Embedding Privacy by Design

Metric Stream Customer Conference

May 12, 2015

TRUSTe Data Privacy Management Solutions

Today's Agenda

- Privacy in the Context of GRC
- Data Privacy Management and Top Privacy Priorities
- TRUSTe Assessments Benchmark Data
- Key DPM Use Cases
  - Global Data Transfer Management
  - Global Data Transfer Interoperability
  - Integrating Privacy Into Product Lifecycle
  - Data Discovery and Mapping

Privacy in the Context of GRC

POWERING TRUST IN THE DATA ECONOMY

GRC Illustrated

DEVELOPED BY OCEG® with contributions from: TRUSTe

What are the elements of privacy risk management and compliance?

Organizations that handle personal information face increasingly complex challenges to effectively manage privacy risk and compliance. The impact of these challenges covers the entire information life cycle.

An Effective Data Privacy Management Capability

An effective data privacy management has defined, auditable processes and policies that are consistent with the Fair Information Practice Principles. Key components include:

- Collection Need Assessment
- Use Risk Assessment
- Privacy Policy with Pre-Approval, Access and Use Provisions
- Transfer Policy and Procedures
- Security and Disposal Policy and Procedures
- Assessment and Monitoring
- Effective Technology Support

Fair Information Practice Principles

Issued by the U.S. Federal Trade Commission

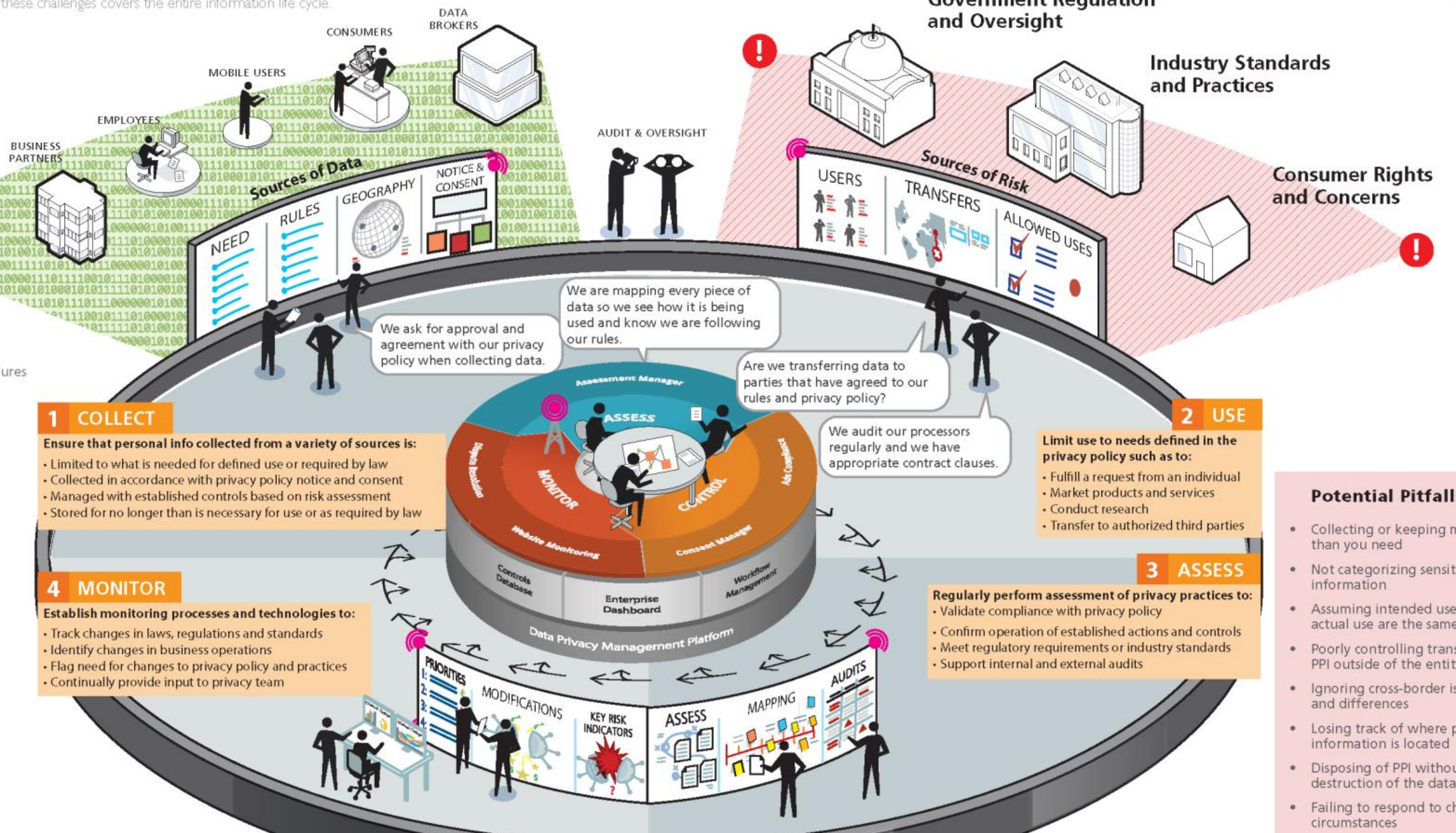
1. Notice/Awareness
How data is collected, used and transfered to others

2. Choice/Consent
Options to control how data is used beyond the immediate transaction

3. Access/Participation
Ability to view and verify the data collected

4. Integrity/Security
Securing data with limited access for neccessary employees

5. Enforcement/Redress
Self-regulation, civil actions and government enforcement



We ask for approval and agreement with our privacy policy when collecting data.

We are mapping every piece of data so we see how it is being used and know we are following our rules.

Are we transferring data to parties that have agreed to our rules and privacy policy?

We audit our processors regularly and we have appropriate contract clauses.

1 COLLECT

Ensure that personal info collected from a variety of sources is:

- Limited to what is needed for defined use or required by law
- Collected in accordance with privacy policy notice and consent
- Managed with established controls based on risk assessment
- Stored for no longer than is necessary for use or as required by law

2 USE

Limit use to needs defined in the privacy policy such as to:

- Fulfill a request from an individual
- Market products and services
- Conduct research
- Transfer to authorized third parties

3 ASSESS

Regularly perform assessment of privacy practices to:

- Validate compliance with privacy policy
- Confirm operation of established actions and controls
- Meet regulatory requirements or industry standards
- Support internal and external audits

4 MONITOR

Establish monitoring processes and technologies to:

- Track changes in laws, regulations and standards
- Identify changes in business operations
- Flag need for changes to privacy policy and practices
- Continually provide input to privacy team

Potential Pitfalls

- Collecting or keeping more than you need
- Not categorizing sensitive information
- Assuming intended use and actual use are the same
- Poorly controlling transfer of PPI outside of the entity
- Ignoring cross-border issues and differences
- Losing track of where private information is located
- Disposing of PPI without full destruction of the data
- Failing to respond to changed circumstances
- Preventing audit and oversight due to poor visibility
- Manually managing a complex information lifecycle

contact info@oceg.org for comments, reprints or licensing requests © 2015 OCEG®

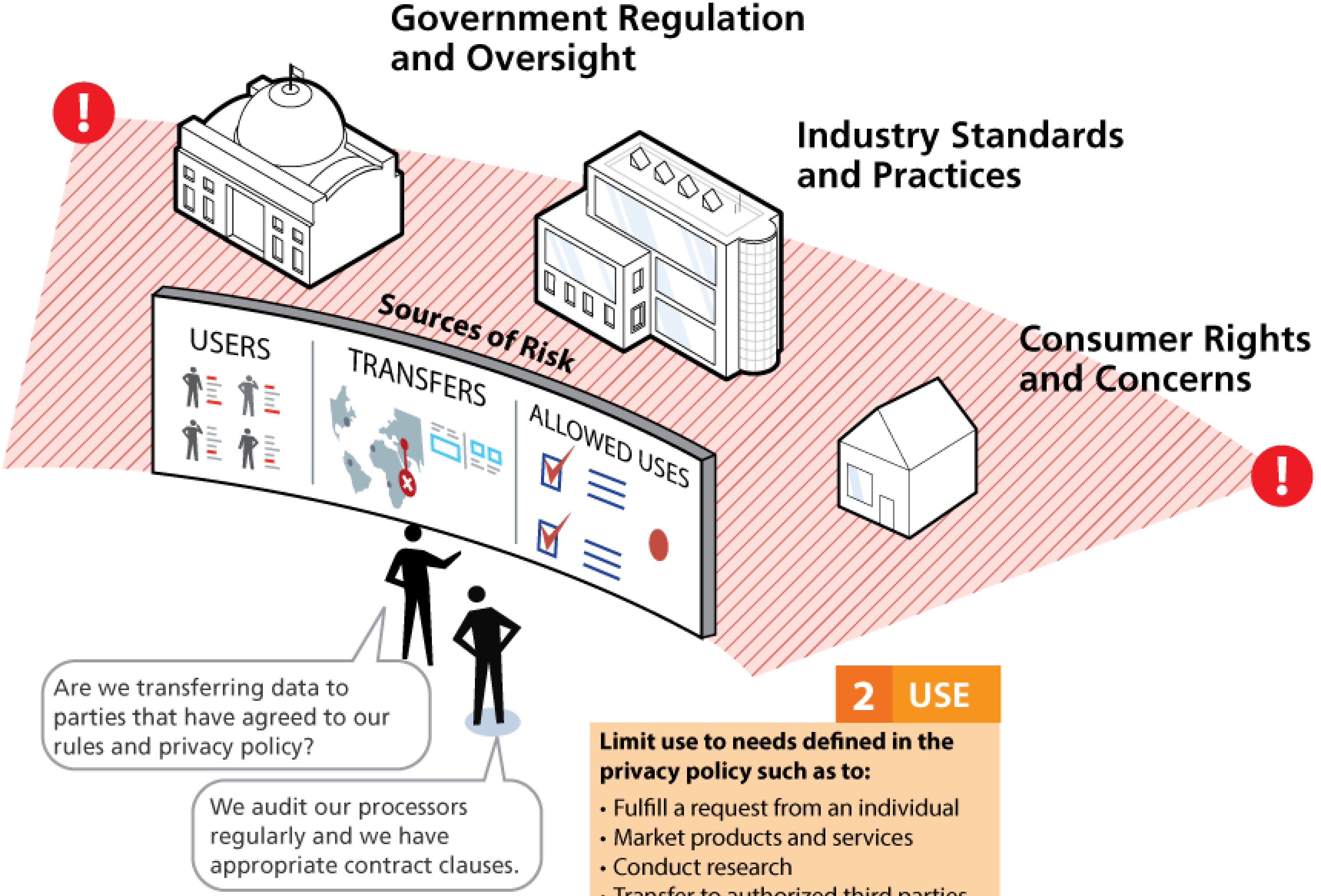
http://www.oceg.org/resources/illustration-privacy-risk-management-compliance-2015/

DATA BROKERS
CONSUMERS
MOBILE USERS
EMPLOYEES
BUSINESS PARTNERS
Sources of Data
NEED
RULES
GEOGRAPHY
NOTICE & CONSENT
We ask for approval and agreement with our privacy policy when collecting data.

1 COLLECT

Ensure that personal info collected from a variety of sources is:

- Limited to what is needed for defined use or required by law
- Collected in accordance with privacy policy notice and consent
- Managed with established controls based on risk assessment
- Stored for no longer than is necessary for use or as required by law



Government Regulation and Oversight

Industry Standards and Practices

Consumer Rights and Concerns

Are we transferring data to parties that have agreed to our rules and privacy policy?

We audit our processors regularly and we have appropriate contract clauses.

