BUILD ON

Application Privacy Assessment

Privacy Workshop

Date

Name
Title
Microsoft Corporation

Microsoft | Services

Workshop Objectives

Our goals today

- Briefly review Microsoft's approach to Privacy
- Confirm customer and consultant alignment on assessment scope and expected outcomes
- Conduct a high-level review of your business and privacy risk

Workshop Agenda

- Privacy Concerns
- Data Protection
- Privacy Assessment Approach
- High Level Review

BUILD ON

Privacy Concerns

Microsoft | Services

Consumer Concerns about Privacy

Organizations are accumulating unprecedented amounts of data on individuals

- Data can be stolen, lost or misused

Inappropriate or careless use of technology puts Privacy at risk

- Software designed to identify and profile individuals for monetary gain
- Poor software design and implementation
  - Most software does not consider privacy aspects
- Weak or non-existent security controls

Organizational Concerns about Data Security and Privacy

2008 Data Breach Statistics

- Average cost of an incident was $6.6 million US, a 2.5% increase over 2007
- Largest percentage of incidents (87%) is due to lost or stolen laptops or media
- Average customer churn attributable to Data Breaches was 3.6%
  - 6% for financial services industry

Source: Ponemon study, “Cost of a Data Breach”, Feb 2009
http://www.encryptionreports.com/

Organizational Concerns about Data Security and Privacy (cont.)

Data Retention

- Accidental misuse of data in violation of privacy policies and legislation
- E-Discovery in civil litigation cases
- Loss or theft of data
  - No breaches on data you don't keep
  - 66% of Data Breaches in 2008 involved data that was not known to reside on the affected system at the time of the incident

Source: "2008 Verizon Data Breach Investigations Report. http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf"

And if That was not Enough …..

Industrial espionage, theft of intellectual property

Need to comply with an increasingly complex/changing regulatory environment:

- EUDPD 95/46/EC compliant national laws
- State Laws: Data Breach Notification
- GLBA
- COPPA
- FCRA/FACTA
- HIPAA

BUILD ON

Data Protection

Microsoft | Services

Data Governance

Is the exercise of decision-making and authority for the management of data assets

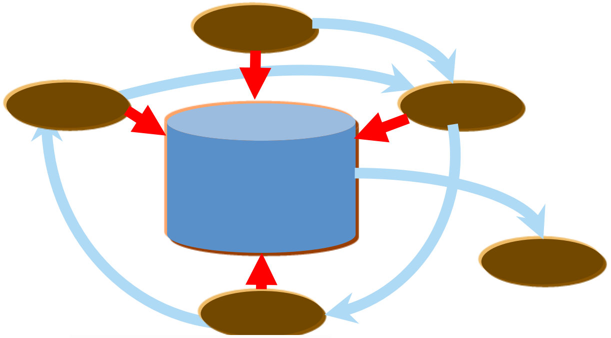
Encompasses the people, processes, and IT required for consistent and proper handling of data across the organization

Is different from IT Governance: IT Governance is about the IT infrastructure whereas Data Governance is about the data

Data Governance helps organizations focus on the specific data elements that need to be protected

