A Privacy Office Guide to

DEMONSTRATING ACCOUNTABILITY

Foreword by

Martin Abrams
Information Accountability Foundation

A Nymity Research Initiative

NYMITY
innovating compliance

A Privacy Office Guide to Demonstrating Accountability

A pragmatic approach for responsible organizations to demonstrate an effective privacy program, in other words to demonstrate accountability - featuring the Nymity Data Privacy Accountability Framework and the Nymity Data Privacy Accountability Scorecard

Lead Author
Terry McQuay, CIPP/C/E/G/US, CIPM
President, Nymity Inc.

Co-Author
Lauren Reid, CIPM, CIPP/US, CISA
Director, Compliance Solutions, Nymity Inc.

Contributing Researchers
Blaine Currie, Ph.D., CIPP/C, CIPP/US, CIPP/E
Privacy Legal Researcher, Nymity Inc.

Lara Hunt
Privacy Legal Researcher, Nymity Inc.

John Jager, CIPP/C, CIPP/US, CIPP/G
Vice President, Research Methodology, Nymity Inc.

Rob Kenigsberg, CIPP/US
Privacy Legal Researcher & Spanish Translator, Nymity Inc.

Meaghan McCluskey, LL.B., CIPP/US, CIPP/E
Senior Privacy Research Lawyer, Nymity Inc.

Camille McQuay, LL.B., CIPM, CIPP/E, CIPP/G, CIPP/US
Vice President, Research, Nymity Inc.

Kristina Smith
Privacy Legal Researcher, Nymity Inc.

Senior Editor: Karinna Neumann, MBA, CIPM, CIPP/E, Nymity Inc.

Copy Editor: Stephanie Mancini, Nymity Inc.

Design and Graphics: Azure Chern, Nymity Inc.

A Nymity Research Initiative

This book is provided by Nymity for free, for an electronic version please visit https://www.nymity.com/demonstratingaccountability

.

Acknowledgements

Nymity would like to thank its customers, friends, think tanks, and regulators for their contributions in this book via Nymity research studies, workshops, and invaluable feedback. Nymity would also like to thank the tireless effort of its research team in conducting the underlying research, without which these frameworks and methodologies would not exist.

Table of Contents

Foreword by Martin Abrams, Information Accountability Foundation

5000 years ago the privacy threatening technology was clay disks with marks that let one record observations about others and transport those observations over time and distance. Writing, the first information technology, fueled the innovation that begat every innovation moving forward.

Today we talk about Big Data facilitating knowledge that will beget every new technology moving forward. The scale is different, but the risk to our need for the space and freedom to define ourselves is the same.

Privacy is about preserving who we are as individuals and allowing us to map our futures and not have our futures pre-ordained by math applied to observations. However, simple rules sets do not deal well with the complex risks that come with complex information driven processes.

The OECD coined the term accountability in a privacy context in 1980. Over the past ten years I have worked with others to define the principle and map how it might be tangible. Nymity has joined me early in that journey.

While we have defined the essential elements of accountability, it has become more clear that for accountability to work we need to be able to measure the effectiveness of privacy programs, and how they link to the essential elements. Accountability requires an organization to be responsible and answerable. Responsibility means preserving dignity and preventing inappropriate harm as we use personally linkable information. Answerability means being able to demonstrate programs in a tangible way with metrics that have integrity

Understanding the risks is hard. Mitigating risks may be harder yet. Measuring accountability may be harder still. It is that last challenge, measuring accountability, which has been Nymity's challenge.

For years Nymity has conducted research on effective privacy programs and how they stand up to obligations mandated by law and the public's explanations. Nymity has then translated the research into tools that are readily usable by privacy practitioners. The newest challenge has been accountability, and Nymity has been following the accountability movement for 10 years to understand how to measure the effectiveness of accountability based privacy programs.

To be perfectly blunt, I couldn't do my job without the work of organizations like Nymity. Nymity has taken on their research and tools challenge with passion, and for this I am grateful.

- *Martin Abrams, Executive Director, Information Accountability Foundation*

Martin Abrams is the executive director of the Information Accountability Foundation, a new non-profit privacy think tank. He was formerly president of the Centre for Information Policy Leadership at Hunton & Williams LLP. He regularly works with data protection authorities to define future priorities. He led the project group that developed multi-layered notices and gained its acceptance from Working Party 29 of the European Commission, OECD and APEC. Abrams speaks and writes on information policy trend issues, and has led privacy seminars in Asia, Australia, Europe, North and South America. He is the 2008 winner of the International Association of Privacy Professionals Vanguard Award.

