

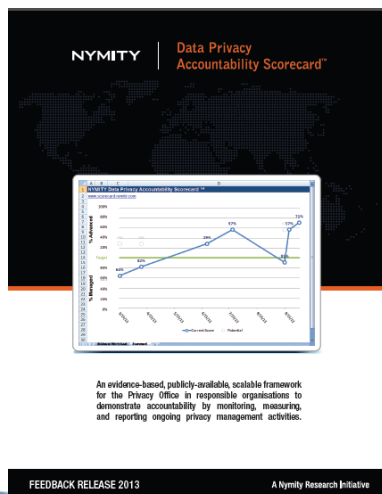
Demonstrating Accountability With a Scorecard Framework

“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



Nymity Research

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.



Today's Workshop

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?

Again: Much Easier Conversation in Canada

“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

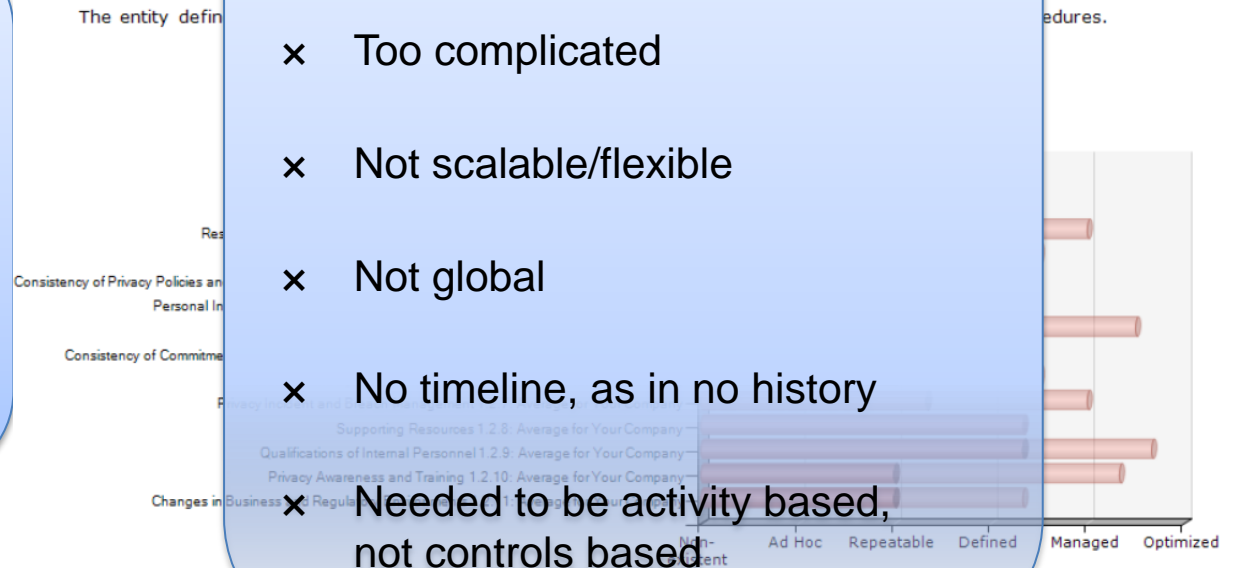
AICPA/CICA Privacy Maturity Model (2011)

Success:

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

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

Nymity Claims-Based Self-Attestation Methodology (2012)

Success:

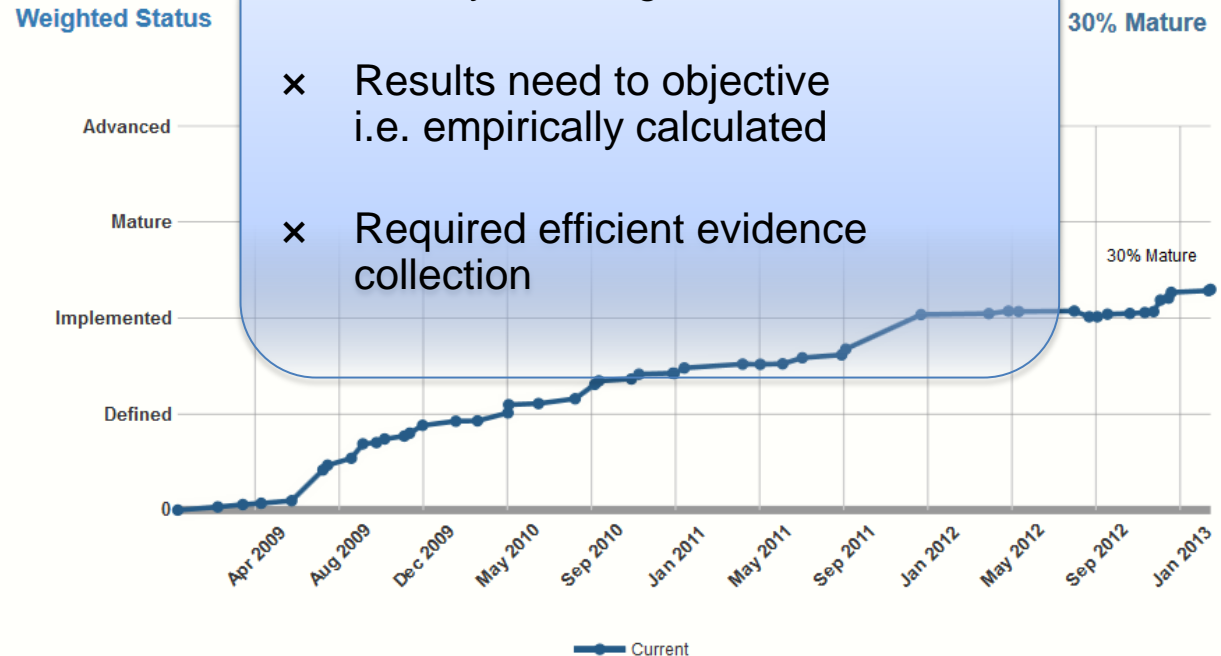
- ✓ Reported status of privacy program
- ✓ Evidence-based
- ✓ Third-party verification not required
- ✓ Free