The Components of the Technology Framework

Information Lifecycle



Data Protection Principles

Technology Domains

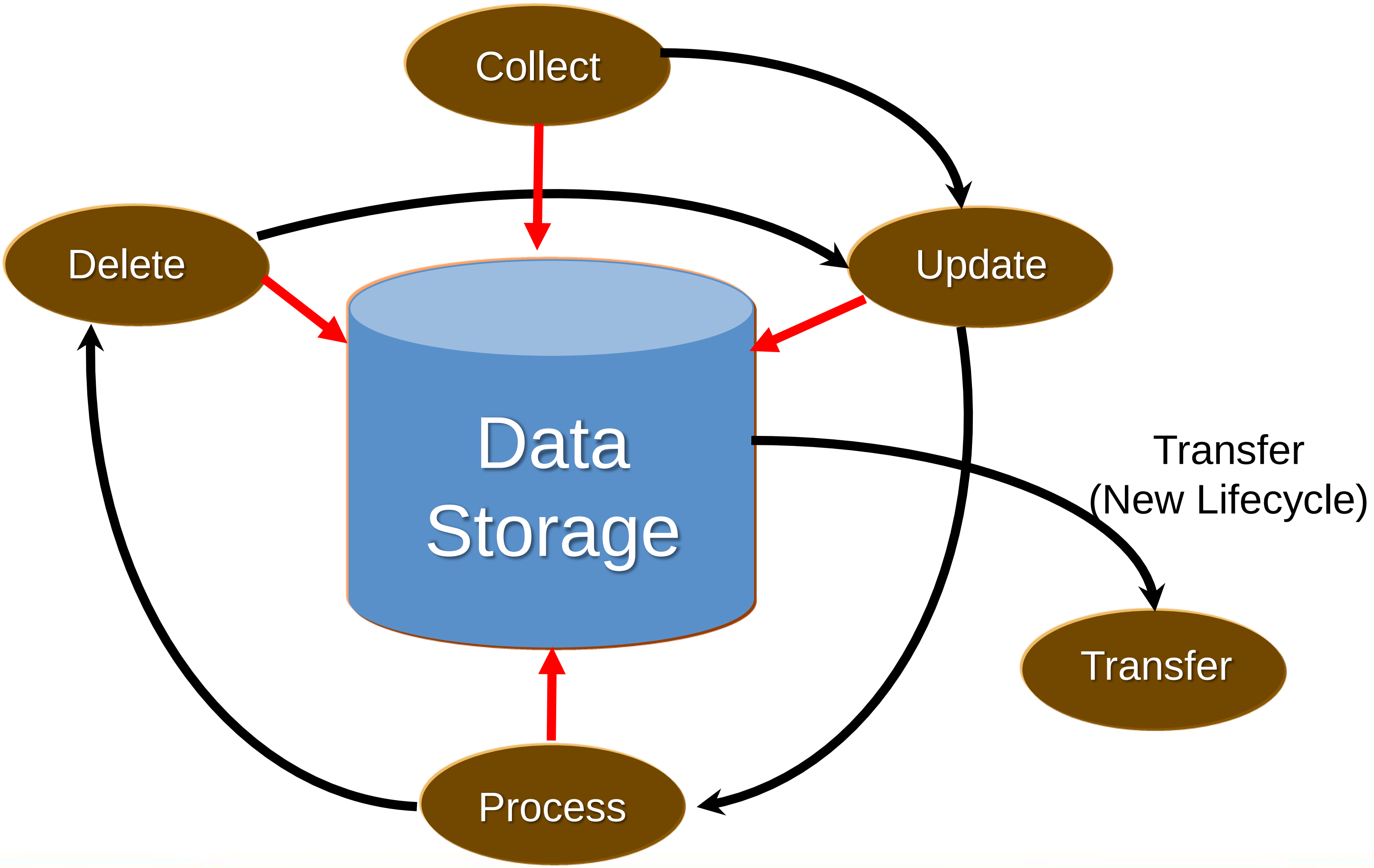
Secure Infrastructure

Identity and Access control

Information Protection

Auditing and reporting

Information Lifecycle



Data Protection Principles

Inspired by OECD* principles of privacy

“Translated” into data protection language

- Detailed by organization specific policies and goals
- Aimed at achieving objectives of:
  - Confidentiality
  - Integrity
  - Availability
  - Compliance

*Organization for Economic Cooperation and Development

The Four Principles of Data Protection

1. Honor policies throughout the confidential data lifespan
2. Minimize risk of unauthorized access or misuse of confidential data
3. Minimize impact of confidential data loss
4. Document applicable controls and demonstrate their effectiveness

First Data Protection Principle

Honor policies throughout the confidential data lifespan

- Data privacy policies are available in digital form
- Private and other sensitive data is tagged with policy associated classification and attributes
- Where appropriate, mechanisms enable individuals to access, understand and manage their private data as well as the policies pertaining to it

Second Data Protection Principle

Minimize risk of unauthorized access or misuse of confidential data

- Permanently tag sensitive data with governing attributes such as policies, access and usage history, and contractual terms of use
- Enforce least privilege, role-based access and segmentation to sensitive data
- Set and enforce clear data retention policies
- Prevent data leakage through periodic scanning of data caches

Third Data Protection Principle

Minimize impact of confidential data loss

- Monitor and analyze patterns of usage and access of private data to identify and respond to emerging control threats
- Periodically audit account and sensitive data access rights
- Encrypt sensitive data while in storage and in transit, on all devices and across all connections
- Have incident response and breach notification plans and escalation paths

Fourth Data Protection Principle

Document applicable controls and demonstrate their effectiveness

- Log execution and outcome of critical events in data flows and processing
- Produce an audit trail detailing access and use of private data in compliance with governing policies and controls

Technology Domains

Secure Infrastructure

- Safeguards against malware
- Safeguards against unauthorized access to sensitive info
- Protect data while on the net
- Protect systems from evolving threats

Identity and Access control

- Protect personal information from unauthorized access or use
- Provide management controls for identity, access and provisioning

