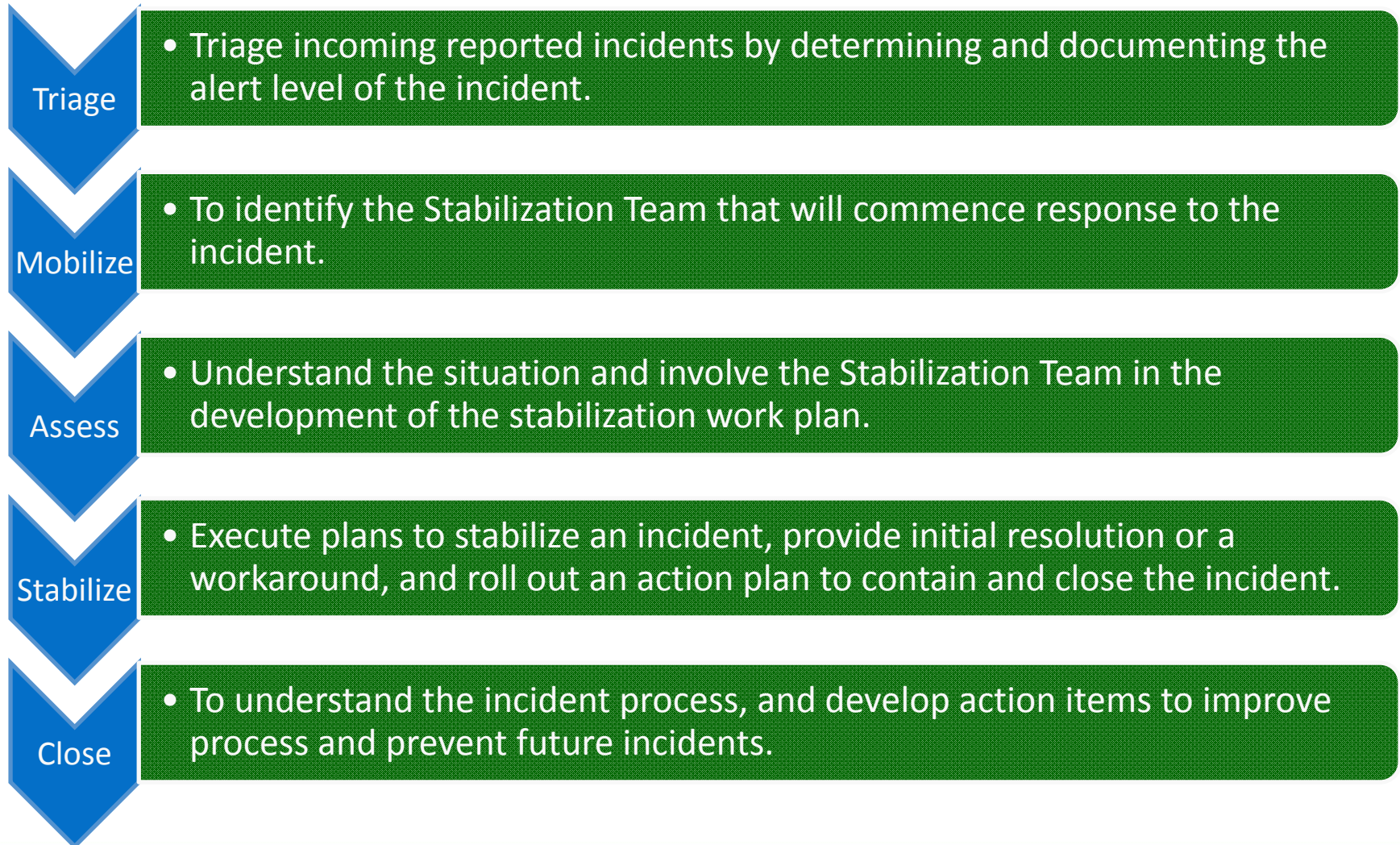
**iapp**

international association  
of privacy professionals

RSACONFERENCE2012

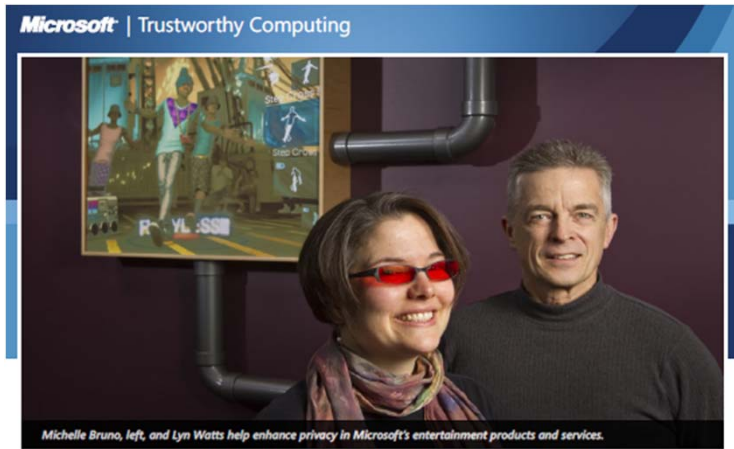


# Privacy Escalation Response Process





# Case Study: Kinect for Xbox 360



Fast Facts

Privacy in Microsoft's Online Gaming Realm Is Serious Business



# Case Study: The Privacy Review



## Skeletal

- Commands
- Session based, then zapped
- Research use only



Identity  
Login using facial  
recognition



Privacy Solution  
Only for service, no promo use  
Kept locally on your box







# Technology innovation.

**RSA**CONFERENCE2012

# Microsoft Research

- Overall, 800+ scientists
  - Computer Science
  - Engineering
  - Psychology
  - Mathematics
  - Physics
  - Sociology
- Privacy projects
  - Database privacy
  - Encryption
  - Social media collective