2 USE

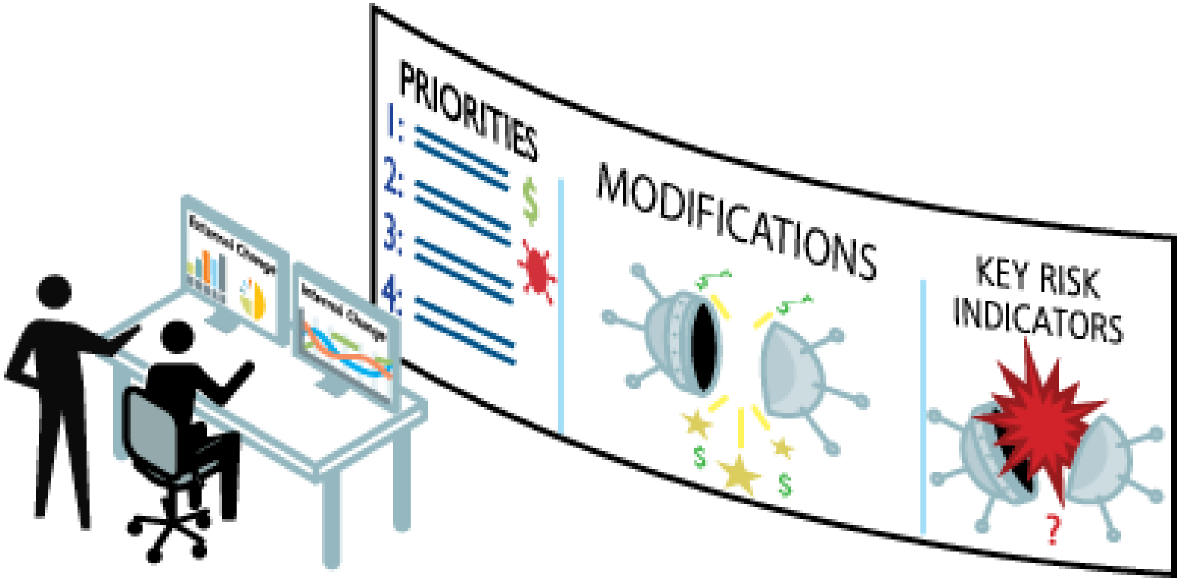
Limit use to needs defined in the privacy policy such as to:

- Fulfill a request from an individual
- Market products and services
- Conduct research
- Transfer to authorized third parties

3 ASSESS

Regularly perform assessment of privacy practices to:

- Validate compliance with privacy policy
- Confirm operation of established actions and controls
- Meet regulatory requirements or industry standards
- Support internal and external audits



4 MONITOR

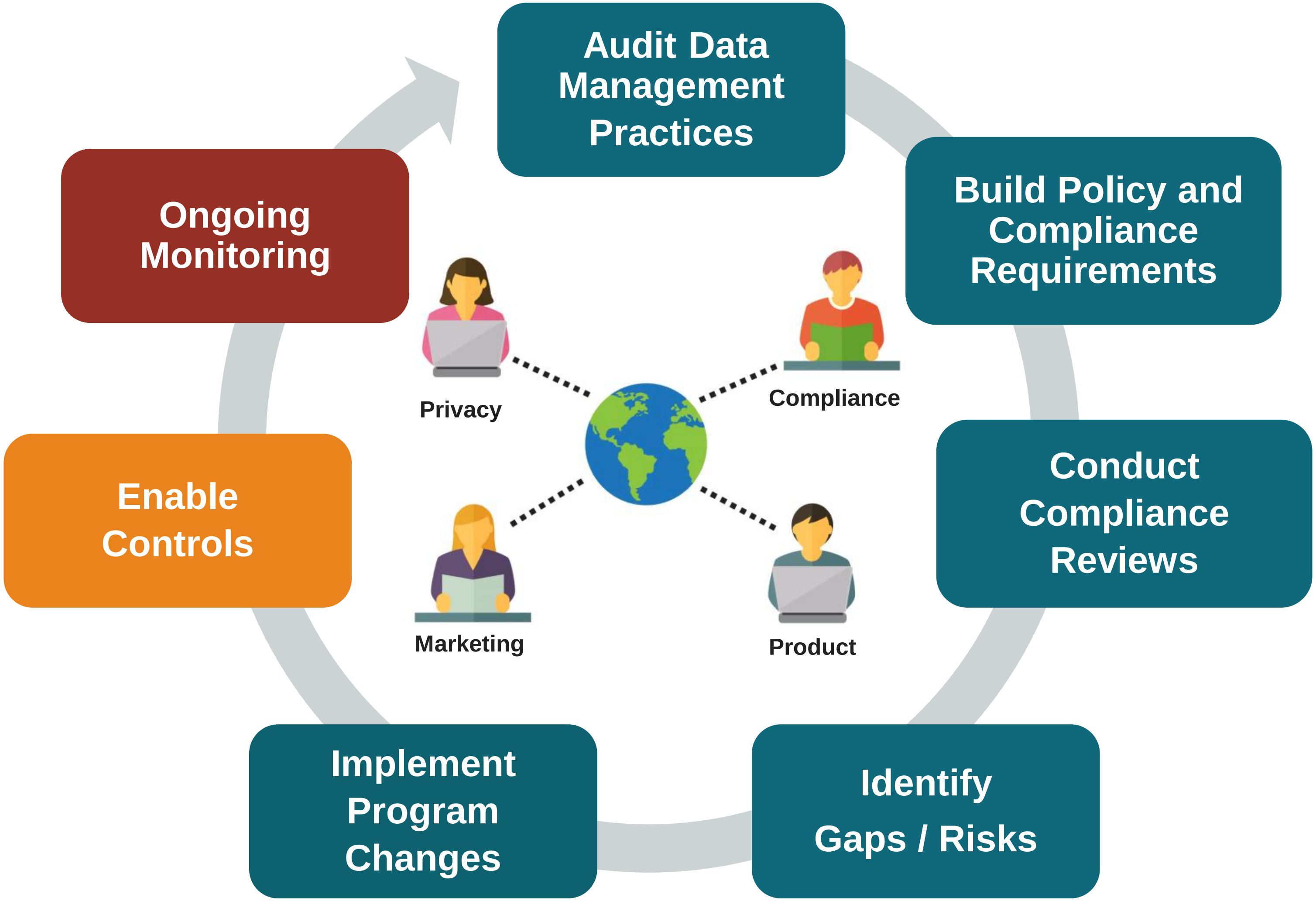
Establish monitoring processes and technologies to:

- Track changes in laws, regulations and standards
- Identify changes in business operations
- Flag need for changes to privacy policy and practices
- Continually provide input to privacy team

Privacy Management Functions

POWERING TRUST IN THE DATA ECONOMY

Data Privacy Management Process



Audit Data Management Practices

Build Policy and Compliance Requirements

Conduct Compliance Reviews

Identify Gaps / Risks

Implement Program Changes

Enable Controls

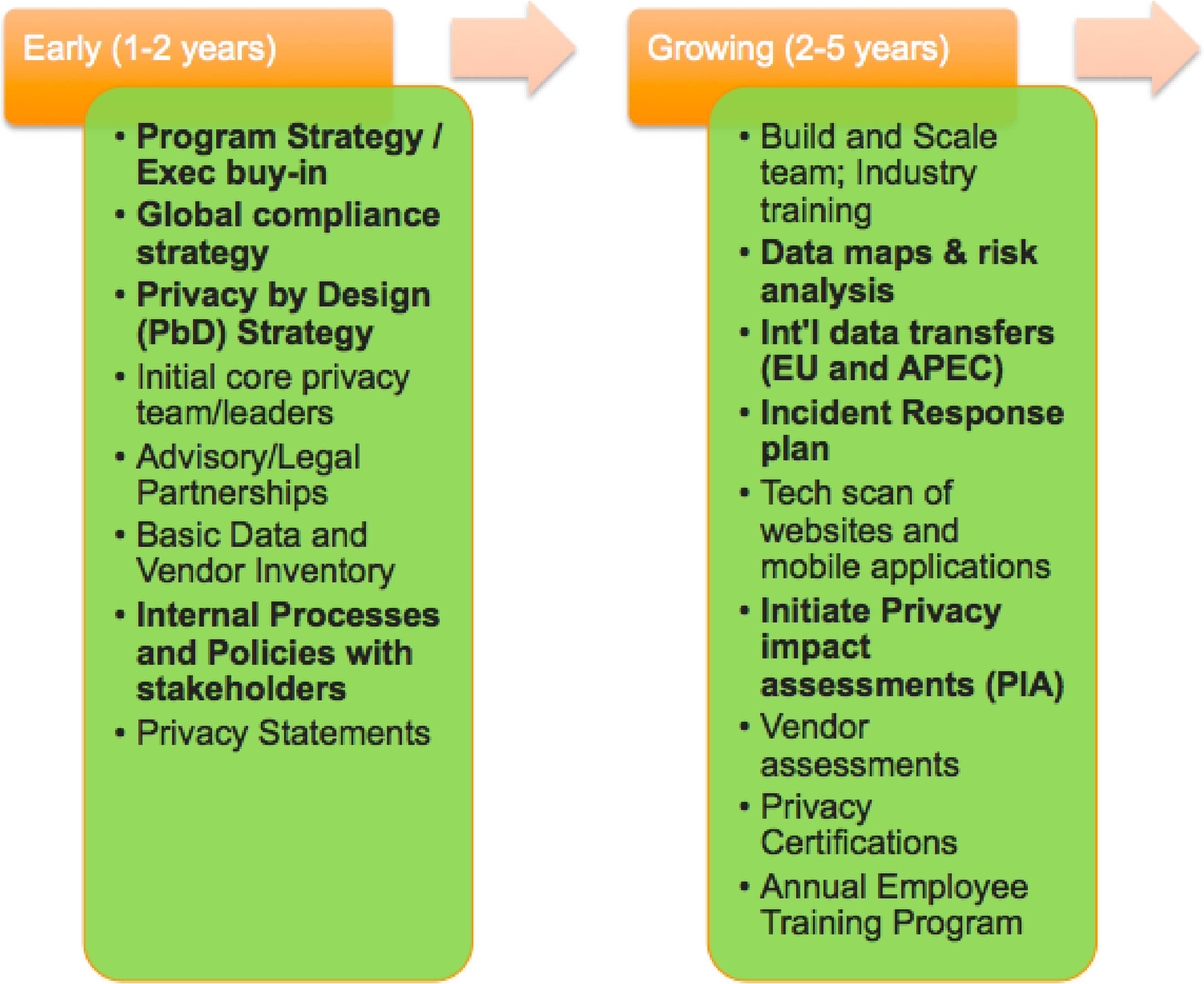
Ongoing Monitoring

Privacy Program Evolution

Early (1-2 years)

- **Program Strategy / Exec buy-in**
- **Global compliance strategy**
- **Privacy by Design (PbD) Strategy**
- Initial core privacy team/leaders
- Advisory/Legal Partnerships
- Basic Data and Vendor Inventory
- **Internal Processes and Policies with stakeholders**
- Privacy Statements