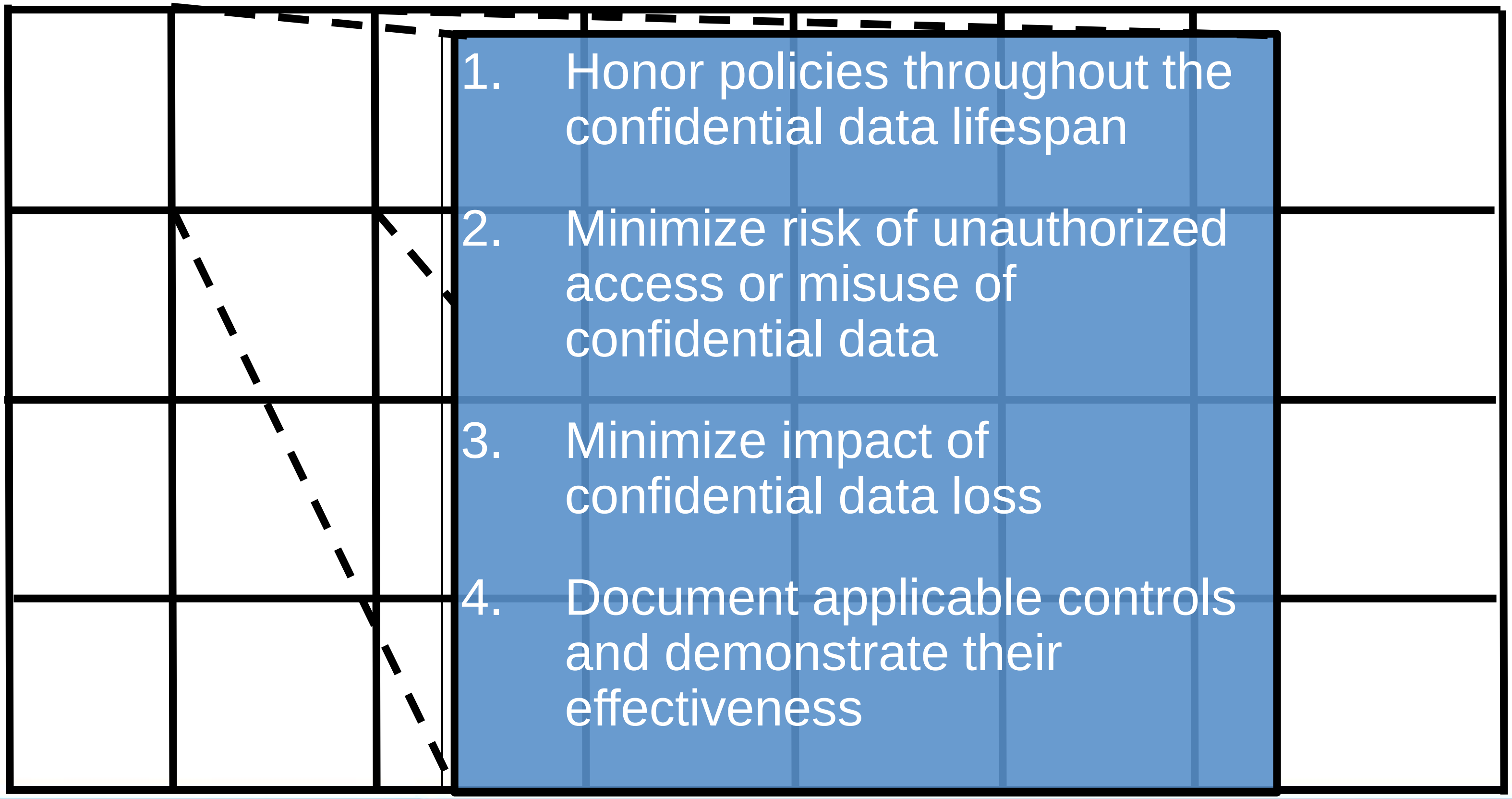
Information Protection

- Protect sensitive personal information in structured databases
- Protect sensitive personal information in unstructured documents, messages and records, through encryption

Auditing and reporting

- Monitor to verify integrity of systems and data
- Monitor to verify compliance with business processes

Gap Analysis



1. Honor policies throughout the confidential data lifespan
2. Minimize risk of unauthorized access or misuse of confidential data
3. Minimize impact of confidential data loss
4. Document applicable controls and demonstrate their effectiveness