New success factors:

- ✓ Not complicated
- ✓ Scalable and flexible
- ✓ Global
- ✓ Timeline based
- ✓ Activity based

Workability challenges:

- × Results need to be objective i.e. empirically calculated
- × Required efficient evidence collection



Third Research Initiative

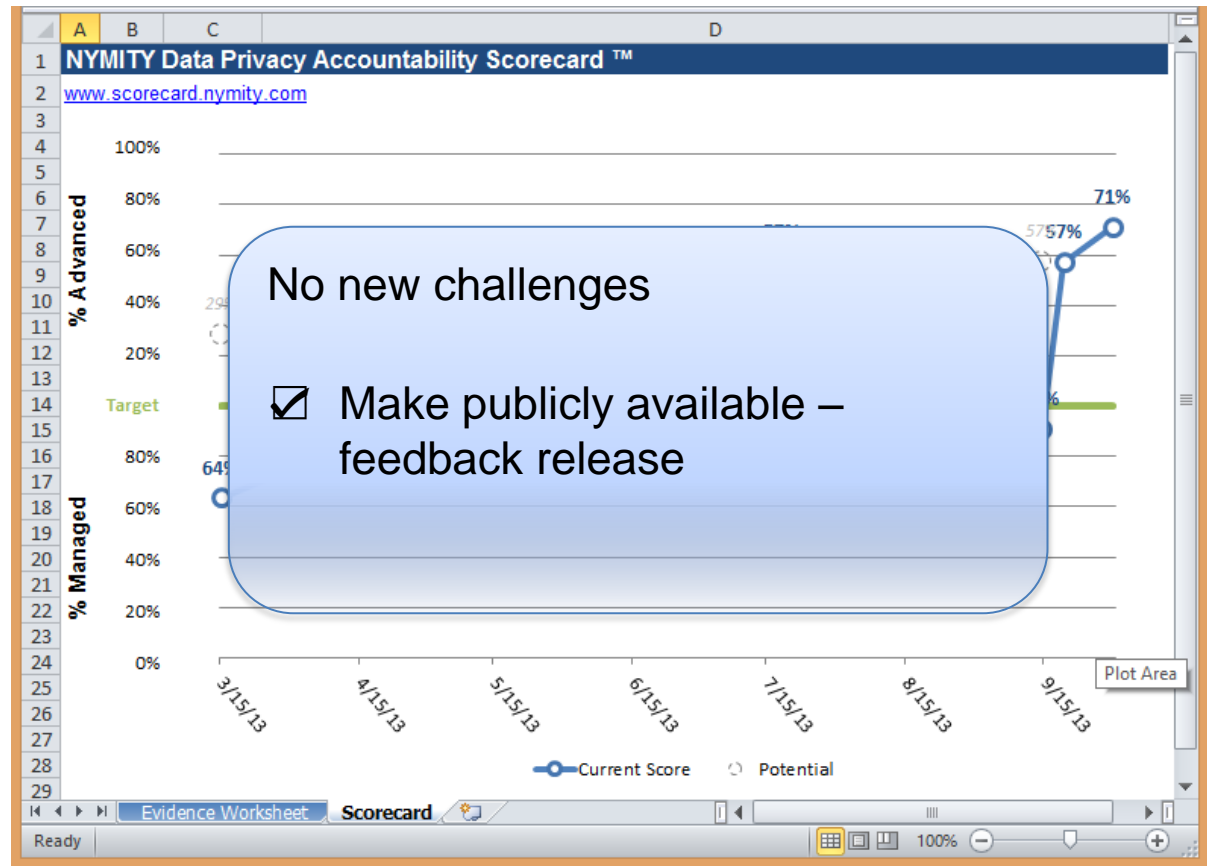
Nymity Data Privacy Accountability Scorecard (2013)

