Getting to Accountability: Maximizing Your Privacy Program

Presented by:
Terry McQuay,
CIPP/US, CIPP/E, CIPP/C, CIPP/G, and CIPM
Medellin, Colombia
May 28th 2015
Introducing NYMITY

A Data Privacy Research Company

Focus: Dedicated to global data privacy compliance research

Established: 2002

Headquarters: Toronto, Canada

Research: Inventor of several compliance methodologies & frameworks

Funding: Partially funded by government R&D grants

Software Solutions for the Privacy Office

Privacy Management Solutions:

- Nymity Attestor™
- Nymity Benchmarks™
- Nymity Templates™

Compliance Research Solutions:

- Nymity Research™
- Nymity LawTables™
- Nymity MofoNotes®

Nymity is a global data privacy compliance research company specializing in accountability, risk, and compliance software solutions for the Privacy Office. Nymity’s suite of software solutions helps organizations attain, maintain, and demonstrate data privacy compliance.
Nymity’s Accountability Research

Objectives of Today’s Presentation:

To support the launch of the Colombian Accountability Guidelines

To share Nymity’s research and help with:

- Understanding accountability
- Demonstrating that compliance is an accountability outcome
- Getting started
- Discussing when the privacy office is successful
- Demonstrating privacy office success
Accountability

Accountability Defined

“an obligation or willingness to accept responsibility or to account for one's actions“

www.merriam-webster.com/dictionary/accountability

“the obligation of an individual or organization to account for its activities, accept responsibility for them, and to disclose the results in a transparent manner“

www.businessdictionary.com/definition/accountability.html
Accountability is a Privacy Principle

Privacy Framework History

Frameworks Listed Alphabetically

<table>
<thead>
<tr>
<th>Framework</th>
<th>Includes an Accountability Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>AICPA/CICA Generally Accepted Privacy Principles</td>
<td></td>
</tr>
<tr>
<td>APEC Privacy Framework</td>
<td></td>
</tr>
<tr>
<td>AICPA/CICA GAPP Maturity Model</td>
<td></td>
</tr>
<tr>
<td>British Standard BS 10012:2009</td>
<td></td>
</tr>
<tr>
<td>Canadian Standards Association Privacy Principles (Q850)</td>
<td></td>
</tr>
<tr>
<td>Council of Europe Convention 108 EU-US Safe Harbor</td>
<td></td>
</tr>
<tr>
<td>EU Data Protection Directive</td>
<td></td>
</tr>
<tr>
<td>International Standards on the Protection of Personal Data and Privacy (Madrid Resolution)</td>
<td></td>
</tr>
<tr>
<td>ISO 27000 and ISO 27011</td>
<td></td>
</tr>
<tr>
<td>OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data</td>
<td></td>
</tr>
<tr>
<td>Organization of American States (OAS) Preliminary Principles and Recommendations on Data Protection</td>
<td></td>
</tr>
<tr>
<td>Privacy by Design</td>
<td></td>
</tr>
<tr>
<td>UN Guidelines for the Regulation of Computerized Personal Data Files</td>
<td></td>
</tr>
<tr>
<td>US Department of Homeland Security Fair Information Practice Principles (FIPPs)</td>
<td></td>
</tr>
<tr>
<td>US FTC Fair Information Practice Principles (FIPPs)</td>
<td></td>
</tr>
</tbody>
</table>


This chart ranks privacy frameworks based on accountability principles criteria and the date they were published. Accountable organizations maintain compliance and effective privacy programs and can demonstrate both.
Regulators: Accountability includes a Privacy Management Program

Getting Accountability Right with a Privacy Management Program

Purpose
The Office of the Privacy Commissioner of Canada works with organizations to help them develop privacy management programs that meet the requirements of the Personal Information Protection and Electronic Documents Act (PIPEDA). The Office’s Privacy Management Program is a best practice guide.

What is accountability?
Accountability in relation to information protection involves policies and procedures that a minimum, with applicable confidence on the part of service providers for organizations subject to what we expect to see in terms of accountability.