BUILD ON

Privacy Assessment Approach

Microsoft | Services

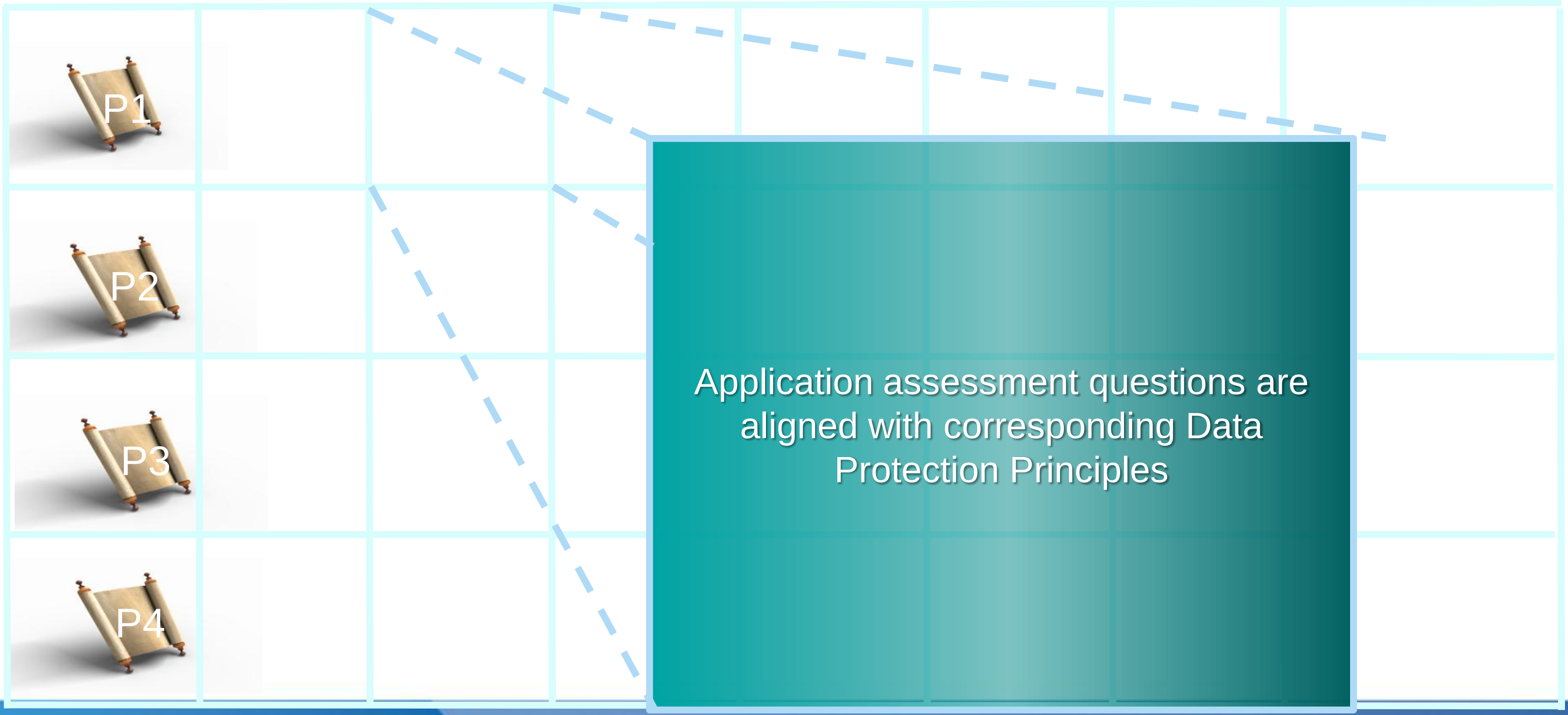
Purpose of Tool

1. Assess compliance of a software application with:

- An organization’s privacy policies and principles
- Software development best practices along the lines of MPSD
- Other industry best practices