Success:

- ✓ Reported status of privacy program
- ✓ Evidence-based
- ✓ Third-part verification not required
- ✓ Free
- ✓ Not complicated
- ✓ Scalable
- ✓ Global
- ✓ Timeline based
- ✓ Activity based

New Success Metrics:

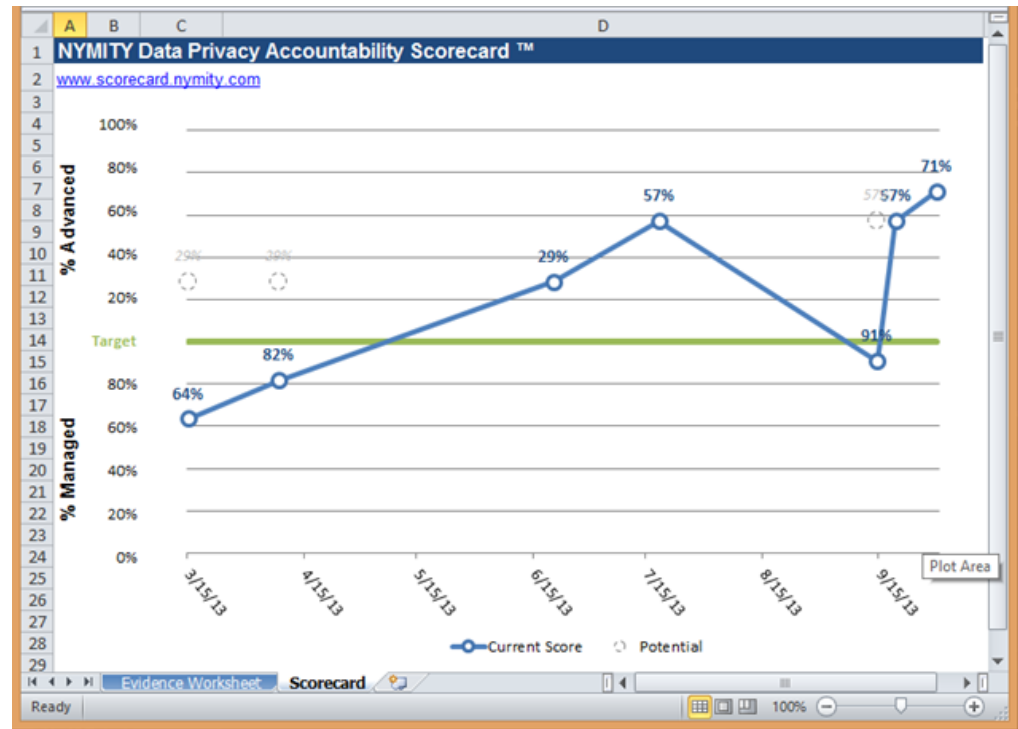
- ✓ Empirical/objective
- ✓ Efficient evidence collection



Nymity Data Privacy Accountability Scorecard™

2013 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

- 5 * Scorecard Instruction Book
- 6 * Nymity Evidencing Accountability Study
- 7 * Training Videos
- 8 * Webinars

Feedback

Nymity would appreciate feedback from users of this framework:

- *How this framework could be improved to help responsible organisations demonstrate accountability; and
- *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.