Privacy Management Programme: A Best Practice Guide

Privacy management framework:
Enabling compliance and encouraging good practice

Guía Para la Implementación del Principio de Responsabilidad Demostrada (Accountability) en las Organizaciones

¿QUÉ ES LA RESPONSABILIDAD DEMOSTRADA O ACCOUNTABILITY?

La responsabilidad demostrada (accountability en inglés), un principio que fue recogido en las Guías sobre Protección de la Privacidad y Flujos Transfronterizos de Información (OCDE, 1980, actualizadas en 2010), establece que si una entidad no resalta y trata datos personales, debe ser responsable del cumplimiento efectivo de las medidas que implementan los principios de privacidad y protección de datos. De acuerdo con las guías de la OCDE, los Responsables del Tratamiento deben contar con un Programa Integral de Gestión de Datos Personales y estar preparados para demostrarle a la autoridad la implementación efectiva de esas medidas en la organización.

El Decreto 1377 de 2013 introdujo en Colombia la responsabilidad demostrada como una obligación en cabeza de los Responsables del Tratamiento. En este sentido, los Responsables deben ser capaces de demostrar, a petición de la SIC, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1027 de 2010.

BENEFICIOS PARA LA ORGANIZACIÓN

La apuesta que hace una organización por implementar estándares elevados de protección de datos personales y desarrollar un Programa Integral de Gestión de Datos Personales, le genera beneficios y se traduce en una mayor protección de los individuos. La SIC, como autoridad de protección de datos, está obligada a tener en cuenta la adopción de esas prácticas al momento de evaluar la imposición de sanciones.
Compliance is an Accountability Outcome

“An accountable organization must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws.”

The Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPC) of Alberta and British Columbia

https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf
Compliance is an Accountability Outcome

“A privacy management programme serves as a strategic framework to assist an organization in building a robust privacy infrastructure supported by an effective on-going review and monitoring process to facilitate compliance.”

Privacy Management Programme: A Best Practice Guide – Hong Kong – Office of the Privacy Commissioner for Personal Data, Hong Kong

“In one of the most relevant paragraphs of Decree 1377 from 2013, Article 26 introduced in the Colombian Data Protection System the “demonstrated responsibility” (or Accountability) criteria as a Data Controller’s responsibility. In the same sense, this Decree established that the Data Controller has to be capable to demonstrate, from a request from the Superintendence of Industry and Commerce, that they have deployed appropriate and effective measures to comply with the obligations set forth in Law 1581 of 2012.”
Research: Nymity Privacy Management Accountability Framework™

What is privacy management?

152 Privacy Management Activities: Procedures, policies, and other initiatives (measures/mechanisms) involving (or impacting) the processing of personal data.

www.nymity.com/pmaf
Tool to Support Colombia Guidelines

The Colombian Guidelines

1. **Senior Management Commitment and Assignment of Responsibilities**
2. **Informs Presentation**
3. **Operational Procedures**
4. **Data Bases Inventory**
5. **Effective Policies**
6. **Risks Administration System in relation with Personal Data**
7. **Training and Education Requirements**
8. **Response Protocols in relation with violations and incidents conducting**
9. **Data Processor’s Management in relation with Personal Data Cross Border Transfers**
10. **External Communications**

A Tool to help implement the Guidelines
Where to start?
Nymity’s Research: A Pragmatic Approach

Where to Start

Assign an individual or individuals responsible for privacy (privacy office)

1. Privacy office **identifies** current Privacy Management Activities across the organization

2. Privacy office **implements core** Privacy Management Activities

3. Privacy office **influences** the implementation or enhancement of Privacy Management Activities found in business and operational units
Step 1: Privacy Office Identifies Status of Privacy Management

Current Status of Privacy Management Across the Organization

Use the Accountability Framework as a Tool to identify Privacy Management Activities throughout the organization. Assign status of each Privacy Management Activity as either:

- Not Applicable
- Implemented
- Planned
- Desired

Identify Resources through a Status Check

While identifying existing Privacy Management Activities:

- Identify people that will help
- Identify motivated management
- Collect documentation