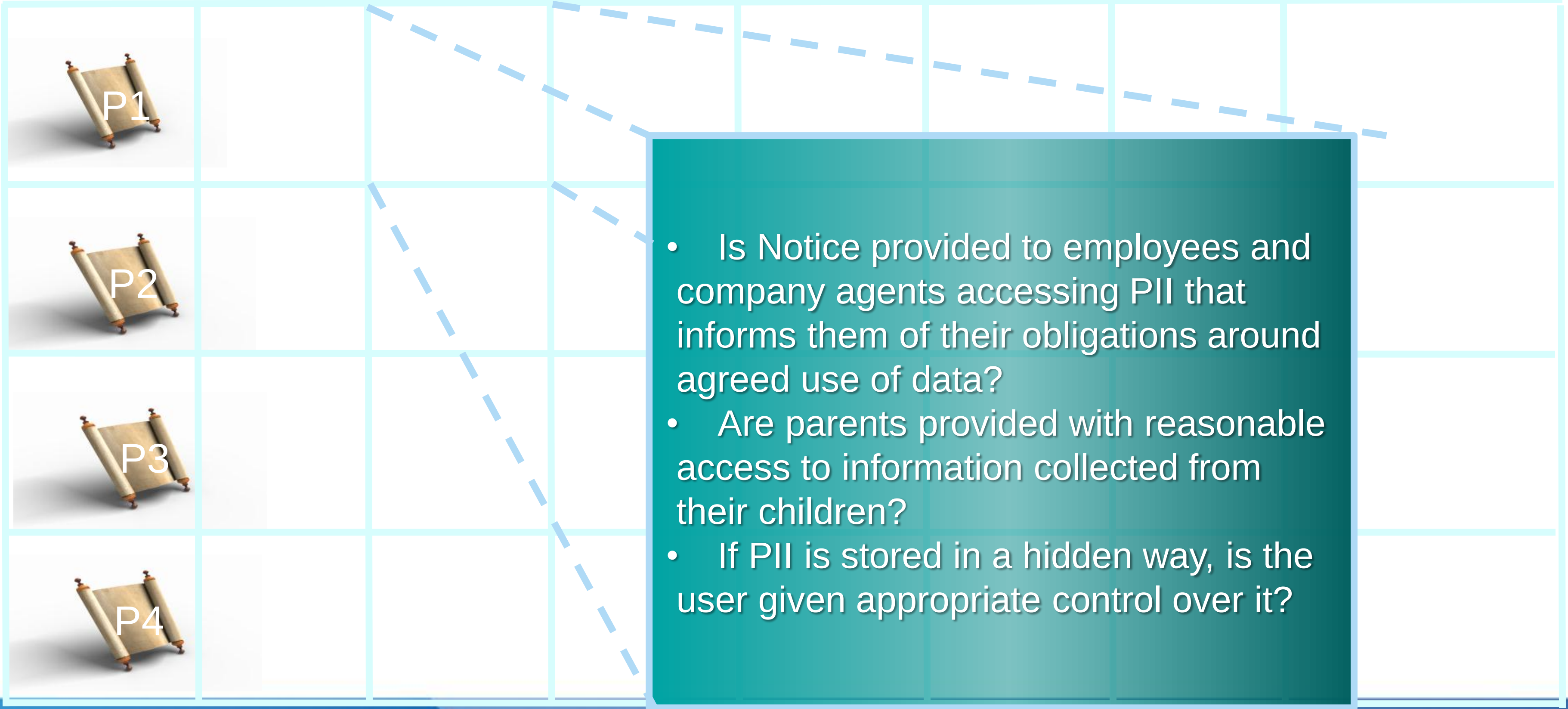
2. Assess privacy-friendliness of the application’s operating environment

Privacy Assessment Tool: App



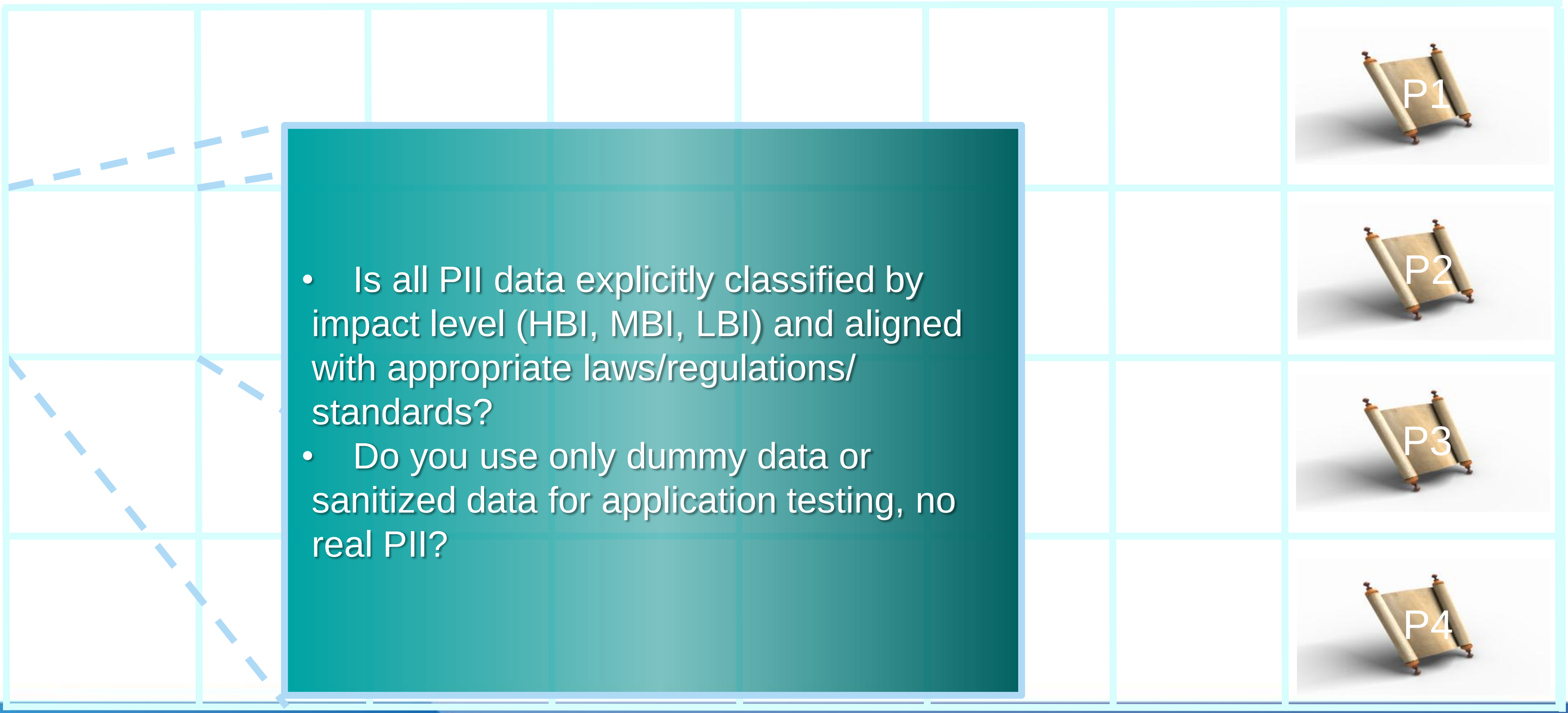
Application assessment questions are aligned with corresponding Data Protection Principles