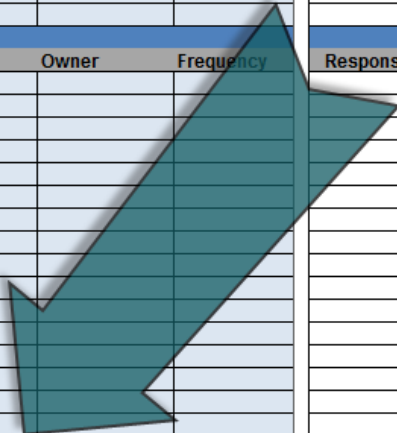
Legal Information

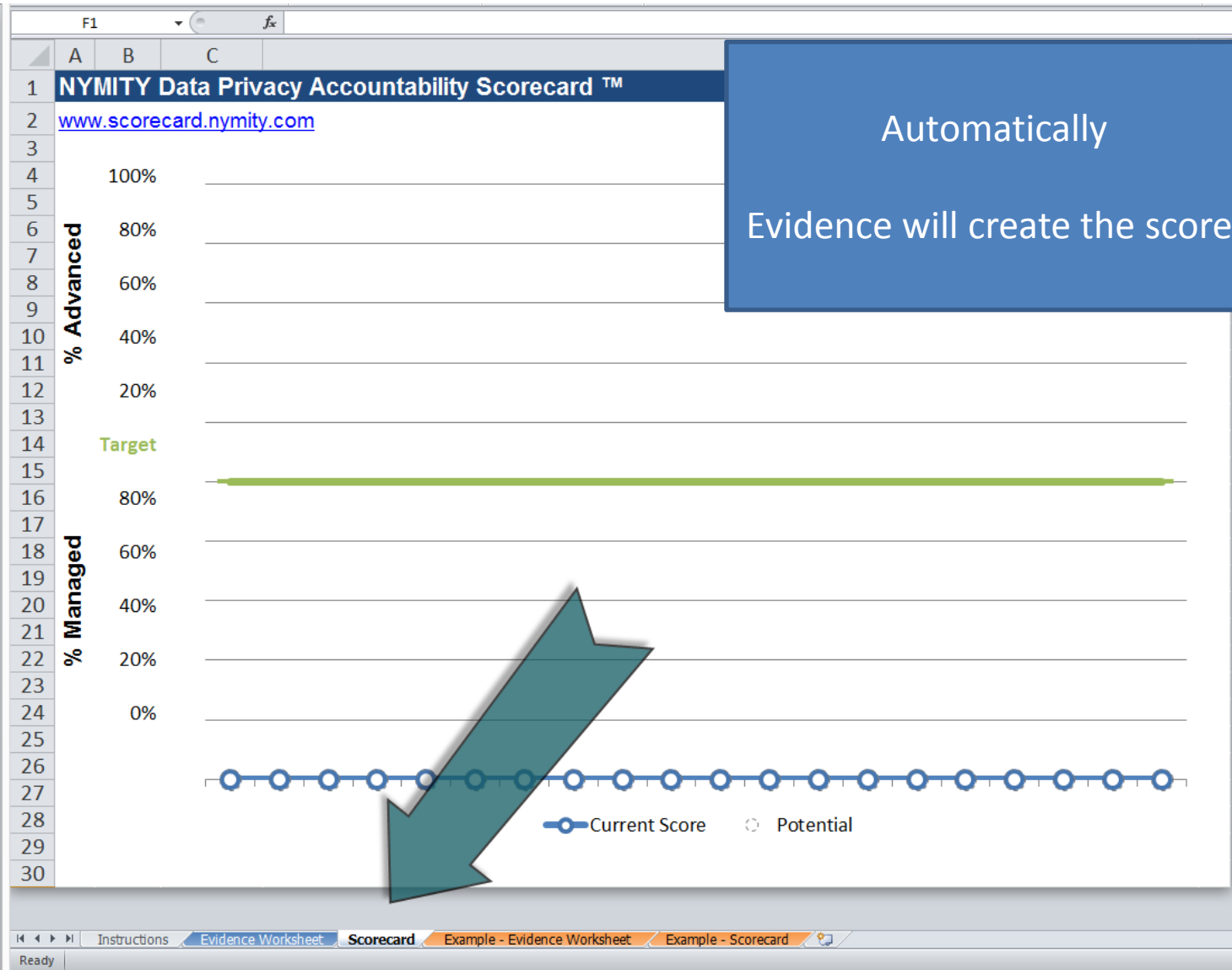
Copyright © 2013 by Nymity Inc.
Nymity Inc. retains all copyright. Copyright is protected under international treaties. Full details of the Terms & Conditions of Use (T&C) are available at <http://www.nymity.com/LegalNotice.aspx>.

