Demonstrating Accountability With a Scorecard Framework

“The Scorecard is an example of how responsible organizations with established privacy programs can stand ready to demonstrate accountability and benefit from doing so.”

Martin Abrams, Executive Director & Chief Strategist of the Information Accountability Foundation

“The ability to demonstrate accountability is a topic of great interest and currency among privacy regulators and professionals alike; Nymity making its "Scorecard" available for free, in an easily accessible format with supporting materials and training videos, enables organizations of all sizes more opportunities to organize and present how they address accountability.”

Joe Alhadeff, VP Global Public Policy and Chief Privacy Strategist, Oracle
About Nymity

Nymity is a global research firm for privacy and data protection compliance, based in Canada, started in 2002.

Subscription Research:
1. Compliance knowledge support solutions
2. Accountability management support solutions

Publicly Available Research:
1. KnowledgeHub
   (Since 2002)
2. Demonstrating Accountability
   (September 24, 2013)

Accountability Research History
See Preface page iv, for Nymity historical accountability research projects and studies.
What is **Accountability**?

**Much Easier Conversation in Canada**

“Accountability, in relation to privacy, is the **acceptance of responsibility for personal information protection**. 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.”

**Getting Accountability Right with a Privacy Management Program**

Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia
What is Demonstrating Accountability?

“Finally, accountable organizations should be able to demonstrate to Privacy Commissioners that they have an effective, up-to-date privacy management program in place in the event of a complaint investigation or audit.”

Getting Accountability Right with a Privacy Management Program

Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia
What Motivates Accountability?

- Laws and regulations
- Organizational culture
- Enforcement actions
- Data breach
- Risk management (e.g. reputation)
- Consumer trust
- Contractual obligations
- Competitive advantage
- Alignment with organisation initiatives
- New privacy officer
- Law firms and consulting firms guidance
- Reduced insurance
- Merger & acquisitions
- What about reporting to Data Protection Authorities?

What motivates the creation and maintenance of an effective privacy program?
How to Demonstrate Accountability?

In other words - how to demonstrate an effective, up-to-date, privacy management program?

How can an established privacy program be demonstrated?

- Audit?
- Trustmark (privacy seal)?

What about self-reporting with documentation?
Nymity Research: Self-Reporting

Goal:
Workable framework for demonstrating accountability

Success Factors (2010)
- Must communicate the privacy program status
- Evidence-based
- Third-party verification not required
- Free of charge
First Research Initiative

Success:

- ✔ Reported status of privacy program
- ✔ Evidence-based
- ✔ Third-party verification not required
- ✔ Free

AICPA/CICA Privacy Maturity Model (2011)

Workability Challenges:

- ✗ Too complicated
- ✗ Not scalable/flexible
- ✗ Not global
- ✗ No timeline, as in no history
- ✗ Needed to be activity based, not controls based
Second Research Initiative

Success:
✓ Reported status of privacy program
✓ Evidence-based
✓ Third-party verification not required
✓ Free

New success factors:
✓ Not complicated
✓ Scalable and flexible
✓ Global
✓ Timeline based
✓ Activity based

Nymity Claims-Based Self-Attestation Methodology (2012)

Workability challenges:
× Results need to objective i.e. empirically calculated
× Required efficient evidence collection
Third Research Initiative

Success:
- Reported status of privacy program
- Evidence-based
- Third-party verification not required
- Free
- Not complicated
- Scalable
- Global
- Timeline based
- Activity based

New Success Metrics:
- Empirical/objective
- Efficient evidence collection

Nymity Data Privacy Accountability Scorecard (2013)

No new challenges
- Make publicly available – feedback release
2013 Feedback Release:

An evidence-based, publicly-available, scalable framework for the Privacy Office in responsible organisations to demonstrate accountability by monitoring, measuring, and reporting ongoing privacy management activities.
Instructions

Feedback
Nymity would appreciate feedback from users of this framework:

* How this framework could be improved to help responsible organisations demonstrate accountability.
* How this framework could be used and/or improved to allow law firms and consulting firms to better assist their clients with maintaining an effective privacy program.