Privacy Program Evolution



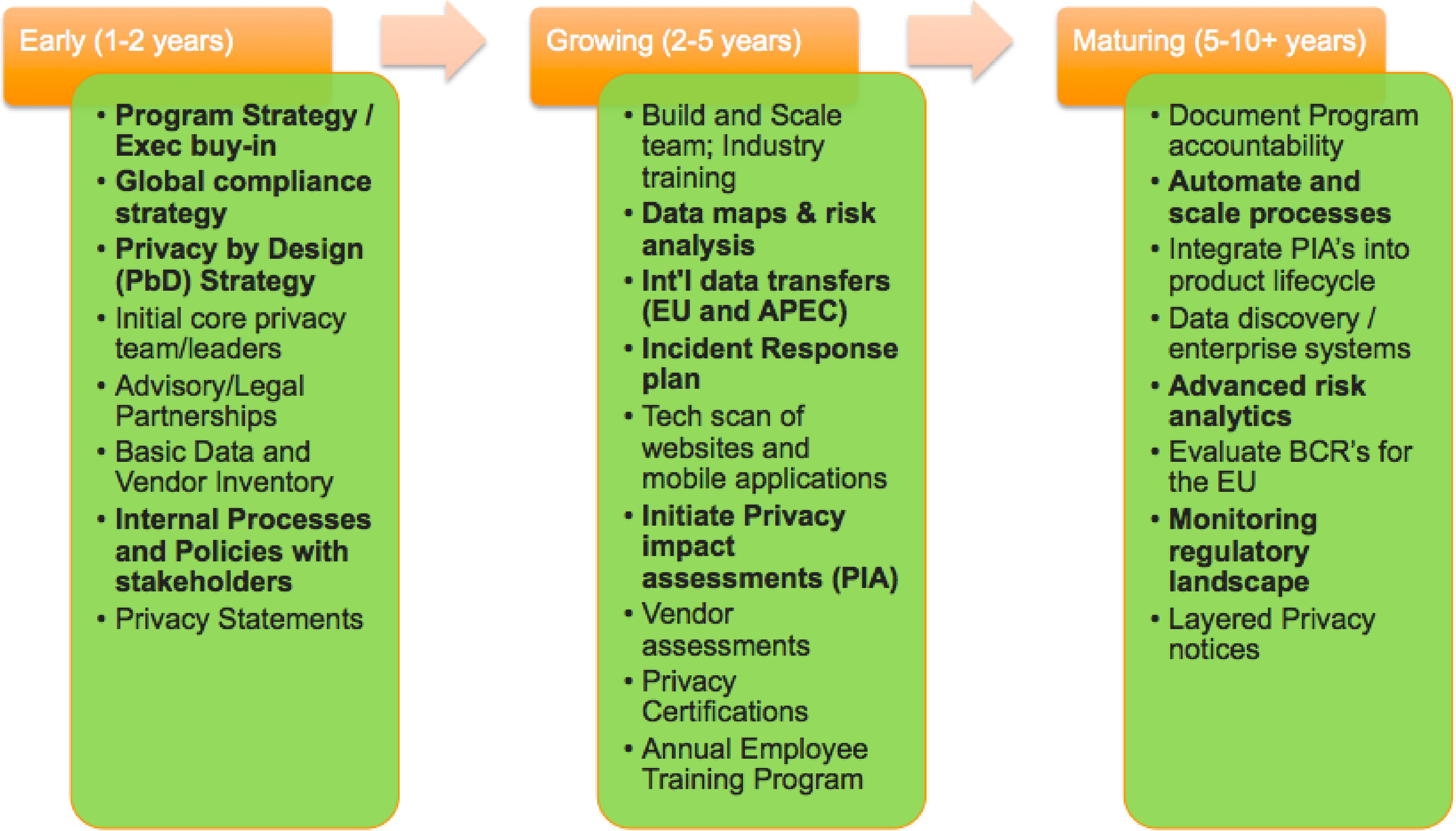
Early (1-2 years)

- **Program Strategy / Exec buy-in**
- **Global compliance strategy**
- **Privacy by Design (PbD) Strategy**
- Initial core privacy team/leaders
- Advisory/Legal Partnerships
- Basic Data and Vendor Inventory
- **Internal Processes and Policies with stakeholders**
- Privacy Statements

Growing (2-5 years)

- Build and Scale team; Industry training
- **Data maps & risk analysis**
- **Int'l data transfers (EU and APEC)**
- **Incident Response plan**
- Tech scan of websites and mobile applications
- **Initiate Privacy impact assessments (PIA)**
- Vendor assessments
- Privacy Certifications
- Annual Employee Training Program

Privacy Program Evolution



Early (1-2 years)

- **Program Strategy / Exec buy-in**
- **Global compliance strategy**
- **Privacy by Design (PbD) Strategy**
- Initial core privacy team/leaders
- Advisory/Legal Partnerships
- Basic Data and Vendor Inventory
- **Internal Processes and Policies with stakeholders**
- Privacy Statements

Growing (2-5 years)

- Build and Scale team; Industry training
- **Data maps & risk analysis**
- **Int'l data transfers (EU and APEC)**
- **Incident Response plan**
- Tech scan of websites and mobile applications
- **Initiate Privacy impact assessments (PIA)**
- Vendor assessments
- Privacy Certifications
- Annual Employee Training Program

Maturing (5-10+ years)

- Document Program accountability
- **Automate and scale processes**
- Integrate PIA's into product lifecycle
- Data discovery / enterprise systems
- **Advanced risk analytics**
- Evaluate BCR's for the EU
- **Monitoring regulatory landscape**
- Layered Privacy notices

Privacy Assessment Benchmarking Study

POWERING TRUST IN THE DATA ECONOMY

Privacy Assessment Study Overview

Survey Background

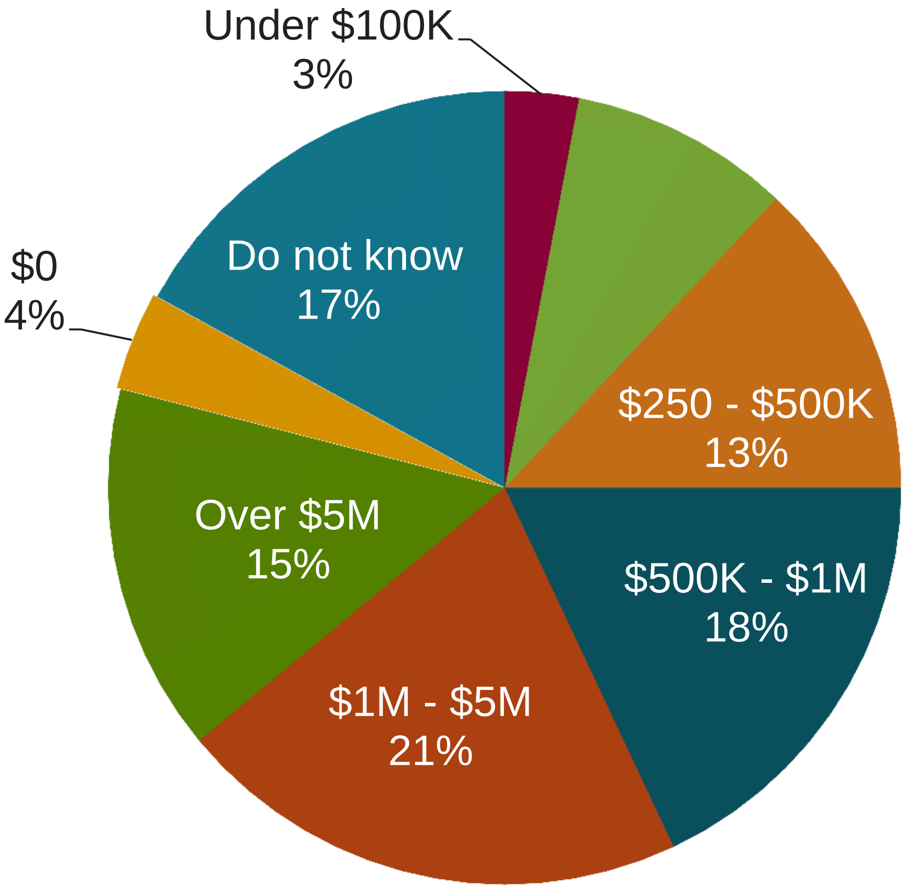
- Online survey conducted December 9 - 15, 2014
- External sample used (not TRUSTe database)
- Participants blind to TRUSTe being the survey sponsor
- External consultant used to administer and analyze
- 203 respondents from large organizations (>1,000 employees)

Respondent Background

- Participants screened to ensure part of company’s privacy function
- Companies ranging in size from 1,000 to 75,000+ (approximately equal distribution)
- US multi-nationals, across wide range of industries

Nearly Half (45%) of Privacy Budgets over $1M Annually

What is the approximate total 2014 privacy budget for your company, including employee salary / benefits, external resources, and external software and tools?



Average = $3.3M

Median = $1.0M

Company Size is a Key Driver

- 1K to 5K Employees, Ave = $1.8M
- Over 75K Employees, Ave = $3.3M

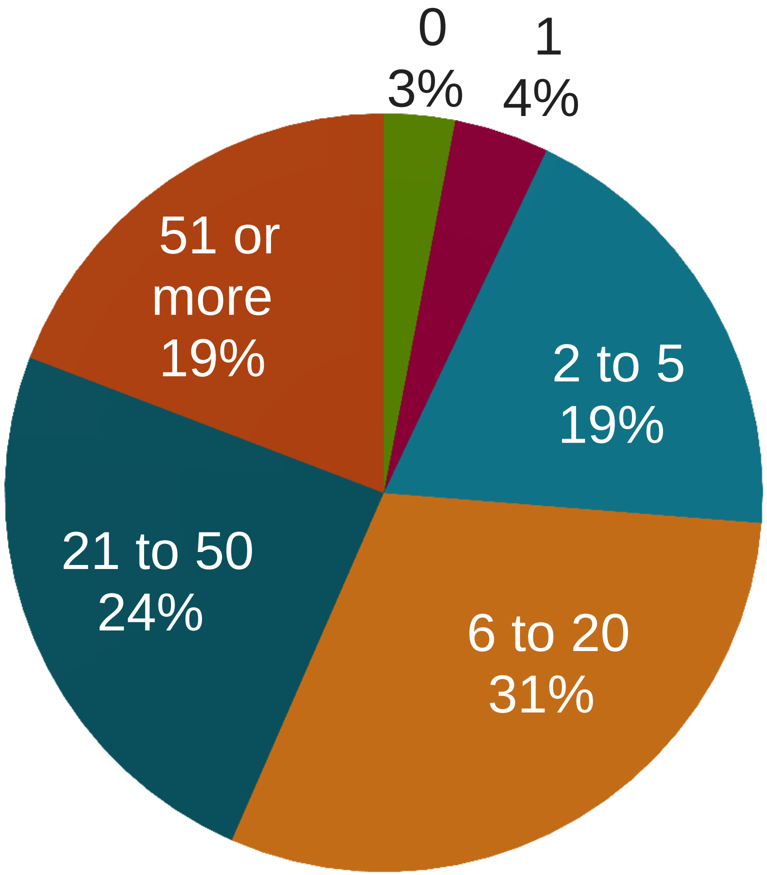
Mature companies 2.5x more likely to have > $1M budget

Calculations exclude “Do Not Know”

n=203

Wide Range of Privacy Team Sizes

How many individuals are involved in your organization's privacy initiatives as their primary responsibility over the course of this year (internal employees and external contractors)?