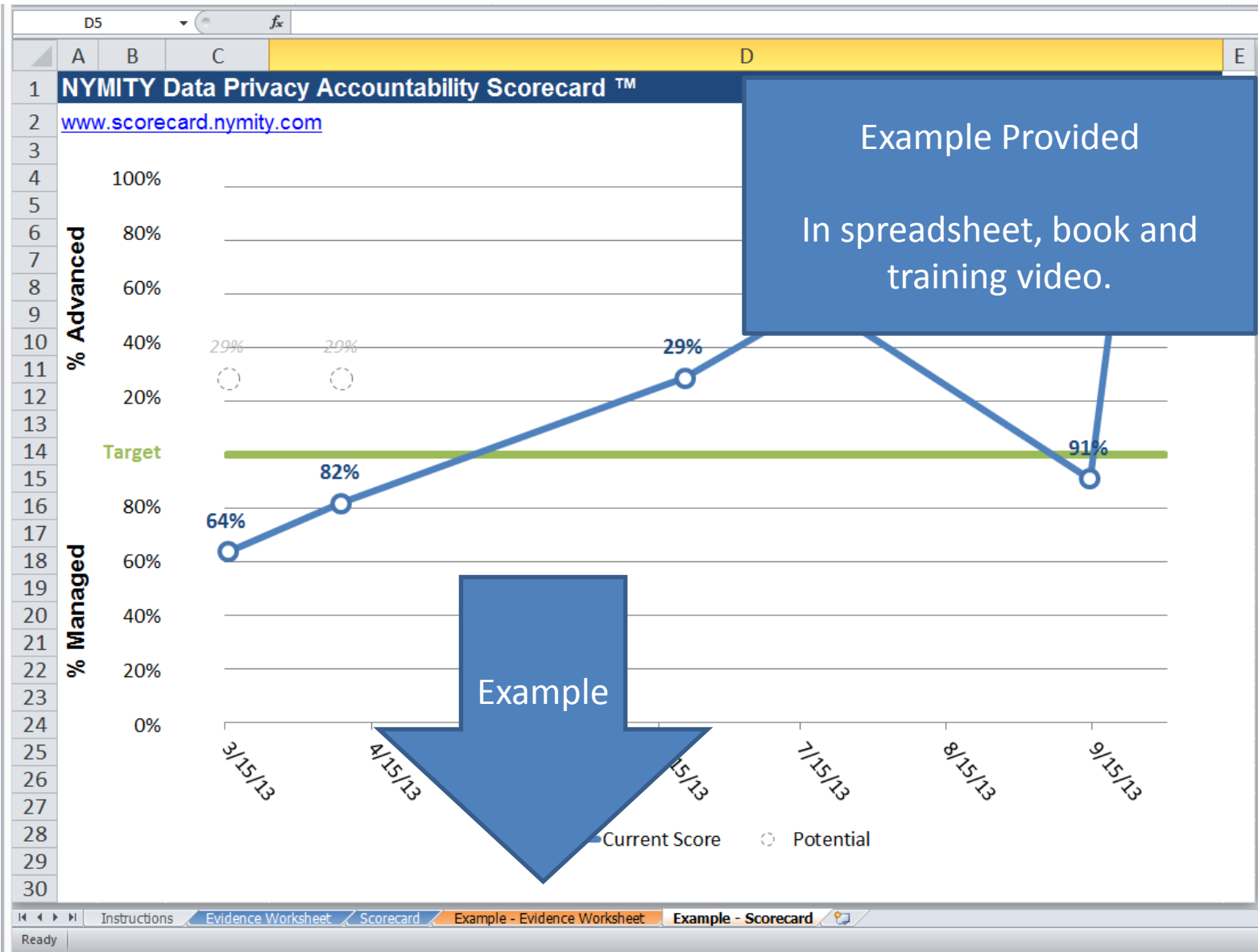
- Nymity makes downloadable templates available and organizations are free to use, edit, modify, distribute and duplicate the templates for the following purposes and under the following conditions:
- 1) For use as a primary reporting framework for organizations to report on the internal and external status of their privacy program.
 - 2) For use by law firms and consultants to assist organisations 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.

NYMITY Data Privacy Accountability Scorecard™							
Evidence Worksheet					1		
www.scorecard.nymity.com							
% Managed (core activities completed and evidenced)							
% Advanced (elective activities completed and evidenced)							
Core Activities							
ID#	Question	Owner	Frequency	Response			
C1							
C2							
C3							
C4							
C5							
C6							
C7							
C8							
C9							
C10							
C11							
C12							
C13							
C14							
C15							
C16							
C17							
C18							
C19							
C20							
C21							
C22							
C23							
C24							
C25							
Elective Activities					Response	Comment	Evidence
ID#	Question	Owner	Frequency				
E1							
E2							
E3							
E4							
E5							
E6							
E7							
E8							
E9							
E10							
E11							
E12							
E13							
E14							
E15							
E16							
E17							

Template
Set up and log evidence.