Provide feedback via email to Research@Nymity.com

About this Spreadsheet
This template is configured to enable automatic score calculation and plotting for up to 20 updates, with 25 core and 25 elective activities.

The worksheet is protected, but no password is required to unprotect the sheet if you wish to modify it. Please note that adding rows or columns may prevent the Scorecard graph from displaying correctly. Please review the legal information below with regard to modifying the spreadsheet.

Legal Information
Copyright © 2013 by Nymity Inc.
Nymity Inc. retains all copyright. Copyright is protected under international treaties. Full details of the Terms & Conditions of Use (T&C) are available at http://www.nymity.com/LegalNotice.aspx.

Nymity makes downloadable templates available and organisations are free to use, edit, modify, distribute and duplicate the templates for the following purposes and under the following conditions:

1) For use as a primary reporting framework for organizations to report on the internal and external status of their privacy program.
2) For use by law firms and consultants to assist organizations with accountability and compliance.
3) The use of this template for the creation of a commercial software offering is strictly prohibited.
4) The use of this template for Trustmarks, Privacy Seals, verification or certification frameworks is strictly prohibited.
5) Organizations that enhance the Scorecard for internal purposes are requested to share these augmentations with Nymity so that other organizations may also benefit.
6) Requests for the use for other purposes may be directed to the contact information below.
**Template**

Set up and log evidence.
Automatically Evidence will create the score.
Example Provided

In spreadsheet, book and training video.
### NYMITY Data Privacy Accountability Scorecard™

#### Evidence Worksheet

www.scorecard.nymity.com

<table>
<thead>
<tr>
<th>% Managed (core activities completed and evidenced)</th>
<th>64% Managed - 7 out of 11 core activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Advanced (elective activities completed and evidenced)</td>
<td>29% Advanced - 2 out of 7 elective activities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID#</th>
<th>Question</th>
<th>Owner</th>
<th>Frequency</th>
<th>Response</th>
<th>Comment</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Is the Data Privacy Policy reviewed based on legislative and operational changes?</td>
<td>Privacy Office</td>
<td>Annual</td>
<td>No</td>
<td>The Data Privacy Policy has not been reviewed in the last two years. No plan to do so within the next two years.</td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>Do the individuals in the privacy office maintain their privacy knowledge?</td>
<td>Privacy Office</td>
<td>Annual</td>
<td>Yes</td>
<td>All members of the Privacy Office maintain privacy certification.</td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>Does the Privacy Office track and analyze the impact of new laws, changes in laws, relevant enforcement actions and new regulator expectations?</td>
<td>Privacy Office</td>
<td>Quarterly</td>
<td>Yes</td>
<td>The Privacy Office subscribes to Nymity's PrivaWorks to track legislative developments. No applicable changes to laws or regulations.</td>
<td>Memo between Privacy and Legal regarding legislative developments (none noted).</td>
</tr>
<tr>
<td>C4</td>
<td>Do all third party contracts contain organizational standard privacy language?</td>
<td>Legal</td>
<td>Annual</td>
<td>No</td>
<td>Contracts are likely being reviewed as they have always been in the past but Legal did not provide evidence on their current status.</td>
<td>Will follow-up.</td>
</tr>
<tr>
<td>C5</td>
<td>Is the online Privacy Notice updated based on changes to policy, operations, or legal developments?</td>
<td>Legal</td>
<td>Annual</td>
<td>Yes</td>
<td>Privacy Notice was reviewed and changes were made for 2013.</td>
<td>Privacy Notice v3.4 (published 2/14/13) <a href="http://www.website.com/privacy">www.website.com/privacy</a></td>
</tr>
<tr>
<td>C6</td>
<td>Are all new employees trained on data privacy?</td>
<td>Human Resources</td>
<td>Quarterly</td>
<td>No</td>
<td>Employee training on data privacy was completed. No plan to track by HR.</td>
<td>Report of employees who have completed data privacy training.</td>
</tr>
<tr>
<td>C7</td>
<td>Are procedures for responding to access requests, complaints, and inquiries reviewed and</td>
<td>Customer</td>
<td>Annually</td>
<td>Yes</td>
<td>Procedures for responding to access requests, complaints and inquiries have not been reviewed in the past two years.</td>
<td></td>
</tr>
</tbody>
</table>