Average = 28 people

Median = 18 people

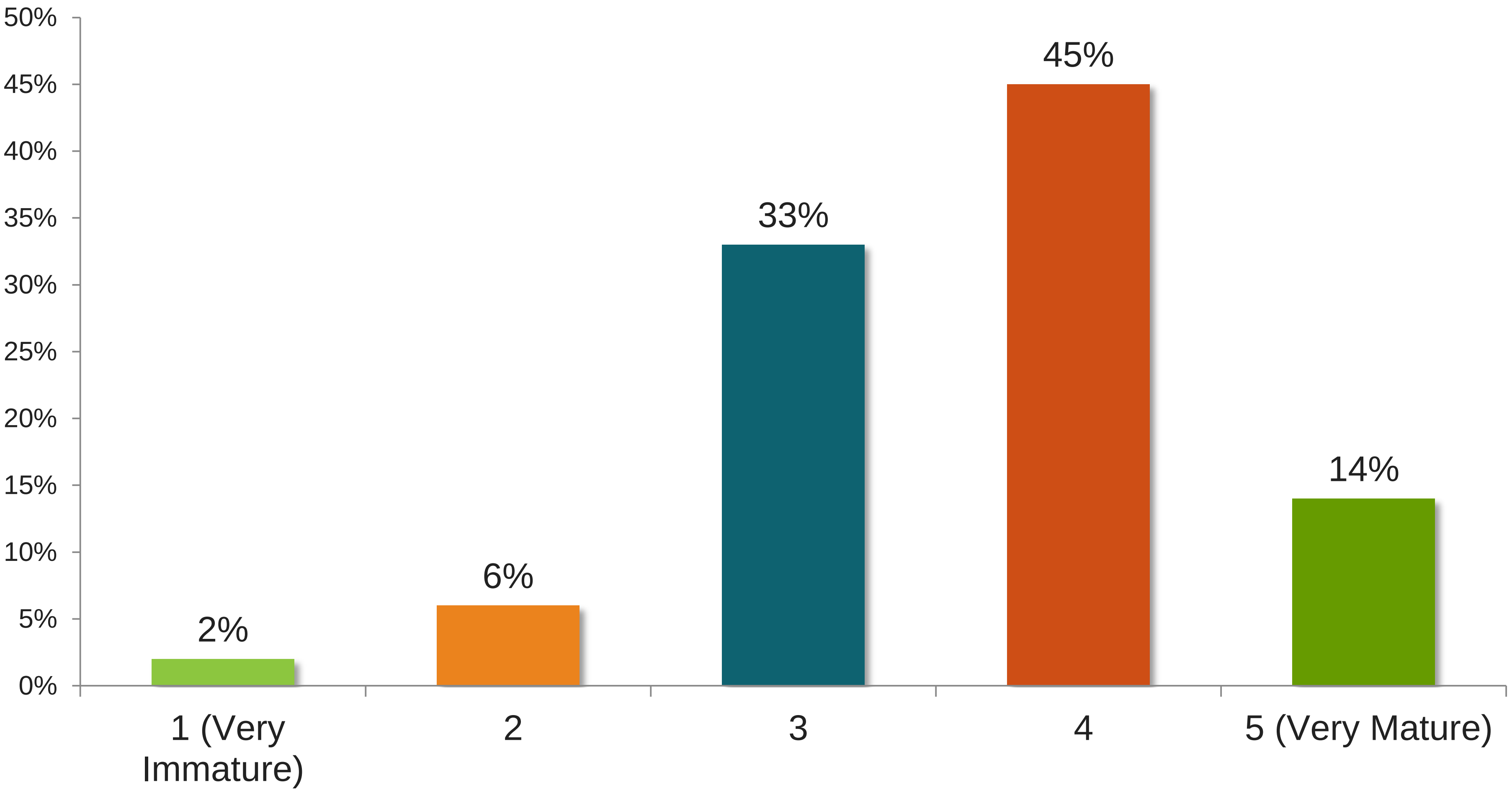
Company Size is a Key Driver

- 1K to 5K Employees, Ave = 18
- Over 75K Employees, Ave = 50

n=203

Company Privacy Maturity

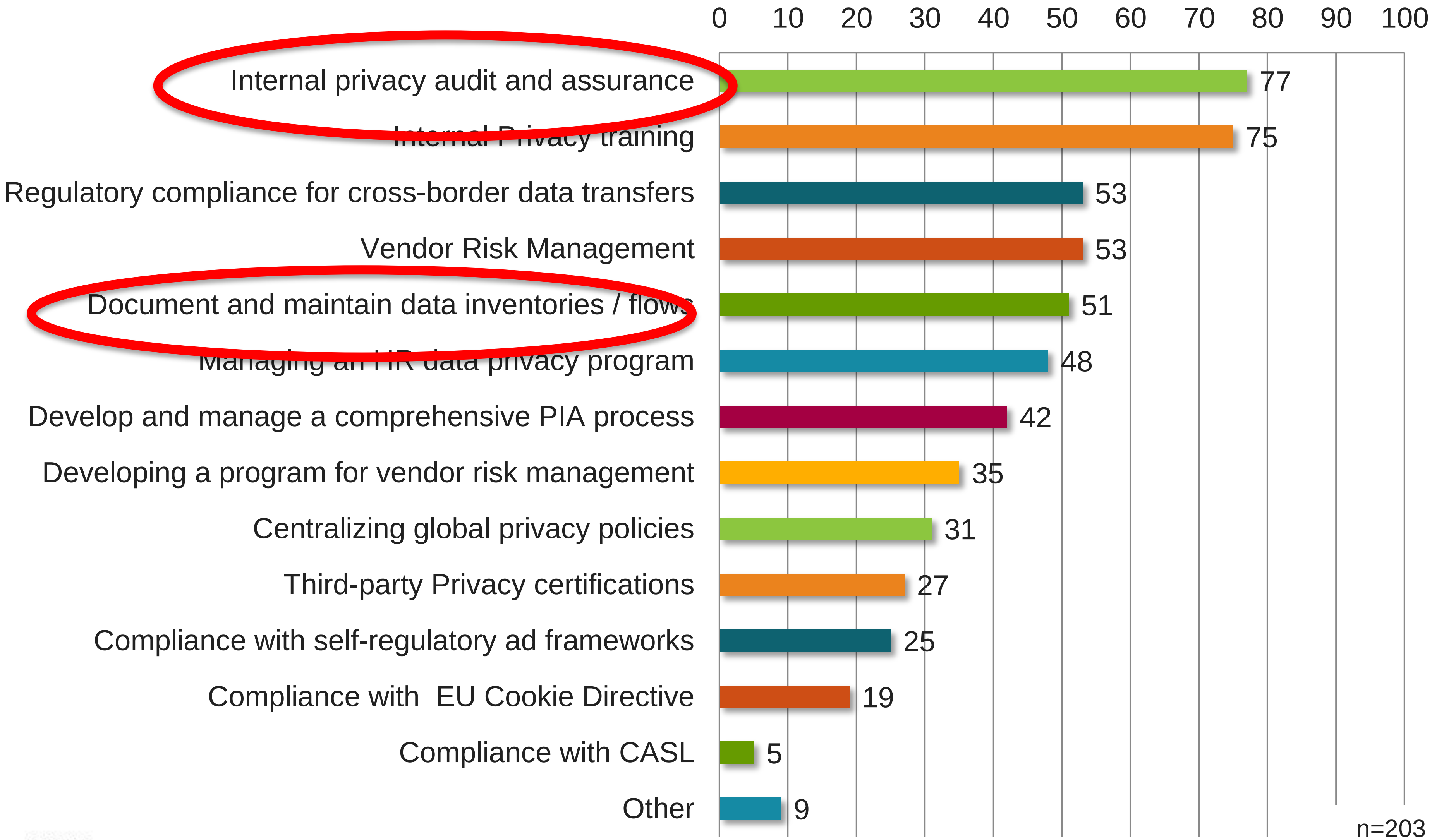
How would you rate the maturity of your company's privacy program?



n=203

Assessment Practices

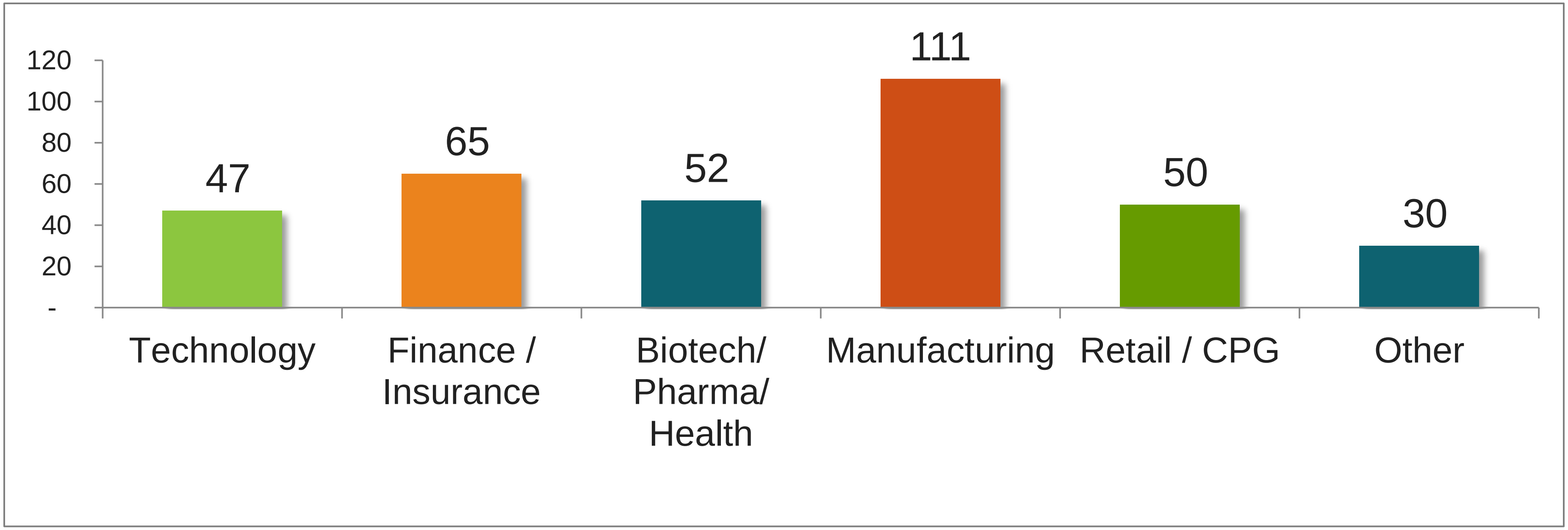
What are your organization's 3 highest priority privacy projects for 2015?



n=203

Privacy Impact Assessment (PIA) Volume Analysis

- Company Average = 59 per year
- Median = 12 per year
- Privacy Maturity Key Driver of Volume – Very Mature = 2x Average
- Company Size Not a Key Driver of Volume



Assessment Benchmarking Summary

1. Conducting Privacy Assessments top priority for many companies
2. Average company conducts 59 PIAs per year
3. 1/3 across offline online and employee data
4. Assessments take a long time – 28 days, 285 hours on average
5. Managing respondents and analysis are top drivers to length
6. Assessments are labor intensive – 56 employees company-wide
7. Budget and team's time top inhibitors to doing more assessments
8. Internal systems, email, and spreadsheets most common tools
9. Individual assessments cost $17K - $71K (length & rate)
10. Annual costs from $210K to $4.2M (volume, length, & rate)

Key Privacy Use Cases

TRUSTe Data Privacy Management Solutions

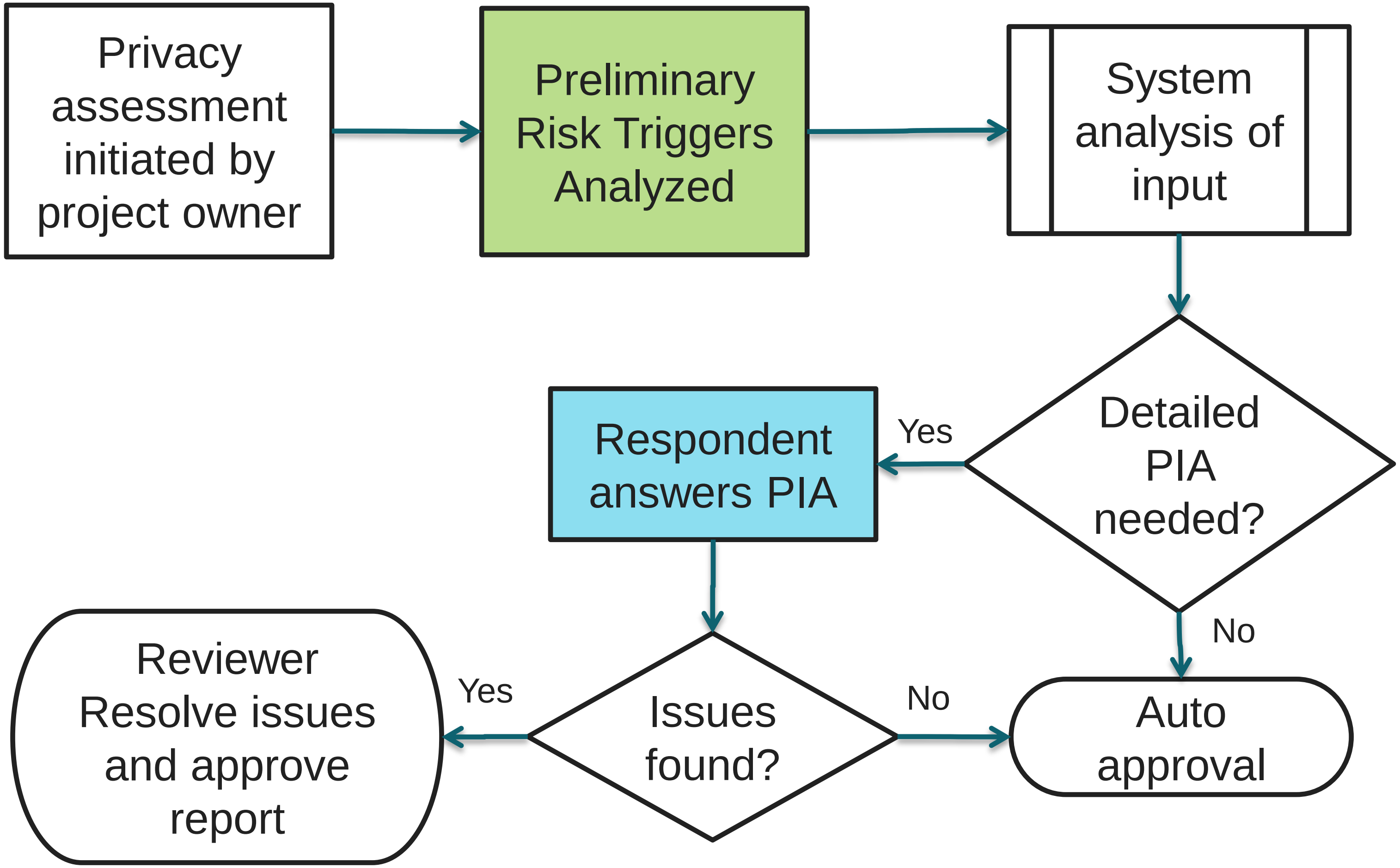
Data Privacy Management Use Cases

Company Type	Use Case
Tech: Computer	Integrated privacy impact assessments into product lifecycle process
Medical Services	Discovering and building business process data flows for privacy risk analysis
Energy and Petroleum	Evaluating data transfers across global enterprise