Privacy Assessment Tool: App



- Is Notice provided to employees and company agents accessing PII that informs them of their obligations around agreed use of data?
- Are parents provided with reasonable access to information collected from their children?
- If PII is stored in a hidden way, is the user given appropriate control over it?

Privacy Assessment Tool: App



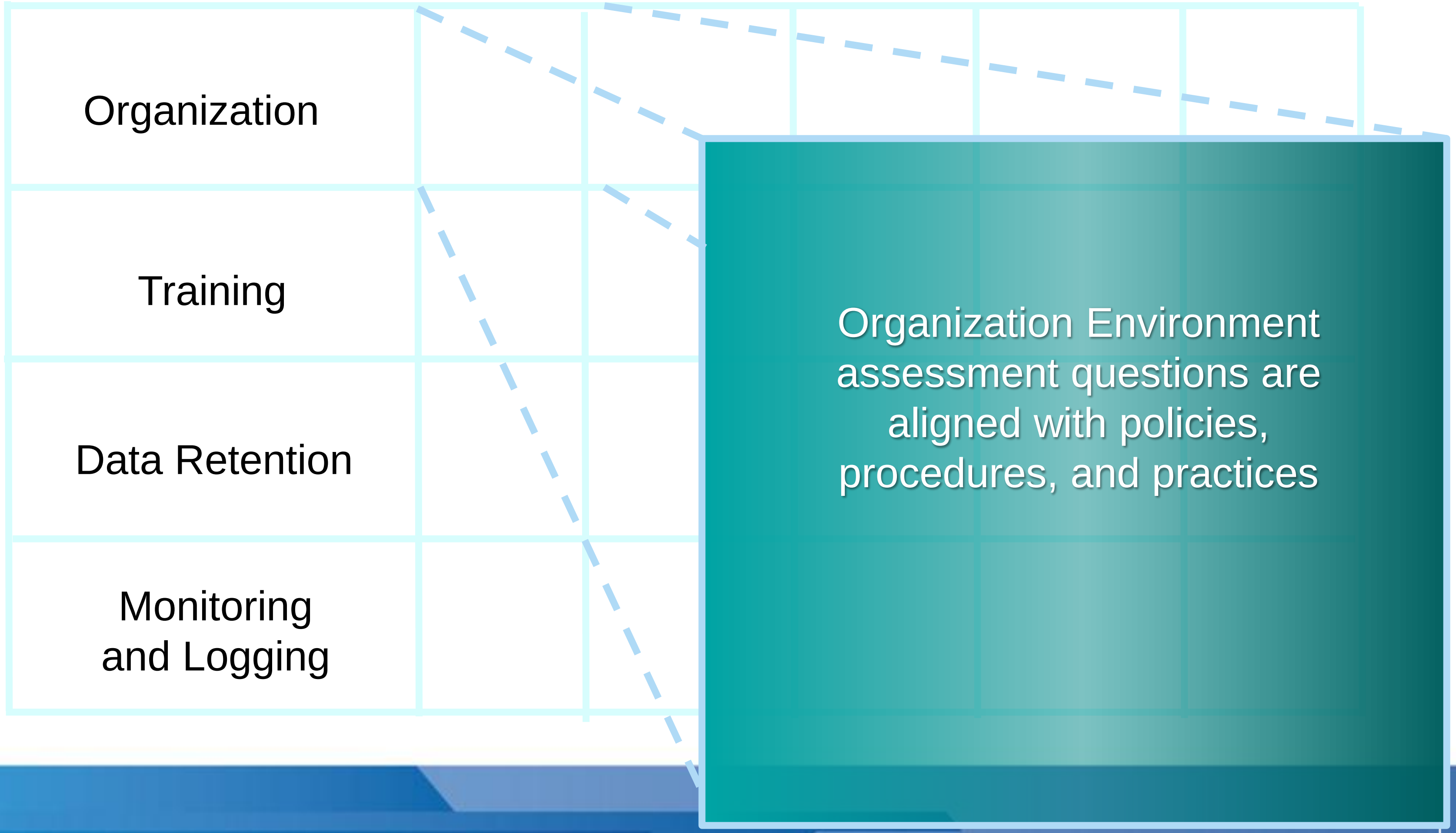
- Is all PII data explicitly classified by impact level (HBI, MBI, LBI) and aligned with appropriate laws/regulations/ standards?
- Do you use only dummy data or sanitized data for application testing, no real PII?