---

Add Evidence

Example Provided
<table>
<thead>
<tr>
<th>Core Activities</th>
<th>Question</th>
<th>Owner</th>
<th>Frequency</th>
<th>Response</th>
<th>Comment</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Is the Data Privacy Policy reviewed based on legislative and operational changes?</td>
<td>Privacy Office</td>
<td>Annual</td>
<td>No</td>
<td>The Data Privacy Policy has not been reviewed in the last two years, we plan to do so within the next two months.</td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>Do the individuals in the privacy office maintain their privacy knowledge?</td>
<td>Privacy Office</td>
<td>Annual</td>
<td>Yes</td>
<td>All members of the Privacy Office maintain privacy certifications. Email confirmation from all members of the Privacy Office that their certifications are in good standing.</td>
<td></td>
</tr>
<tr>
<td>C3</td>
<td>Does the Privacy Office track and analyze the impact of new laws, changes in laws, relevant enforcement actions and new regulator expectations?</td>
<td>Privacy Office</td>
<td>Quarterly</td>
<td>Yes</td>
<td>The Privacy Office subscribes to Nymity’s PrivacyWorks to track legislative developments. No applicable changes to laws or regulations. Memo between Privacy and Legal regarding legislative developments (none noted).</td>
<td></td>
</tr>
<tr>
<td>C4</td>
<td>Do all third party contracts contain organizational and standard privacy language?</td>
<td>Legal</td>
<td>Annual</td>
<td>No</td>
<td>Contracts are likely being reviewed as they have always been in the past but Legal did not provide evidence on schedule. Will follow up.</td>
<td></td>
</tr>
<tr>
<td>C5</td>
<td>Is the online Privacy Notice updated based on changes to policy operations, or legal developments?</td>
<td>Legal</td>
<td>Annual</td>
<td>Yes</td>
<td>The Privacy Notice was reviewed and no changes were made for 2013. Privacy Notice v3.4 (published 2/14/13) <a href="http://www.website.com/privacynotice">www.website.com/privacynotice</a></td>
<td></td>
</tr>
<tr>
<td>C6</td>
<td>Are all new employees trained on data privacy?</td>
<td>Human Resources</td>
<td>Quarterly</td>
<td>Yes</td>
<td>Employees are required to complete e-learning module for data privacy and results are tracked by HR. Report of employees who have completed data privacy training.</td>
<td></td>
</tr>
<tr>
<td>C7</td>
<td>Are procedures for responding to access requests, complaints, and inquiries reviewed and updated?</td>
<td>Customer</td>
<td>Annual</td>
<td>Yes</td>
<td>The procedures for responding to access requests, complaints and grievances have not been reviewed in the last two months.</td>
<td></td>
</tr>
</tbody>
</table>

Example Provided
NYMITY Data Privacy Accountability Scorecard™

Example Provided
Download Spreadsheet Template

Note:

Only works for established privacy programs.

No evidence – no score.
Publicly Available Scorecard Version 2
March 2014 – IAPP Summit

Nymity Invites Feedback from:

- Responsible organizations with established privacy programs
- Data Protection Authorities
- Law firms, consulting firms and other privacy professionals
Thank You!

2013 Feedback Release:

Direct Feedback to research@nymity.com

- Organizations with established programs
- Data Protection Authorities
- Law firms, consulting firms and other privacy professionals interested in demonstrating accountability

Version 2

- March 2014 – IAPP Summit – Washington DC