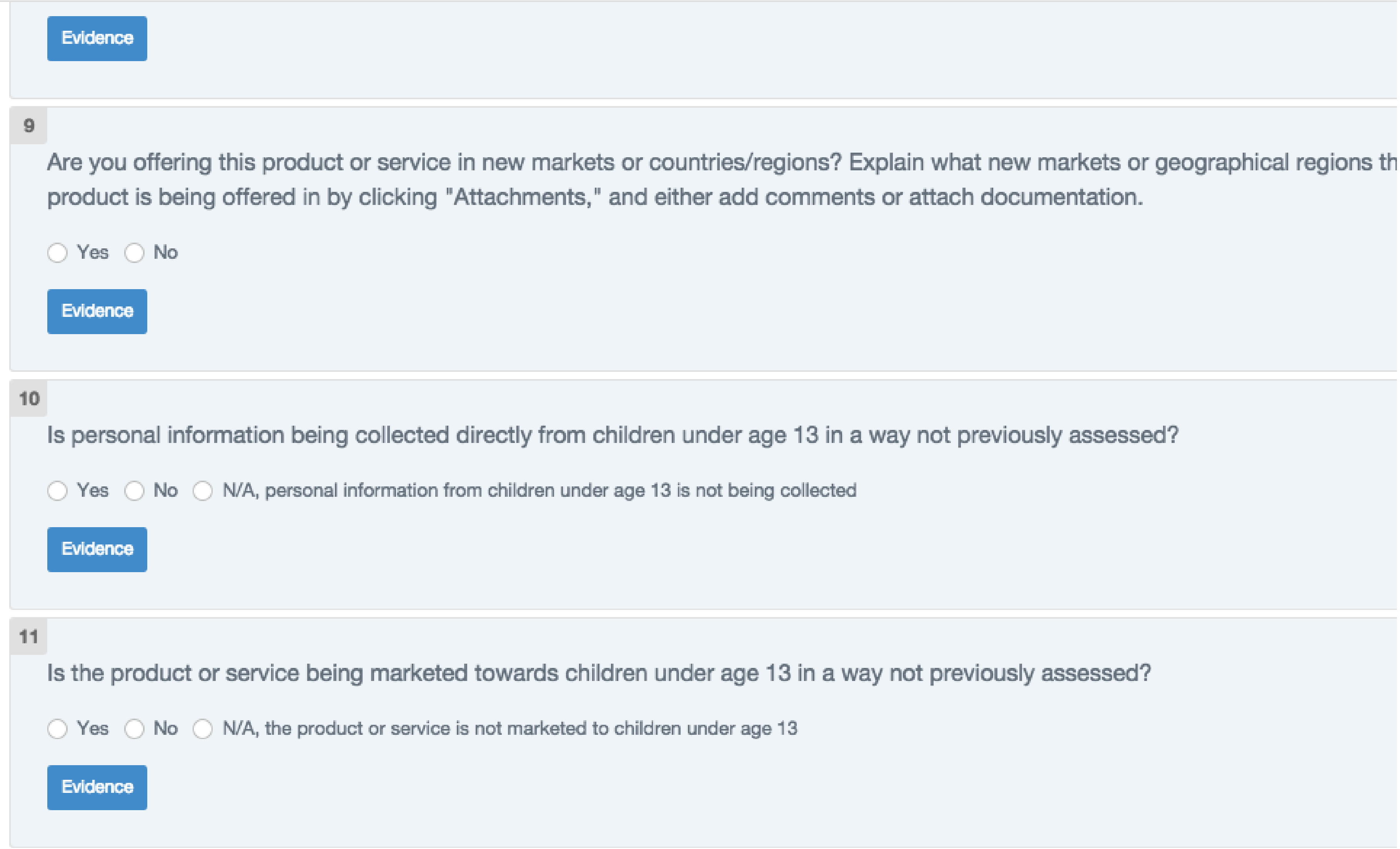
Use Case:
Automating Privacy Impact Assessments

TRUSTe Data Privacy Management Solutions

Privacy Impact Assessment (PIA) Automation


Privacy assessment initiated by project owner
Preliminary Risk Triggers Analyzed
System analysis of input
Detailed PIA needed?
Yes
Respondent answers PIA
No
Issues found?
Yes
Reviewer Resolve issues and approve report
No
Auto approval

Privacy Threshold Assessment



Evidence

9

Are you offering this product or service in new markets or countries/regions? Explain what new markets or geographical regions th product is being offered in by clicking "Attachments," and either add comments or attach documentation.

○ Yes ○ No

Evidence

10

Is personal information being collected directly from children under age 13 in a way not previously assessed?

○ Yes ○ No ○ N/A, personal information from children under age 13 is not being collected

Evidence

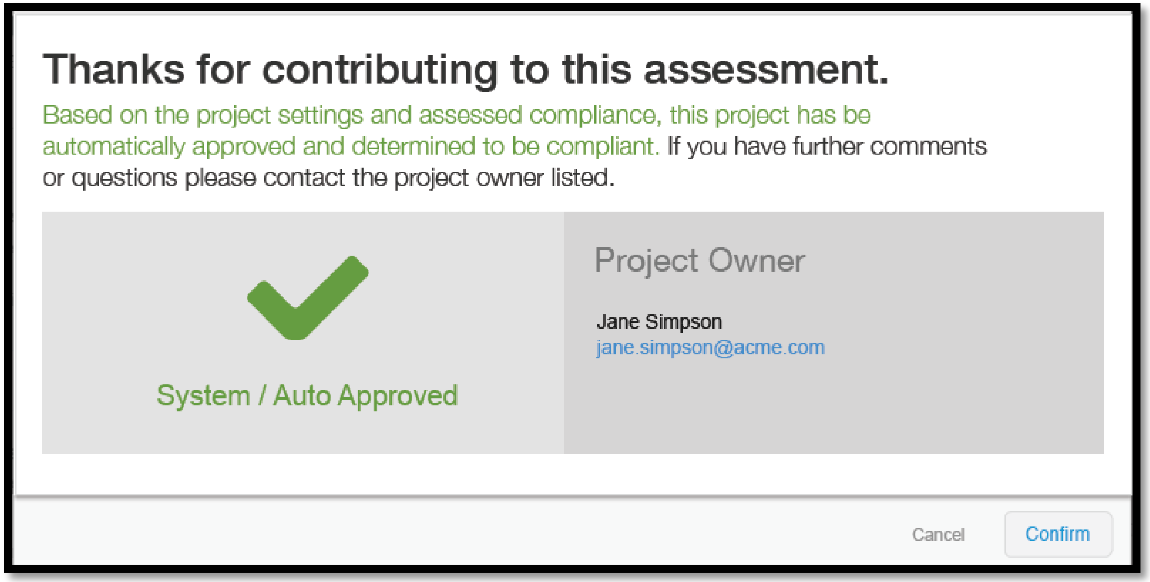
11

Is the product or service being marketed towards children under age 13 in a way not previously assessed?

○ Yes ○ No ○ N/A, the product or service is not marketed to children under age 13

Evidence

Auto approval if no issues



Thanks for contributing to this assessment.

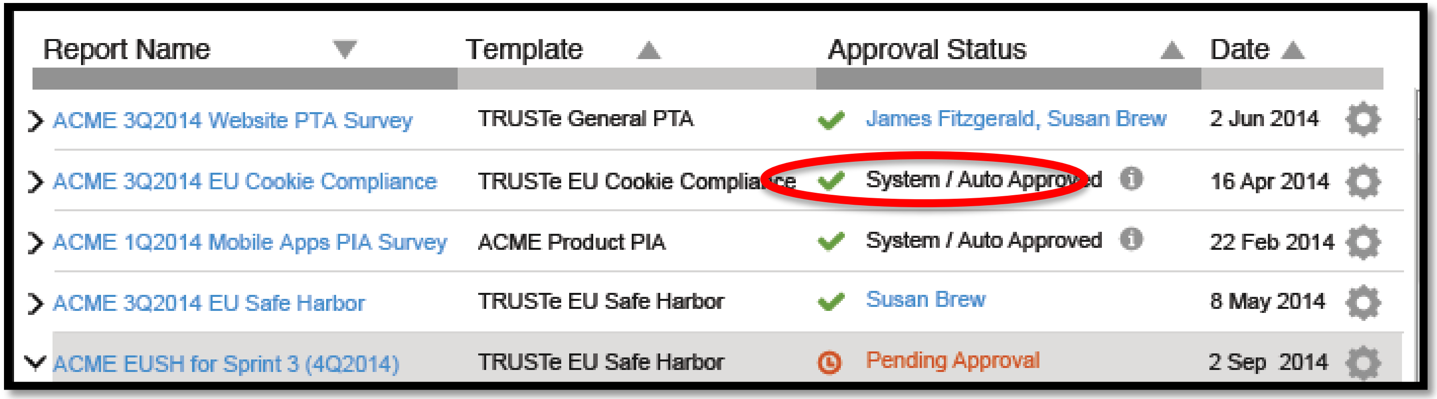
Based on the project settings and assessed compliance, this project has be automatically approved and determined to be compliant. If you have further comments or questions please contact the project owner listed.

✓ System / Auto Approved

Project Owner

Jane Simpson
jane.simpson@acme.com

Answers to preliminary questions may result in platform approval – no need for privacy review

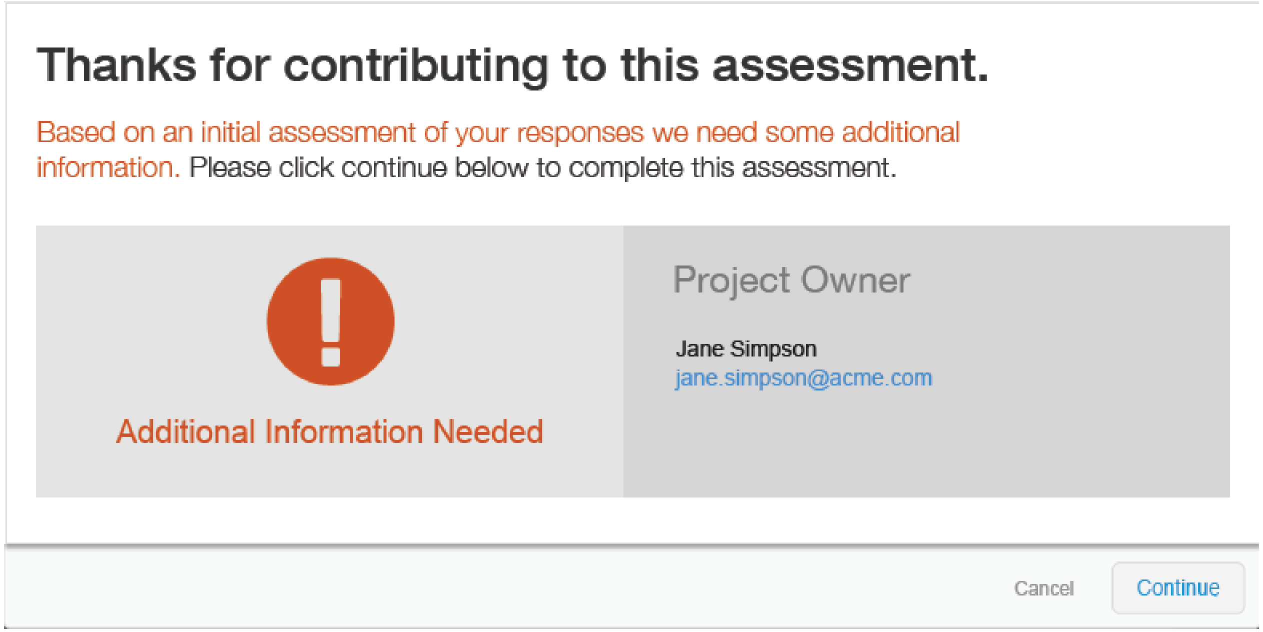


Report Name ▼	Template ▲	Approval Status ▲	Date ▲
› ACME 3Q2014 Website PTA Survey	TRUSTe General PTA	✓ James Fitzgerald, Susan Brew	2 Jun 2014
› ACME 3Q2014 EU Cookie Compliance	TRUSTe EU Cookie Compliance	✓ System / Auto Approved ⓘ	16 Apr 2014
› ACME 1Q2014 Mobile Apps PIA Survey	ACME Product PIA	✓ System / Auto Approved ⓘ	22 Feb 2014
› ACME 3Q2014 EU Safe Harbor	TRUSTe EU Safe Harbor	✓ Susan Brew	8 May 2014
⌄ ACME EUSH for Sprint 3 (4Q2014)	TRUSTe EU Safe Harbor	Pending Approval	2 Sep 2014

System approved assessments are available if needed

Presence of Risks Triggers Deeper PIA

Answers to preliminary questions may result in user being presented a more detailed PIA review



Thanks for contributing to this assessment.