Use Framework to identify resources available
## Nymity’s Research - Understand Responsibilities

<table>
<thead>
<tr>
<th>Privacy Office Activities</th>
<th>Operational Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy officer responsibilities:</td>
<td>Privacy officer influences/observes:</td>
</tr>
<tr>
<td>Privacy Management Activities that are the Responsibility of the privacy office.</td>
<td>Privacy Management Activities that are the responsibility of operational units, including, Marketing, HR, IT, Legal, Procurement, and Product Development.</td>
</tr>
</tbody>
</table>

*Privacy management activities are mostly within operations*
# Example Privacy Management Activities

<table>
<thead>
<tr>
<th>Privacy Office Activities</th>
<th>Operational Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy officer responsibilities:</strong></td>
<td><strong>Privacy officer influences /observes:</strong></td>
</tr>
<tr>
<td>Examples:</td>
<td>Examples:</td>
</tr>
<tr>
<td>▪ maintain a data privacy policy</td>
<td>▪ maintain an information security policy</td>
</tr>
<tr>
<td>▪ maintain core training for all employees</td>
<td>▪ maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)</td>
</tr>
<tr>
<td>▪ maintain a data privacy notice that details the organization’s personal data handling policies</td>
<td>▪ maintain data privacy requirements for third parties</td>
</tr>
<tr>
<td>▪ consult with stakeholders throughout the organization on privacy matters</td>
<td>▪ integrate data privacy into practices for monitoring employees</td>
</tr>
</tbody>
</table>
Step 2: Privacy Office Implements New Privacy Management Activities

Responsibility of the Privacy Office
Implement core privacy management activities.

Privacy Office Activities
Privacy officer responsibilities:

Examples:

- maintain a data privacy policy
- maintain core training for all employees
- maintain a data privacy notice that details the organization’s personal data handling policies
- consult with stakeholders throughout the organization on privacy matters
Step 3: Privacy Office Influences Operational Privacy Management Activities

Responsibility of the Business and Operational Units

Implement/enhance Privacy Management Activities that can be maintained by the resources made available from business and operational units.

Example: Human Resources, IT, Legal, Product Development, Procurement, Marketing, Sales.

Operational Activities

Privacy officer influences /observes:

Examples:

- maintain an information security policy
- maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- maintain data privacy requirements for third parties
- integrate data privacy into practices for monitoring employees
Nymity’s Research: Where do I Start?

It Depends on your Resources (Identified in Step 1)

Select One:

- Minimal Resources – Take a Privacy Policy Approach
  For part-time privacy officers with limited resources

- Medium Resources – Take a Governance Approach
  For privacy officers with support from management and business and operational units, e.g., examples: HR, IT, Legal, Marketing, Sales, etc.

- Well Resourced – Take a Textbook Approach
  Senior management provides support and budget, a dedicated team, plus operational support.

Goal: Getting started using available resources
Where to Start - Minimal Resources

☑ Take a Privacy Policy Approach

1. Maintain a Data Privacy Policy
A policy written for employees outlining the organizations privacy practices.

2. Maintain Notices
Place your policy on the website and elsewhere to provide notice to individuals to which you collect, use, or disclose their personal data.

3. Training and Awareness Program
Training employees based on your data privacy policy.
Where to Start – Minimal Resources

Nymity Privacy Management Accountability Framework

1. Maintain Governance Structure
   - Establish a Board-level policy for accountability and transparency.
   - Develop a policy for monitoring and evaluating the management of privacy and security risks.

2. Maintain Personnel Data Inventory
   - Establish a data inventory to track the sensitivity of personal data.
   - Develop a policy for collecting and tracking sensitive personal data.