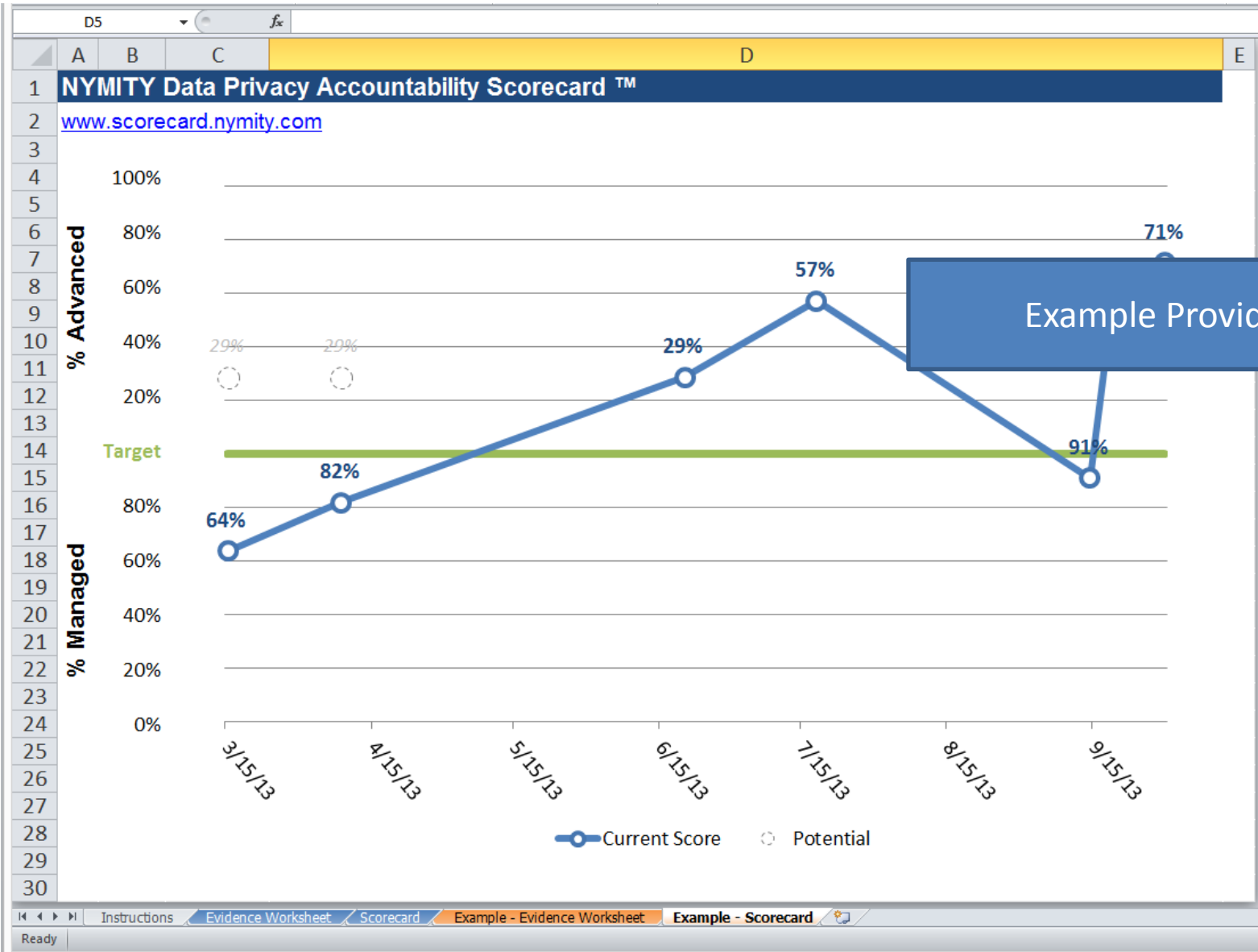




1	NYMITY Data Privacy Accountability Scorecard™							
2	Evidence Worksheet							
3	www.scorecard.nymity.com				1			
4	% Managed (core activities completed and evidenced)				64%	Managed - 7 out of 11 core activities		
5	% Advanced (elective activities completed and evidenced)				29%	Advanced - 2 out of 7 elective activities		
6	Core Activities							
7	ID#	Question	Owner	Frequency	Response	Comment	Evidence	
8	C1	Is the Data Privacy Policy reviewed based on legislative and operational changes?	Privacy Office	Annual	No	The Data Privacy Policy has not been reviewed in the last two years to do so within the next two		
9	C2	Do the individuals in the privacy office maintain their privacy knowledge?	Privacy Office	Annual	Yes	All members of the Privacy Office maintain privacy certification	Privacy Office that their certifications are in good standing.	
10	C3	Does the Privacy Office track and analyze the impact of new laws, changes in laws, relevant enforcement actions and new regulator expectations?	Privacy Office	Quarterly	Yes	The Privacy Office subscribes to Nymity's PrivaWorks to track legislative developments. No applicable changes to laws or regulations.	Memo between Privacy and Legal regarding legislative developments (none noted).	
11	C4	Do all third party contracts contain organizational standard privacy language?	Legal	Annual	No	Contracts are likely being reviewed as they have always been in the past but Legal did not provide evidence on		
12	C5	Is the online Privacy Notice updated based on changes to policy, operations, or legal developments?	Legal	Annual		Privacy Notice was reviewed and updates were made for 2013.	Privacy Notice v3.4 (published 2/14/13) www.website.com/privacy	
13	C6	Are all new employees trained on data privacy?	Human Resources	Quarterly		Employees are trained to completed data privacy and tracked by HR.	Report of employees who have completed data privacy training.	
	C7	Are procedures for responding to access requests, complaints, and inquiries reviewed and	Customer	Annual	No	Procedures for responding to access requests, complaints and inquiries have not been reviewed in the		