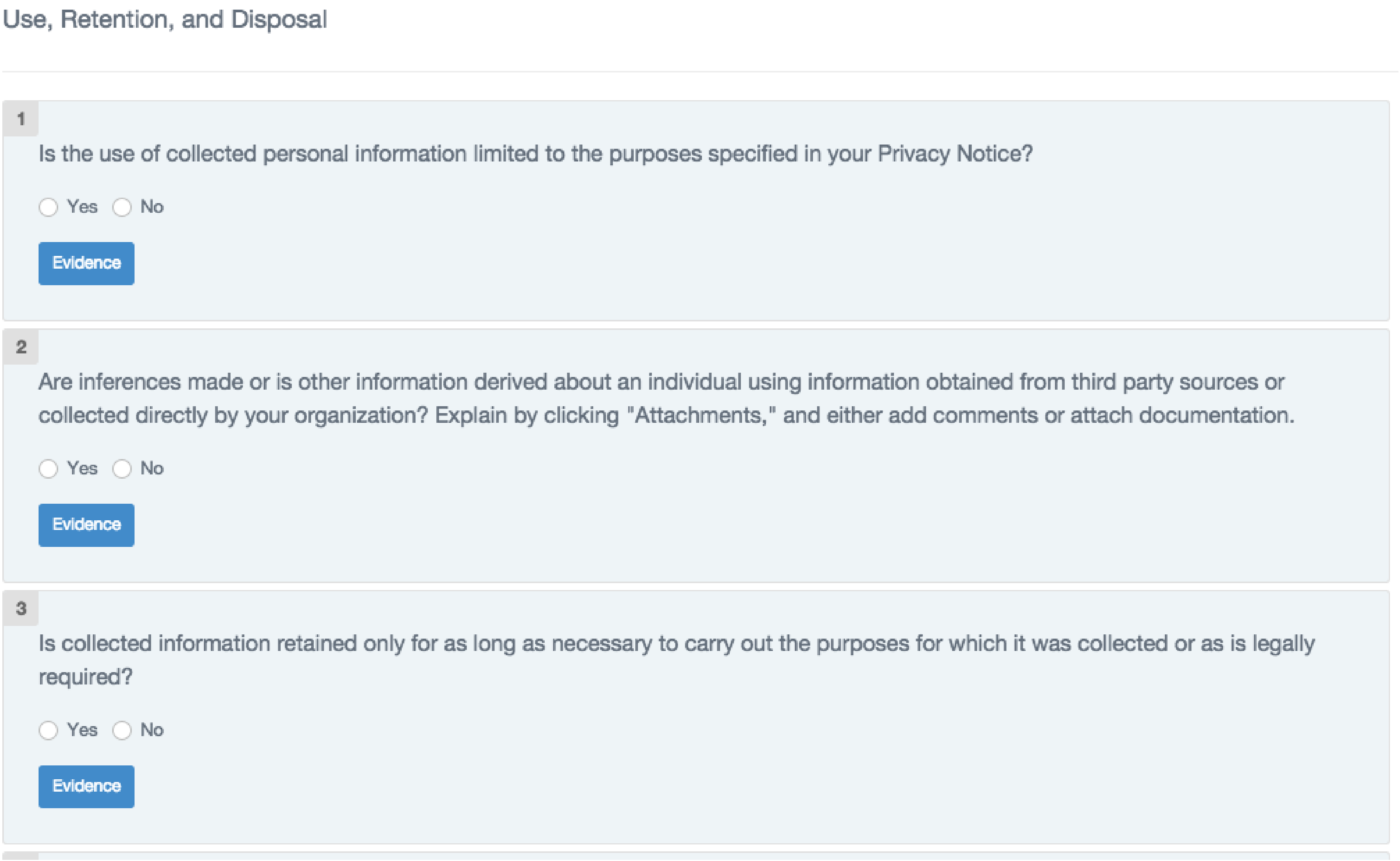
Based on an initial assessment of your responses we need some additional information. Please click continue below to complete this assessment.

Additional Information Needed

Project Owner

Jane Simpson
jane.simpson@acme.com

Privacy Impact Assessment (PIA)



Use, Retention, and Disposal

1

Is the use of collected personal information limited to the purposes specified in your Privacy Notice?

○ Yes ○ No

2

Are inferences made or is other information derived about an individual using information obtained from third party sources or collected directly by your organization? Explain by clicking "Attachments," and either add comments or attach documentation.

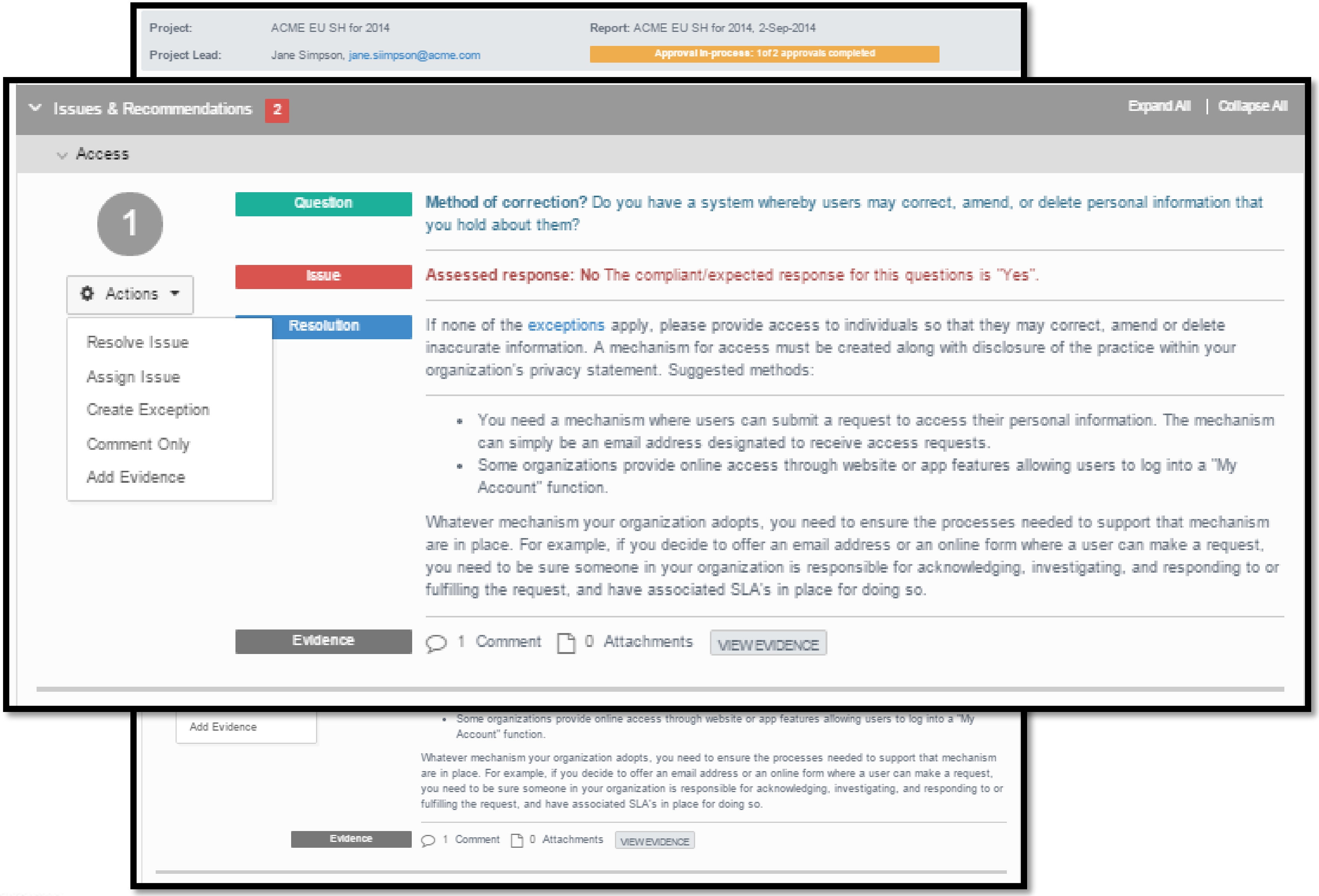
○ Yes ○ No

3

Is collected information retained only for as long as necessary to carry out the purposes for which it was collected or as is legally required?

○ Yes ○ No

Privacy Analyst Risk Administration



Project: ACME EU SH for 2014

Project Lead: Jane Simpson, jane.siimpson@acme.com

Report: ACME EU SH for 2014, 2-Sep-2014

Approval in-process: 1of2 approvals completed

Question: Method of correction? Do you have a system whereby users may correct, amend, or delete personal information that you hold about them?

Issue: Assessed response: No The compliant/expected response for this questions is "Yes".

Resolution: If none of the exceptions apply, please provide access to individuals so that they may correct, amend or delete inaccurate information. A mechanism for access must be created along with disclosure of the practice within your organization's privacy statement. Suggested methods:

- You need a mechanism where users can submit a request to access their personal information. The mechanism can simply be an email address designated to receive access requests.
- Some organizations provide online access through website or app features allowing users to log into a "My Account" function.

Whatever mechanism your organization adopts, you need to ensure the processes needed to support that mechanism are in place. For example, if you decide to offer an email address or an online form where a user can make a request, you need to be sure someone in your organization is responsible for acknowledging, investigating, and responding to or fulfilling the request, and have associated SLA's in place for doing so.

Evidence: 1 Comment 0 Attachments VIEW EVIDENCE

Add Evidence

- Some organizations provide online access through website or app features allowing users to log into a "My Account" function.

Whatever mechanism your organization adopts, you need to ensure the processes needed to support that mechanism are in place. For example, if you decide to offer an email address or an online form where a user can make a request, you need to be sure someone in your organization is responsible for acknowledging, investigating, and responding to or fulfilling the request, and have associated SLA's in place for doing so.