3. Maintain Data Privacy Policy
   - Ensure legal requirements and associated operational risk are addressed.

4. Embed Data Privacy Information System
   - Embed privacy policies into systems, processes, and requirements.

5. Maintain Training and Awareness Program
   - Ensure awareness and compliance with privacy policies and practices.

6. Manage Informed Consent Agreement
   - Establish a process for obtaining informed consent from data subjects.

7. Manage Third-Party Risk
   - Establish a process for selecting and monitoring third parties.

8. Maintain Notice
   - Establish a process for providing notice to data subjects.

9. Maintain Procedures for Inquiries and Complaints
   - Establish a process for handling inquiries and complaints.

10. Monitor for New Operational Practices
    - Establish a process for monitoring new operational practices.

11. Monitor Data Privacy Risk Management
    - Establish a process for monitoring data privacy risks.

12. Data Handling Practices
    - Establish a process for handling data.

13. Track External Criteria
    - Establish a process for tracking external criteria.

Copyright © 2015 by Nymity Inc. All rights reserved | WWW.NYMITY.COM
Take a Governance Approach:

1. Maintain Governance Structure
   Maintaining an annual privacy risk assessment, a charter, job descriptions, assign responsibilities throughout the organization, consult with stakeholders, report to management, etc.

2. Maintain a data privacy policy
   A policy written for employees outlining the organizations privacy practices.

3. Maintain Notices
   Place your policy on the website and elsewhere to provide notice to individuals to which you collect, use, or disclose their personal data.

4. Training and Awareness Program
   Training employees based on your data privacy policy.
Where to Start - Well Resourced

☑ Take a Textbook Approach

1. Maintain Personal Data Inventory
Maintain an inventory of data holding, with classification and data flows.

2. Maintain Governance Structure
Maintaining an annual privacy risk assessment, a charter, job descriptions, assign responsibilities throughout the organization, consult with stakeholders, report to management, etc.

3. Maintain a data privacy policy
A policy written for employees outlining the organizations privacy practices

4. Maintain Notices
Place your policy on the website and elsewhere to provide notice to individuals to which you collect, use or disclose their personal data.

5. Training and Awareness Program
Training employees based on your data privacy policy
## Where to Start – Sufficient Resources

<table>
<thead>
<tr>
<th>Nymity Privacy Management Accountability Framework™</th>
<th>NYMITY</th>
</tr>
</thead>
</table>

### 1. Maintain Governance Structure
- Ensure that individuals and teams are responsible for data privacy, accountable management, and operational reporting procedures.

### 2. Maintain Personnel Data Inventory
- Track the location of key personnel data storage or personal data flows with defined points of personal data.

### 3. Maintain Data Privacy Policy
- Ensure that a data privacy policy meets legal requirements and addresses operational risk.

### 4. Embed Data Privacy into Operations
- Integrating data privacy policies into operations and processes with the data privacy policies, legal requirements, and operational risk management objectives.

### 5. Maintain Training and Awareness Programs
- Ensure that employees are trained on data privacy policies to promote compliance with data privacy policies and related operational risk management objectives.

### 6. Manage Information Security Risk
- Manage information security risk based on legal requirements and ongoing risk assessments.

### 7. Manage Third-Party Risk
- Manage data privacy requirements for third parties (e.g., vendors, suppliers, contractors) to ensure that third parties are aware of and comply with data privacy policies and related operational risk management objectives.

### 8. Maintain Notice
- Maintain notices to individuals consistent with the data privacy policies, legal requirements, and operational risk management objectives.

### 9. Maintain Procedures for Inquiries and Complaints
- Ensure that effective procedures for inquiries and complaints are in place to address data privacy policies and related operational risk management objectives.

### 10. Monitor for New Operational Practices
- Monitor operational practices to identify new practices or changes to existing practices to ensure the implementation of data privacy policies and related operational risk management objectives.

### 11. Maintain Data Privacy Risk Management Program
- Ensure an effective data privacy incident and incident management program to manage data privacy policies and related operational risk management objectives.

### 12. Monitor Data Handling Processes
- Ensure that operational processes comply with data privacy policies and operational policies and procedures.

### 13. Track External Criteria
- Track new compliance requirements, expectations, and best practices.
After Identifying Status and Implementing: Tactical Privacy Management

- **Minimal Resources – Take a Privacy Policy Approach**
  For part-time privacy officers with limited resources.

- **Medium Resources - Take a Governance Approach**
  For privacy officers with support from management and
  business and operational units, such as HR, IT, Legal,
  Marketing, Sales, etc.