# Privacy Guidelines for Developing Software and Services

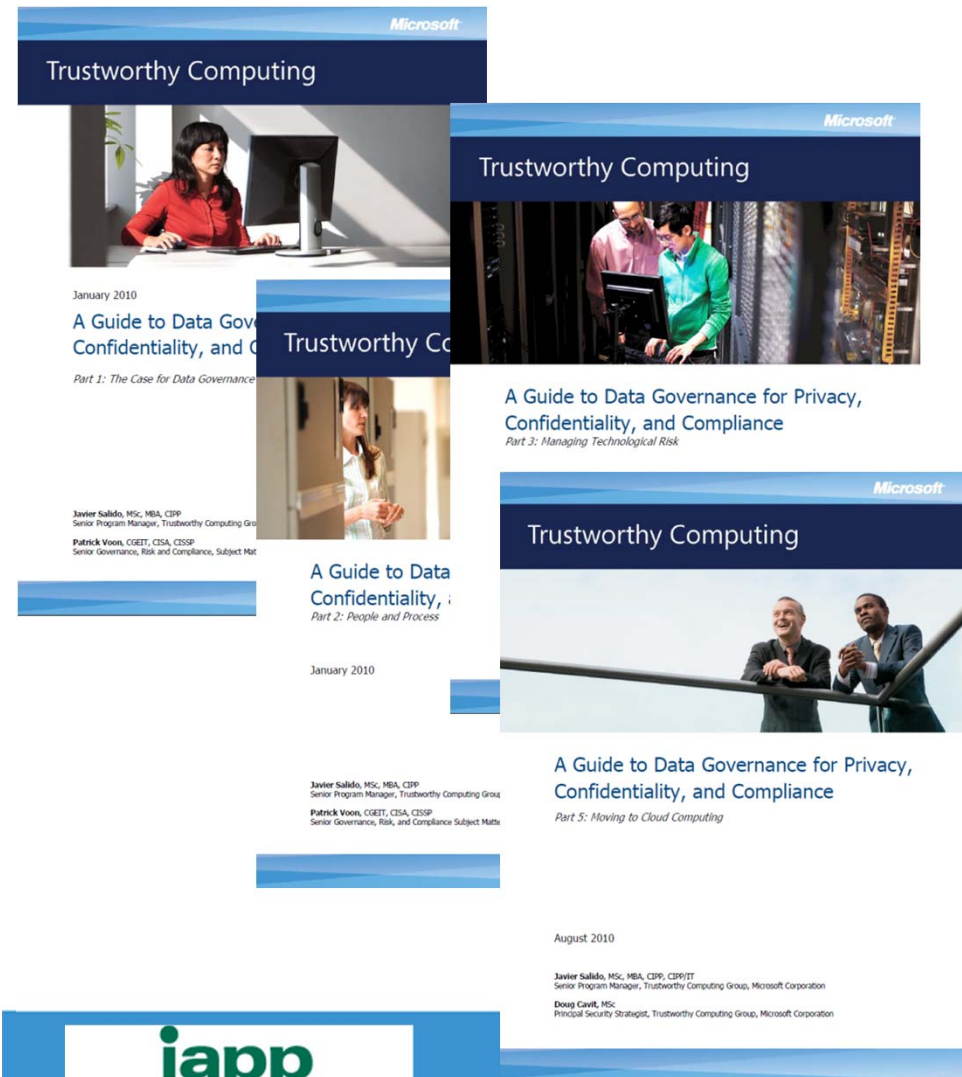
When and how to:

- Provide different types of notice
- Present customers with choices
- Obtain informed consent from users



# Data Governance

- “How-to” series
- People
  - Process
  - Technology
  - Cloud Computing





# What's Next

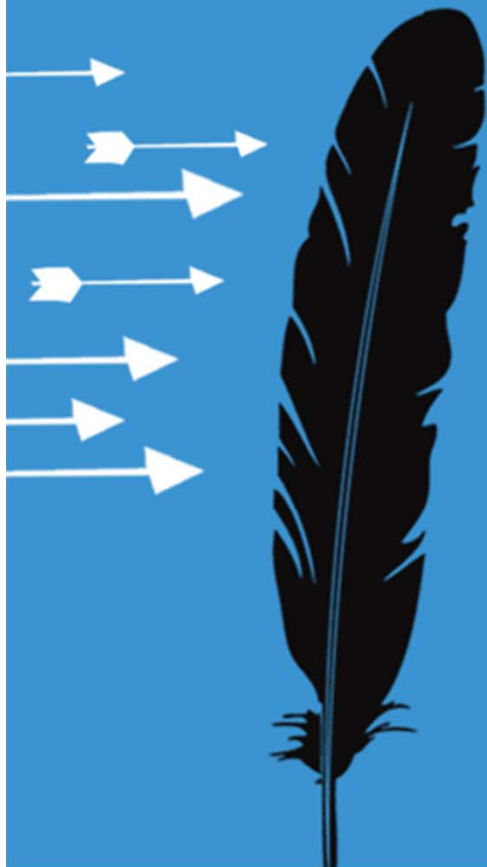
**RSA**CONFERENCE2012

# What next?

- Privacy by Design is here to stay.
  - Just good business – privacy matters
- Scale according to risk
  - PIAs, governance models, monitoring
  - Management ownership, “skin in the game”
- Watch regulatory developments
  - FTC, Commerce
  - EU framework



# Applying Privacy by design.



# Applying privacy by design

- Learn more about privacy by design at:
  - <http://privacybydesign.ca/>
  - <http://microsoft.com/privacy/bydesign.aspx>
- Implement a comprehensive privacy program covering people, policy, process and tools
- Identify and attach to existing processes where practical (e.g., security assessments)