Executive Summary

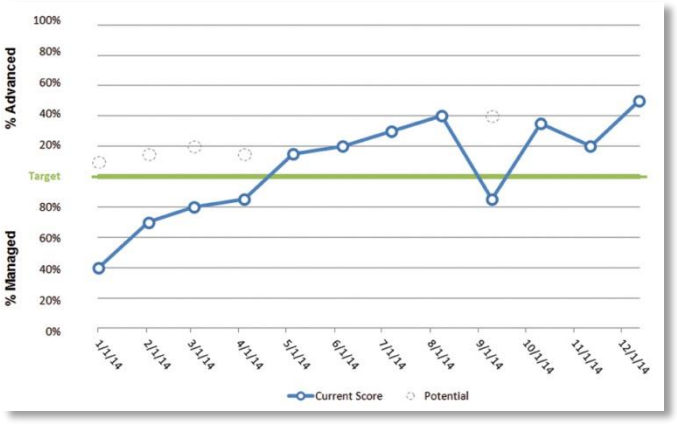
The ultimate goal of the privacy office in many organizations is to be able to answer the question, 'how do we know that the privacy program is effectively embedded throughout the organization?', in other words, to be accountable and to demonstrate it.

This book is a guide for the privacy office to demonstrate accountability using the Nymity Data Privacy Accountability Scorecard™ ("Scorecard"). Demonstrating accountability is more than reporting, and even more than reporting with evidence, it is the ability to show that a privacy program is managed and monitored.

The Scorecard Demonstrates Accountability

The Scorecard uses a simple concept –a single objective - to answer the question, 'does the organization have effective privacy management – yes or no?' In other words, the Scorecard shows: are we above or below the target line?

The Scorecard works because the privacy office defines and justifies which activities must be completed to meet the Target, that is, to reach the line. The privacy office also identifies the activities that, if completed, will show that privacy management is above the line.



Leverage Existing Documentation

Processing personal data responsibly takes place throughout the organization – many organizations were doing so long before the establishment of the privacy office. The Scorecard enables the privacy office to collect evidence already being produced by activities that are taking place across the organization whether they are:

- Implemented by privacy office: the privacy office has direct responsibility for performing the activity;
- Influenced by the privacy office: in some cases, the privacy office supports other parts of the organization in embedding privacy into operational practices; or
- Independent of the privacy office: the activity may be performed entirely within another part of the organization, and the privacy office observes with limited influence.

Realize Additional Benefits

Not only does the Scorecard answer the question 'how do we know the privacy program is effectively embedded throughout the organization?' it does so while providing additional benefits. Case studies have shown that users realize the following benefits, among others:

- **Shift accountability into operational units:** the Scorecard approach utilizes evidence from across the organization. Gathering information and collecting the evidence has been shown to be an effective first step in shifting accountability to the operational units, while encouraging open flow of information to the privacy office. Accountability in operational units is the key to embedding data privacy throughout the organization.
- **Reduce the burden on operational units:** The Scorecard's simple, straightforward approach to gathering evidence significantly reduces the time and energy invested by the operational units to support the privacy office needs, thereby motivating them to participate.
- **Attest compliance:** Evidence collected via the Scorecard for the purpose of demonstrating accountability can be re-purposed in order to provide evidence of compliance, in other words, to attest compliance.

Chapter 1. Drivers for Investing in a Privacy Program

Responsible organizations were processing personal data responsibly long before data privacy laws were enacted. Responsible organizations processed personal data responsibly as a result of corporate culture, a general adherence to societal values, and out of a desire to 'do the right thing'. These types of organizations were among the first to establish a **privacy office** and implement a formal **privacy program**. As a result, it is also these organizations that are taking the lead in implementing a workable framework to demonstrate that they are responsible and accountable.

This chapter outlines the drivers that motivate organizations to invest in their privacy program, or in other words, allocate resources to data privacy accountability. By investing in their privacy program, they ultimately establish the foundation for **demonstrating accountability**.

Laws and Regulations

The most straightforward justification for data privacy accountability is compliance with a law or regulation. This may include compliance with privacy and data protection laws, or compliance with other related laws and regulations such as employment law or industry self-regulation (e.g. PCI DSS), as they relate to the processing of personal data. For multinational organizations, risks related to cross border data flows (e.g. risk of penalties or enforcement actions) are often the compelling reason to invest resources in privacy management.

Increasingly, **Data Protection Authorities** (DPAs) around the world communicate their expectations for organizations to have an effective privacy program in place – to go a step further by adhering to the spirit of the law and not only the letter of the law. Appendix B: Demonstrating Accountability to Data Protection Authorities contains a more detailed discussion of this shift and provides recent examples of changes to

legislative and self-regulatory frameworks to incorporate the accountability principle and the requirement for organizations to be prepared to demonstrate to regulators on demand.

Enforcement Actions

Enforcement actions (e.g. a **consent decree**[1], fine, or sanction imposed by a regulatory body, court decisions) against an organization have an impact beyond direct monetary penalties and restrictions on business. Enforcement actions require investment in that organization's privacy program.