- **Well Resourced – Take the Textbook Approach**
  Senior management provides support and budget, a
dedicated team, plus operational support.

**Tactical**

Implement New Privacy Management Activities
Where Resources are Made Available
When the right Privacy Management Activities are implemented and maintained, ongoing compliance is one of the outcomes.
Measuring Success

What is a successful privacy management program?
When has the Privacy Officer Achieved Success?

Nymity’s Research: Three Theories for Defining Success:

- **Maximized Resources Theory**
  Is the Privacy Officer successful once all the resources have been maximized and she/he can report this fact to management?

- **Core Activities Theory**
  Is the Privacy Officer successful based on his/her own definition of core activities?

- **Independent Review Theory**
  Is the Privacy Officer successful based on a determination from someone outside the privacy office?
Maximized Resources Theory

Is the Privacy Officer successful once all the resources have been maximized and she/he can report this fact to management?

Based on Resources:

- Can demonstrate the privacy management activities maintained by the Privacy Officer

- Can demonstrate the privacy management activities maintained by business and operational units

Is the Privacy Officer successful if they have maximized all resources?
Is the Privacy Officer successful based on what she/he decides are core activities?

- Privacy Officer defines core activities for success
- Obtains necessary resources
- Implements and maintains
- Reports on an ongoing basis

Is the Privacy Officer the best person to define success?
Independent Review Theory

Is the privacy officer successful based on a determination from someone outside the privacy office?

- Internal assessment/audit?
- External assessment/audit?
- Privacy or data protection regulator?
- Privacy seal – Trustmark?

Success Frameworks:
- Binding Corporate Rules
- Cross Border Privacy Rules
- Regulator Accountability Guidelines
- The law (the future?)

*Is success being defined by someone that does not understand the business? Privacy?*
Which Theory Defines Success?

- **Maximized Resources Theory**
  Is the Privacy Officer successful once all the resources have been maximized and she/he can report this fact to management?

- **Core Activities Theory**
  Is the Privacy Officer successful based on his/her own definition of core activities?

- **Independent Review Theory**
  Is the Privacy Officer successful based on a determination from someone outside the privacy office?
How to Demonstrate Success

- **Maximized Resources Theory**  
  Is the Privacy Officer successful once all the resources have been maximized and she/he can report this fact to management?

- **Core Activities Theory**  
  Is the Privacy Officer successful based on his/her own definition of core activities?

- **Independent Review Theory**  
  Is the Privacy Officer successful based on a determination from someone outside the privacy office?
You are Responsible

Privacy program is in place

You Implemented

- Privacy strategy
- Access request procedures
- Data Inventory
  Many more........

You Influenced

- Privacy Impact Assessment
- Breach Response Protocol
- Code of Conduct
  Many more........
## You Have Documentation (Evidence)

<table>
<thead>
<tr>
<th>You Implemented</th>
<th>You Influenced</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Privacy Strategy</td>
<td>- Privacy Impact Assessment</td>
</tr>
<tr>
<td>- Access Request Procedures</td>
<td>- Breach Response Protocol</td>
</tr>
<tr>
<td>- Data Inventory</td>
<td>- Code of Conduct</td>
</tr>
<tr>
<td>Many more........</td>
<td>Many more........</td>
</tr>
</tbody>
</table>
Maximized Resources Theory

Stand Ready to Demonstrate
Core Activities Theory

NYMITY Data Privacy Accountability Scorecard™
www.scorecard.nymity.com

% Advanced = # of Elective activities completed and evidenced ÷ # of Elective activities

Target = 100% of Core activities completed and evidenced

% Managed = # of Core activities completed and evidenced ÷ # of Core activities
☑ Independent Review Theory

Assess
How Nymity’s Research Helps

✓ Understanding Accountability

✓ Demonstrating that Compliance is an Accountability Outcome

✓ Getting Started

✓ Discussing when the Privacy Office is Successful

✓ Demonstrating Privacy Office Success
Thank You!

Please feel free to contact us with any questions or comments concerning this presentation at feedback@nymity.com.