Evidence 1 Comment 0 Attachments VIEW EVIDENCE

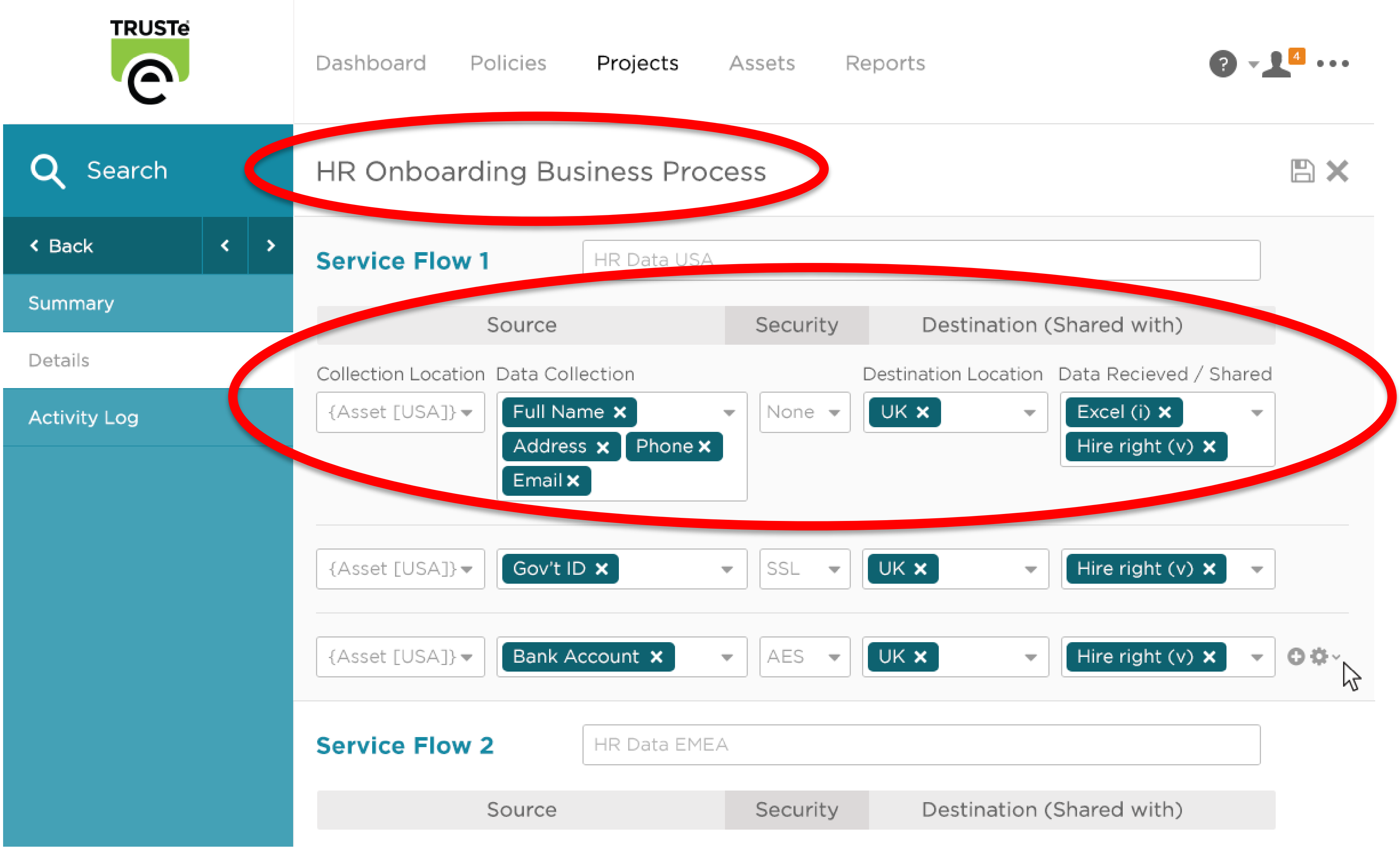
Use Case:
Data Flow Analysis

TRUSTe Data Privacy Management Solutions

Objectives

- Describe business processes for full data lifecycle
  - Source (collection)
  - Intermediaries (hosting and processing)
  - Destinations (data transfers, vendors)
- Describe a policy for risk analysis
  - Global data transfer
  - Data sensitivity (PII)
  - Data protection strategy (security)

Data Flow Management



HR Onboarding Business Process

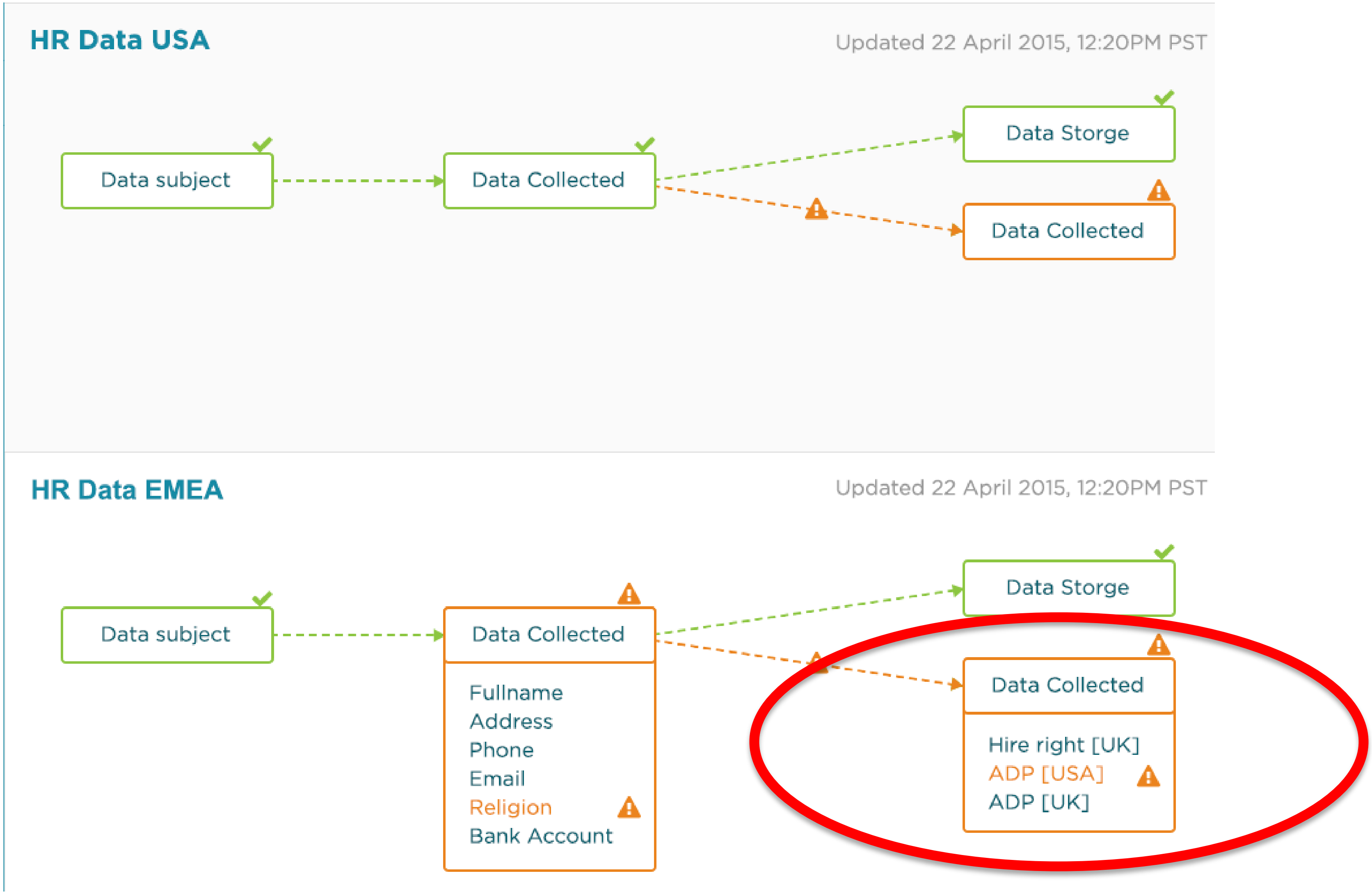
Service Flow 1: HR Data USA

Source		Security	Destination (Shared with)	
Collection Location	Data Collection		Destination Location	Data Recieved / Shared
{Asset [USA]}	Full Name Address Phone Email	None	UK	Excel (i) Hire right (v)
{Asset [USA]}	Gov't ID	SSL	UK	Hire right (v)
{Asset [USA]}	Bank Account	AES	UK	Hire right (v)

Service Flow 2: HR Data EMEA

Source	Security	Destination (Shared with)

Data Flow Policy Analysis



HR Data USA

Updated 22 April 2015, 12:20PM PST

Data subject ✓

Data Collected ✓

Data Storge ✓

Data Collected ⚠

HR Data EMEA

Updated 22 April 2015, 12:20PM PST

Data subject ✓

Data Collected ⚠

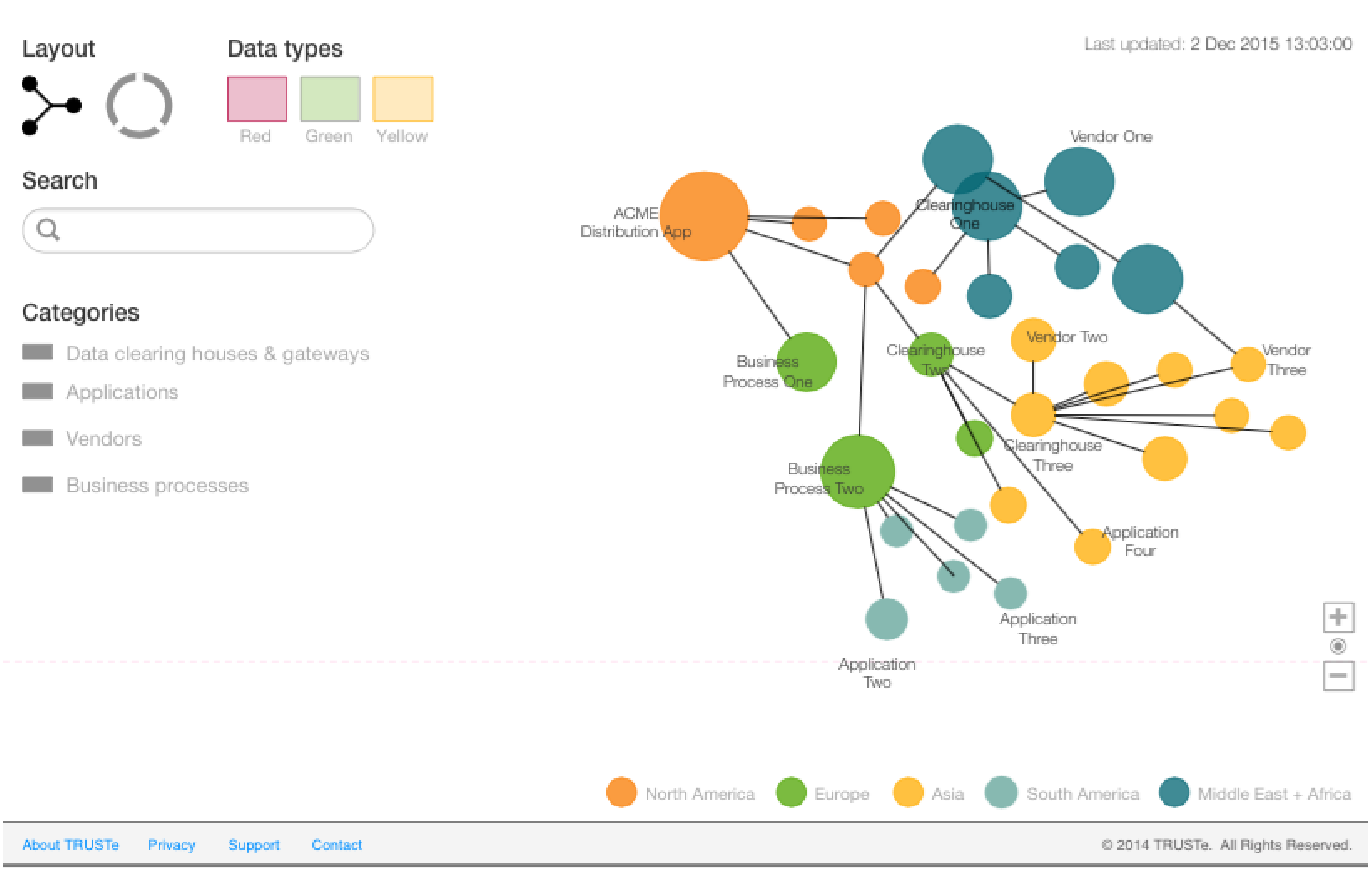
Fullname
Address
Phone
Email
Religion ⚠
Bank Account

Data Storge ✓

Data Collected ⚠

Hire right [UK]
ADP [USA] ⚠
ADP [UK]

Aggregate Analysis



Layout

Data types

🟥 Red 🟩 Green 🟨 Yellow

Search

Categories

- ▬ Data clearing houses & gateways
- ▬ Applications
- ▬ Vendors
- ▬ Business processes

Last updated: 2 Dec 2015 13:03:00

● North America ● Europe ● Asia ● South America ● Middle East + Africa

About TRUSTe Privacy Support Contact

© 2014 TRUSTe. All Rights Reserved.