Another important, although less tangible impact of an enforcement action, is the impact on other organizations. Enforcement actions often clarify interpretation of the law, thereby motivating many organizations to adjust their approach accordingly or invest in relevant aspects of privacy management.

Data Breach

Most organizations that experience a significant **data breach** will increase investment in their privacy program in order to prevent reoccurrences.

A 2013 study by the Ponemon Institute estimated the total organizational cost of a data breach in the United States to average over USD$5.4 million. The consequences of a data breach are far reaching and go beyond the direct financial implications of responding to the breach. US organizations experienced over USD$3.03 million in lost business costs associated with data breach, including abnormal turnover of customers, increased customer acquisition activities, reputation losses, and diminished goodwill.[2]

Similar to an enforcement action, a related effect of a high profile data breach is the business case justification for other organizations to take measures to prevent a similar event.

Culture

Culture can be a driver for privacy management, both in the broader context of a society's norms and values and in terms of the corporate culture. Collective attitudes

[1] A consent decree is an enforcement mechanism in the United States which is a binding, voluntary agreement of a person or company to take specific actions (such as ceasing the conduct that is the subject of the suit/case) without admitting fault or guilt.
[2] Ponemon Institute. (2013). *2013 Cost of Data Breach Study: Global Analysis*. Traverse City, Michigan.

toward privacy vary across the world. Sometimes the justification for investing in privacy is simply because it is the right thing to do.

The organization's corporate culture and attitudes toward privacy are strongly influenced by the industry. Heavily regulated industries such as the public sector, financial services, healthcare, and telecommunications tend to place a higher priority on compliance. For example, organizations with a lower privacy risk profile (i.e. where processing personal data is not core to the business or tends to be less complex) such as manufacturing and industrials, may be inclined to take a more narrowly focused and cost-effective approach when implementing a privacy program.

Competitive Advantage

In some cases, organizations will promote their privacy programs to enhance their brand equity or position themselves more favourably in the marketplace. For example, **third party processors** may make claims to their corporate clients regarding their robust privacy program. Websites or technology companies may make statements to users about how they protect the **individual**'s information. To back these statements, investment in the privacy program is necessary.

The 2013 Consumer Data Privacy Study revealed that consumer privacy concerns were continuing to rise; 53% of UK[3] and 64% of US[4] consumers reported they were more concerned about privacy than in the prior year. As public awareness and expectations for privacy increase, it becomes increasingly important to establish and maintain trust.

Alignment with Organizational Initiatives

In some cases, privacy management becomes an area of focus because of its relationship to another important organizational project. Examples of such projects include: business process reengineering, a merger or acquisition, restructuring a functional unit such as Human Resources, customer service improvement initiatives, implementation of a new customer complaint tracking system, and IT security initiatives.

[3] TRUSTe. (2013). *UK 2013 Consumer Data Privacy Study - Advertising Edition.* United Kingdom.
[4] TRUSTe. (2013). *US 2013 Consumer Data Privacy Study - Advertising Edition*. United States.

Business Partner Expectations

Many organizations are, at least in some capacity, processing personal data on behalf of partner organizations and entrusted to protect it. These organizations often have legal and contractual obligations related to the protection of the personal data. Failure to process data responsibly could result in the loss of the contract, directly impacting the future livelihood of the organization as well as creating the risk of subsequent legal action.

New Privacy Officer

Anecdotally, based on Nymity's experience, one of the largest influences on an organization's privacy program is the **privacy officer**. Over the years, Nymity has observed many examples where one person within an organization influences large teams of individuals within operational units (outside the privacy office budget) to accomplish privacy objectives.

Excess Budget (just kidding)

Sometimes an organization just has too much money to spend, and decides to invest it in privacy. Just kidding!

In summary, investment in the privacy program builds over time. Nymity has identified some of the drivers, recognizing that most organizations are motivated by a combination of these and other factors. For example, a new privacy officer establishes a program, a new law results in further investment, and a breach results in allocation of more resources. By investing in their privacy program, organizations establish the foundation for demonstrating accountability.

Chapter 2. Elements of Data Privacy Accountability

Accountability was first established as a privacy principle over 30 years ago when the Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Data Flow* placed responsibility on organizations "for complying with measures that give effect" to all of the OECD principles.[5] In July 2013, the OECD Guidelines were updated with guidance on implementing accountability, thus emphasizing and clarifying the importance of accountability:[6]

> *In recent years, the principle of accountability received renewed attention as a means to promote and define organisational responsibility for privacy protection. Building on this experience, the new Part Three of the Guidelines ("Implementing Accountability") introduces the concept of a privacy management programme and articulates its essential elements.*

Definitions of accountability vary slightly and have evolved over the years[7], but are generally aligned on the importance of maintaining an effective privacy program, and being able to show that the organization has an established privacy program in place