Privacy Assessment Tool: App Env

Email					
Web					
File					
Malware					

Application Environment assessment questions are aligned with corresponding avenues for loss or compromise

Privacy Assessment Tool: Org Env



Organization

Training

Data Retention

Monitoring and Logging

Organization Environment assessment questions are aligned with policies, procedures, and practices

Steps to Gap Analysis Process

Define purpose of flow

Model flow:

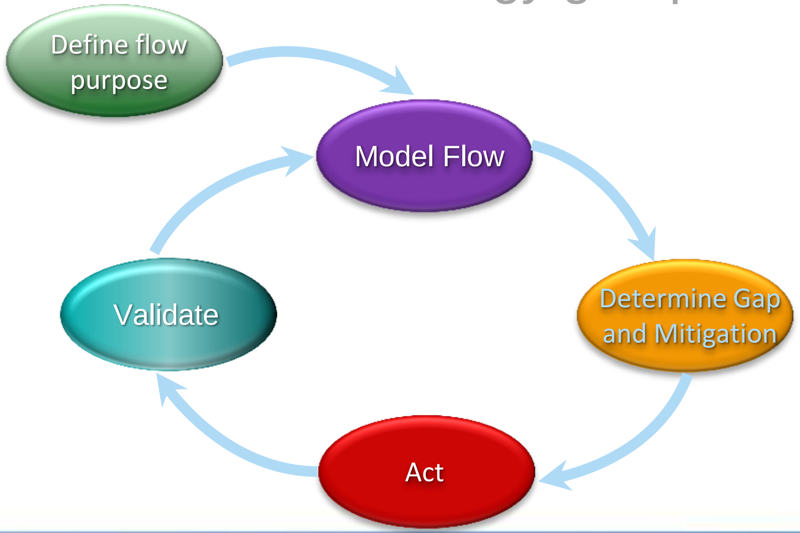
- Construct a diagram of the systems involved
- Match flow to information lifecycle phases

Determine the Gap and mitigation

- How do current technology elements in each of the technology groups meet the principles of data protection?
- Determine gaps and mitigation

Implement mitigation

Validate



BUILD ON

High-level Review

Microsoft | Services

Industry Overview

Regulatory Influences

- What federal, state, local, or industry regulations govern your business?
  - Code of Federal Regulations, Federal Trade Commission, Securities and Exchange Commission, others?

Industry Challenges

- Economic Climate
  - How do minor or significant changes in the economy affect your business?
- Electronic Commerce
  - Channels to market continue to evolve with the latest trend being social networking sites. How has this affected your business?
- Competitive Landscape
  - To what extent is effective use of technology tied to your competitive position?
  - Do customers' views of your privacy posture affect your competitive position?

Map Supporting Technologies to Critical Application

A critical application was chosen as the focus of this assessment

- Do you have a critical asset classification process? What is it?
- How was this application determined to be of critical importance?

Where does the application reside?

Who are the business owners of the application?

What technologies, processes, and people support the application?

- Operating systems, servers, applications, databases, programming languages
- Key policies in place (data classification & handling, privacy consent, etc.)
- Incident management process
- What personnel are authorized to update and/or revise?
- What training is provided to ensure awareness of privacy and data handling?
- What external partners are authorized to access this critical application?