Example Provided

Add Evidence



Example Provided

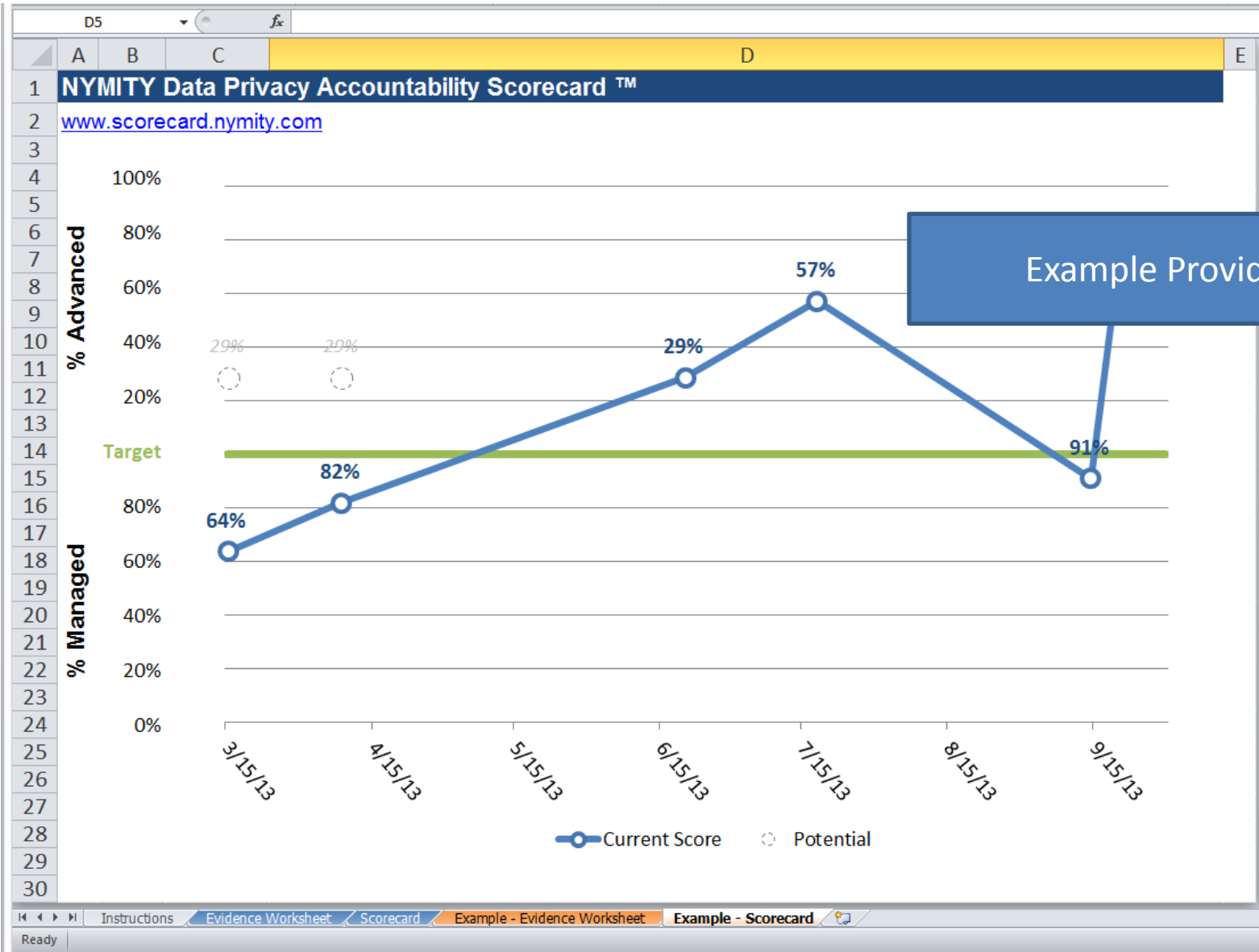
N1 fx

NYMITY Data Privacy Accountability Scorecard™											
Evidence Worksheet				1				2			
www.scorecard.nymity.com				3/15/2013				Update: 4/8/2013			
% Managed (core activities completed and evidenced)				64% Managed - 7 out of 11 core activities				82% Managed - 9 out of 11 core activities			
% Advanced (elective activities completed and evidenced)				29% Advanced - 2 out of 7 elective activities				29% Advanced - 2 out of 7 elective activities			
Core Activities				Response				Update?			
ID#	Question	Owner	Frequency	Response	Comment	Evidence	Update?	Response	Comment	Evidence	
C1	Is the Data Privacy Policy reviewed based on legislative and operational changes?	Privacy Office	Annual	No	The Data Privacy Policy has not been reviewed in the last two years, we plan to do so within the next two months.		Yes	Yes	The Data Privacy Policy was reviewed, and no changes were made for 2013.	Data Privacy Policy v2.8 (published 2/14/13)	
C2	Do the individuals in the privacy office maintain their privacy knowledge?	Privacy Office	Annual	Yes	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.		Yes	Refer to previous comment.	Refer to previous evidence.	
C3	Does the Privacy Office track and analyze the impact of new laws, changes in laws, relevant enforcement actions and new regulator expectations?	Privacy Office	Quarterly	Yes	The Privacy Office subscribes to Nymity's PrivaWorks to track legislative developments. No applicable changes to laws or regulations.	Memo between Privacy and Legal regarding legislative developments (none noted).		Yes	Refer to previous comment.	Refer to previous evidence.	
C4	Do all third party contracts contain organizational standard privacy language?	Legal	Annual	No	Contracts are likely being reviewed as they have always been in the past but Legal did not provide evidence on schedule. Will follow-up.			No	Refer to previous comment.	Refer to previous evidence.	
C5	Is the online Privacy Notice updated based on changes to policy, operations, or legal developments?	Legal	Annual	Yes	The Privacy Notice was reviewed and no changes were made for 2013.	Privacy Notice v3.4 (published 2/14/13) www.website.com/privacy		Yes	Refer to previous comment.	Refer to previous evidence.	
C6	Are all new employees trained on data privacy?	Human Resources	Quarterly	Yes	Employees are required to completed eLearning module for data privacy and results are tracked by HR.	Report of employees who have completed data privacy training.		Yes	Refer to previous comment.	Refer to previous evidence.	
C7	Are procedures for responding to access requests, complaints, and inquiries reviewed and updated annually?	Customer	Annual	No	The procedures for responding to access requests, complaints and inquiries have not been reviewed in the last two years.		Yes	Yes	Reviewed the Customer Service Operations Manual procedures for responding to access requests.	www.intranet.com/customer-service/operations-manual	