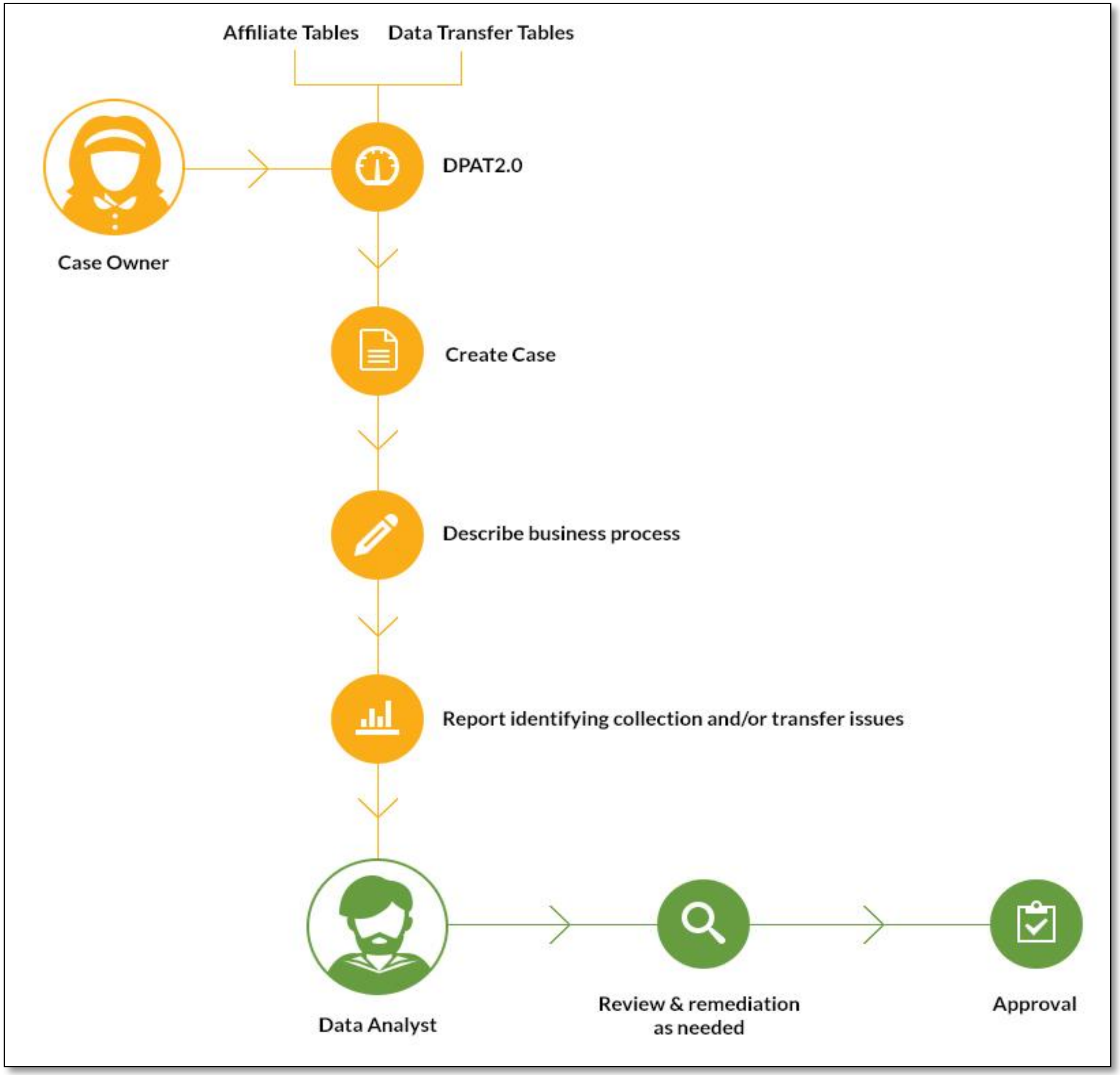
Use Case:
Evaluating Global Data Transfers

TRUSTe Data Privacy Management Solutions

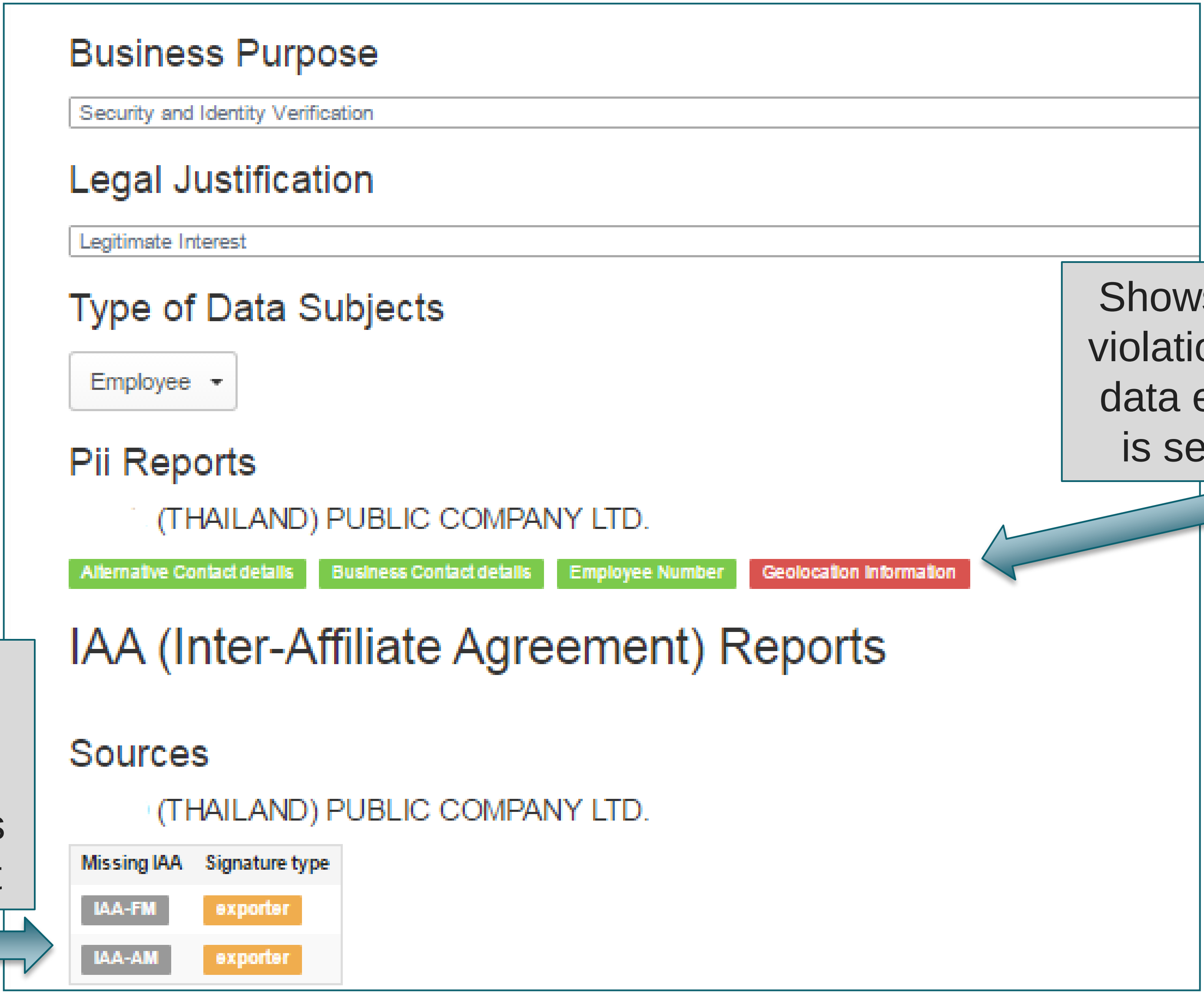
Data Transfer Management

- Large global energy company
- Located in 80 countries
- 1,000 project managers requesting 5,000 data transfer requests per year
- Goals:
  - Use system to automate decision and remove ‘routine use cases’
  - Inform users of when requested data is high risk
  - Operationalize legal data transfer layers
  - Involve privacy analyst on high risk areas for manual intervention

Data Transfer Analysis


Affiliate Tables
Data Transfer Tables
Case Owner
DPAT2.0
Create Case
Describe business process
Report identifying collection and/or transfer issues
Data Analyst
Review & remediation as needed
Approval

Data Transfer Analysis



Business Purpose

Security and Identity Verification

Legal Justification

Legitimate Interest

Type of Data Subjects

Employee ▾

Pii Reports

(THAILAND) PUBLIC COMPANY LTD.

Alternative Contact details | Business Contact details | Employee Number | Geolocation Information

IAA (Inter-Affiliate Agreement) Reports

Sources

(THAILAND) PUBLIC COMPANY LTD.

Missing IAA	Signature type
IAA-FM	exporter
IAA-AM	exporter

Shows policy violation when data element is selected

Highlights where proper agreements do not exist

Thank You

POWERING TRUST IN THE DATA ECONOMY

TRUSTe Data Privacy Management (DPM) Solutions

DPM Services

Assessments

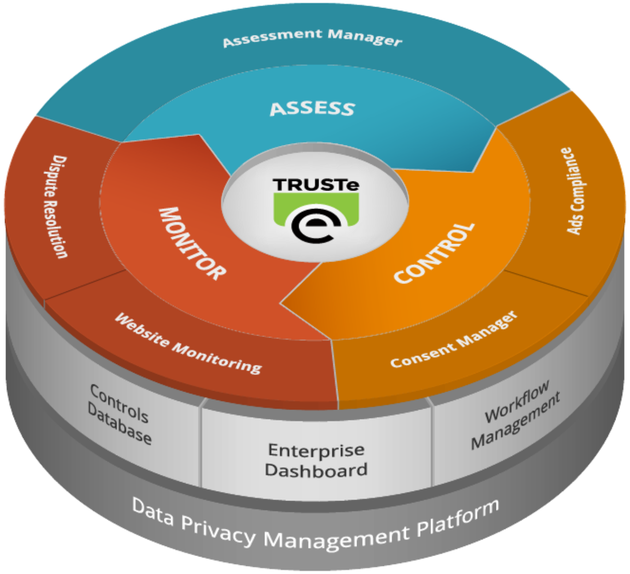
- EU Safe Harbor
- Privacy Impact Assessments
- Custom Engagements

TRUSTe Certified Privacy

Certifications

- Apps, Cloud, Websites
- APEC, COPPA, EDAA

DPM Platform

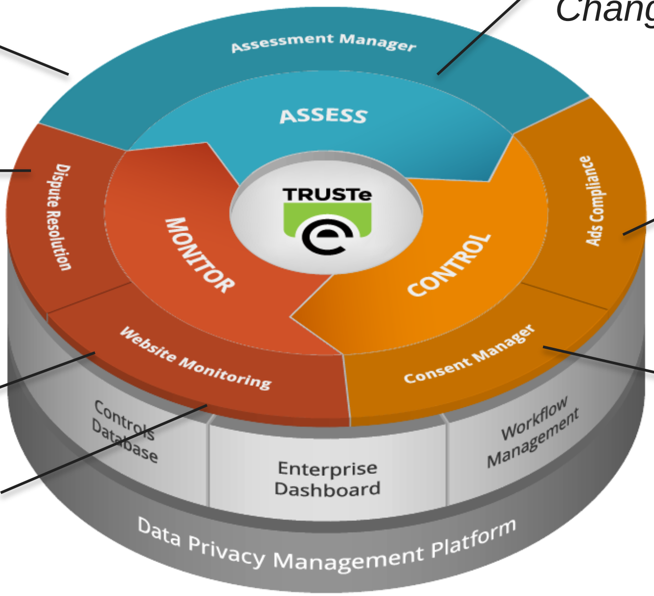


Extensive Expertise - Proven Methodology - Leading Technology

TRUSTe Data Privacy Management Platform

Enterprise Privacy Automation

Privacy Assessments, Compliance Controls, and Monitoring Tools



Data Flow Mapping

Compliance Reviews, Gap Analysis, Change Management

Safe Harbor Dispute Handling

DAA / EDAA OBA Compliance

EU Cookie Directive Compliance

Website Analysis

Mobile App Analysis

Proven SaaS Technology
Self Service & Managed Service Options