Model Privacy and Data Protection

Define connections to and dependencies of the critical application

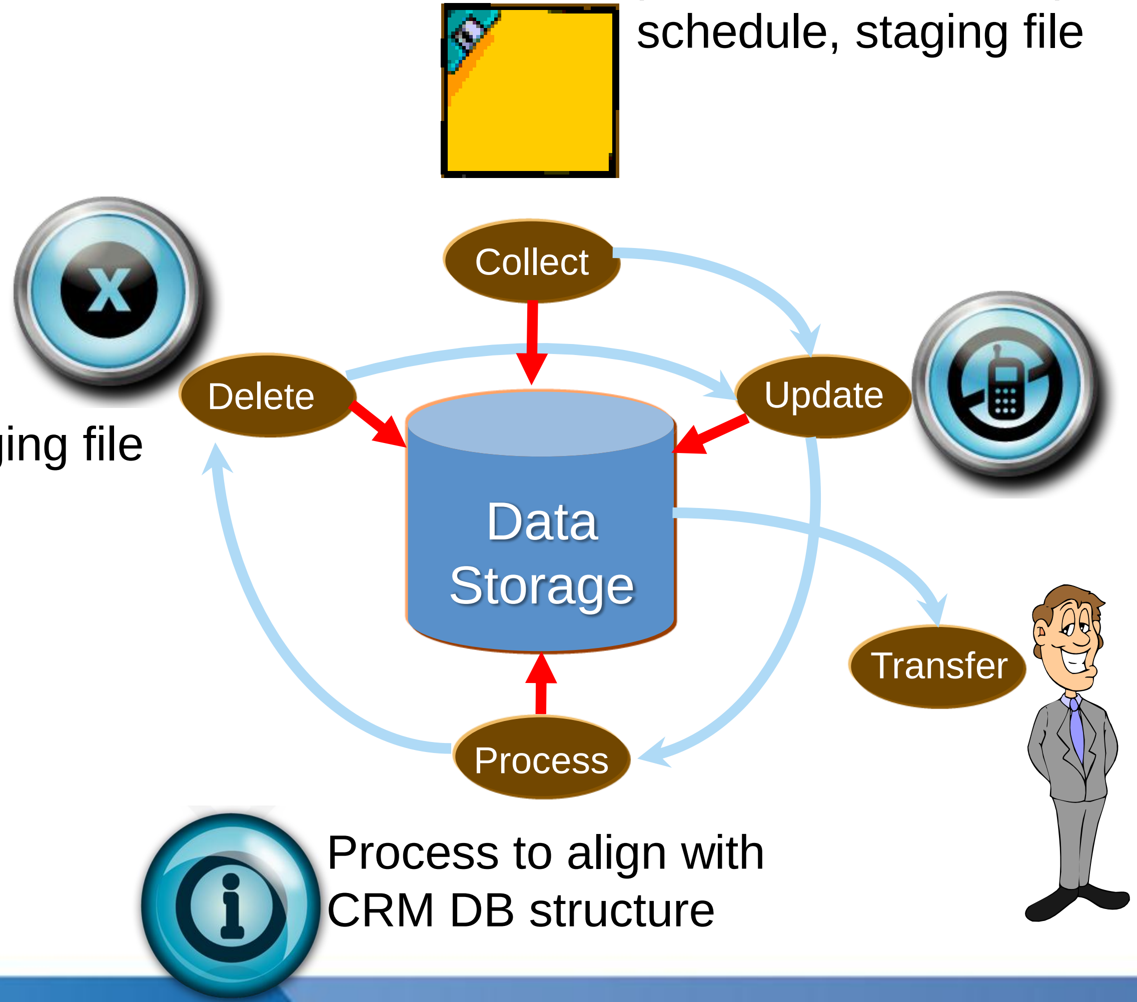
- Create information lifecycle flow diagram to identify the threat paths
- Identify critical processing along the paths
- Identify access categories
- Identify critical dependencies

Identify privacy threats and possible data protection issues

Evaluate potential impact to business functions if critical application is used to facilitate a breach or data leakage

Model the Flow (Example)

Customer lead information is purchased from 3rd party on bi-weekly schedule, staging file



Delete staging file

Reconcile with Do Not Call List, delete unnecessary fields

Process to align with CRM DB structure

Based on sales performance, transfer lead data to top tier sales force

What are the Current Strategies to Mitigate Risk?

Secure Infrastructure

- Safeguards against malware
- Safeguards against unauthorized access to sensitive info
- Protect data while on the net
- Protect systems from evolving threats

Identity and Access control

- Protect personal information from unauthorized access or use
- Provide management controls for identity, access and provisioning

Information Protection

- Protect sensitive personal information in structured databases
- Protect sensitive personal information in unstructured documents, messages and records, through encryption

Auditing and reporting

- Monitor to verify integrity of systems and data
- Monitor to verify compliance with business processes

What are Current Strategies to Protect Data?

1. Honor policies throughout the confidential data lifespan
2. Minimize risk of unauthorized access or misuse of confidential data
3. Minimize impact of confidential data loss
4. Document applicable controls and demonstrate their effectiveness

Other questions?

Microsoft®

Your potential. Our passion.™

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.