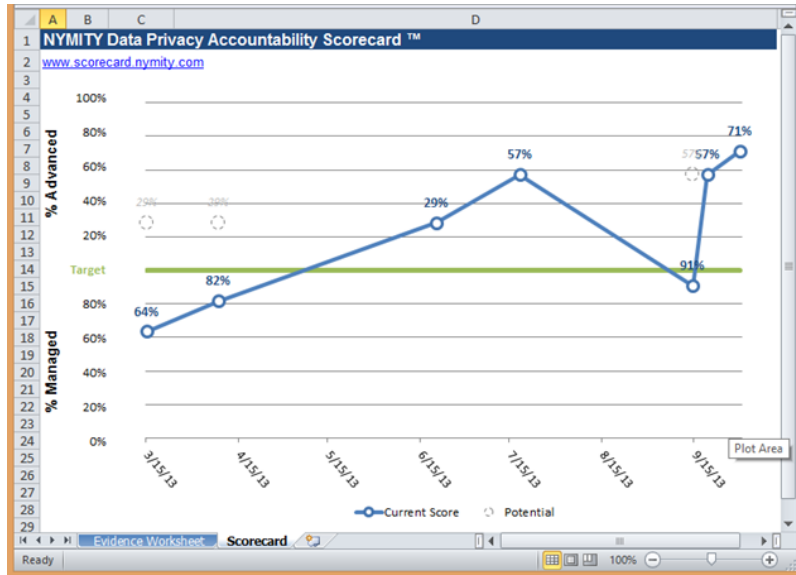
Ready 120% 100%

16 Click to add notes

Slide 15 of 18 "Office Theme" English (Canada)



Download Spreadsheet Template



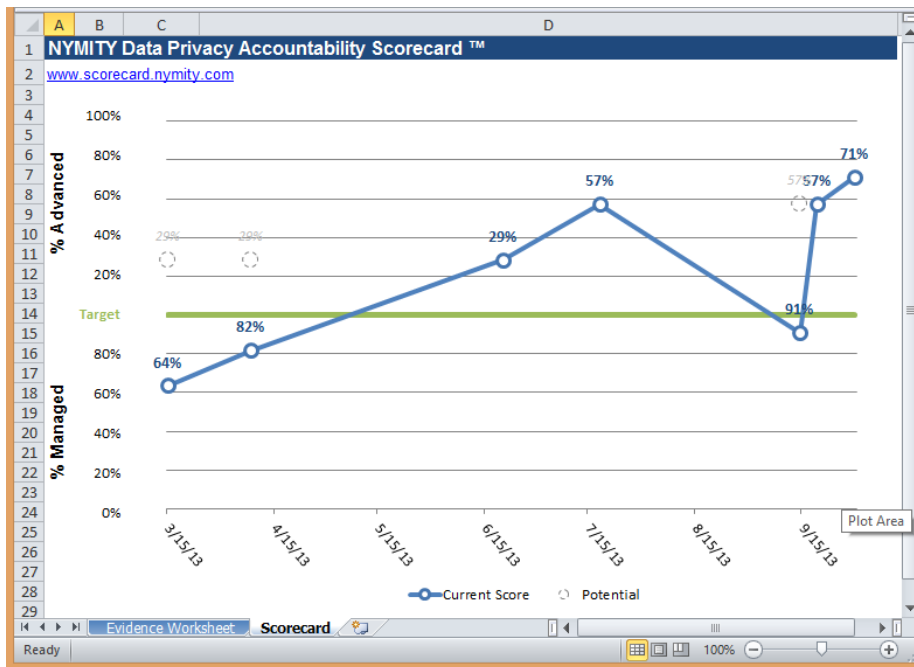
Note:

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

314/471