[5] OECD. (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.
[6] OECD. (2013). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*
[7] When the concept of accountability was introduced in 1980 in the OECD Guidelines, the accountability principle was intended to serve two purposes: (1) to identify the data controller as the entity responsible (meaning, the organization that collected the data was responsible for protecting it even if it was transferred to a third party); and (2) to encourage Member Countries to institute mechanisms which ensure that data controllers are held answerable in the event that responsibility is not met. The Guidelines did not specify to whom the data controller should be accountable. Twenty years later, Canada's Federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) went on to require organizations 'to implement policies and practices to give effect to the principles' and to more explicitly outline the requirements for responsible organizations. Alhadeff, J., & Van Alsenoy, B., & Dumortier, J. (2011). *The accountability principle in data protection regulation: origin, development and future directions*. Berlin.

– in other words, "demonstrate accountability". Nymity does not propose an alternative definition of the term "data privacy accountability". On the contrary, Nymity has leveraged existing definitions to break down accountability into key elements.

The **Article 29 Working Party** describes Accountability as, "showing how responsibility is exercised and making this verifiable."[8] This definition highlights the fundamental elements of accountability: responsibility, ownership, and evidence. Each of these is necessary for demonstrating accountability and to remove or weaken any one of these elements would prevent the organization from being accountable.

In the following section, Nymity discusses the three key elements of data privacy accountability:

1. Responsibility

The organization maintains an effective privacy program consisting of ongoing Privacy Management Activities.

The foundation for data privacy accountability is responsibility; therefore, only a responsible organization can be accountable.

> *Responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed. – Article 29 Working Party*[9]

Responsible organizations manage their privacy programs via ongoing **Privacy Management Activities**. Privacy Management Activities are ongoing activities that

[8] Article 29 Data Protection Working Party. (2010). *Opinion 3/2010 on the Principle of Accountability.* Belgium.
[9] Article 29 Data Protection Working Party. (2010). *Opinion 3/2010 on the Principle of Accountability.* Belgium.

have a positive impact on the processing of personal data. Privacy Management Activities vary between organizations as widely as the purposes for processing personal data and the types of personal data being processed.

2. Ownership

An individual is answerable for the management and monitoring of the Privacy Management Activities.

Ownership is the second element of accountability and builds upon responsibility. Ownership requires accountability at both an individual and organizational level.

When an individual is assigned responsibility for the management and monitoring of the Privacy Management Activity, he or she is the **Owner**. The Owner does not necessarily complete the Privacy Management Activity, but is ultimately responsible or answerable for it.

> *Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations. Accountability goes beyond responsibility by obligating an organization to be answerable or its actions. – Office of the Information Privacy Commissioner of Ontario*[10]

Ownership related to data privacy accountability requires that the organization be accountable or answerable to a variety of stakeholders including data subjects/individuals, regulators, and business partners.

3. Evidence

Documentation supports the completion of Privacy Management Activities.

The third element of data privacy accountability is **evidence**. In responsible organizations, the Owner of a Privacy Management Activity provides supporting evidence that the activity was completed.

[10] Abrams, M. E., Cavoukian, A., Taylor, S. (November 2009) *Privacy by Design: Essential for Organization Accountability and Strong Business Practices.* Toronto, Canada.

Alignment of Responsibility, Ownership, and Evidence across Definitions of Data Privacy Accountability

As the three elements of data privacy have now been discussed, Nymity will examine some common definitions of data privacy accountability to illustrate how responsibility, ownership, and evidence are aligned with these definitions.

Definition A: Article 29 Working Party Opinion on the Principle of Accountability

The Article 29 Working Party describes accountability as "showing how responsibility is exercised and making this verifiable," and goes on to describe how an accountability principle would be implemented:

> *A statutory accountability principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request.*[11]

Responsibility: The definition references a privacy program that consists of ongoing Privacy Management Activities ("appropriate and effective measures").

Ownership: While the definition does not explicitly reference ownership, the paper states that "the allocation of resources including the designation of individuals who are responsible for the organization of data protection compliance are examples of such measures (that deliver the outcomes of the data protection principles)."

Evidence: The definition references the need for supporting evidence ("demonstrate this on request").

Definition B: Data Protection Accountability: The Essential Elements

The Galway Project was an effort initiated in January 2009 by the Centre for Information Policy Leadership, an international group of experts from government, industry, and academia to define the essential elements of accountability and consider how an accountability approach to information privacy protection would work in practice.[12] The project defines accountability as follows:

> *Accountability is the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations.*

[11] Article 29 Data Protection Working Party. (2010). *Opinion 3/2010 on the Principle of Accountability.* Belgium.
[12] Centre for Information Policy Leadership. (2009). *Data Protection Accountability: The Essential Elements A Document for Discussion.* Washington, DC.

> *Accountability goes beyond responsibility by obligating an organization to be answerable for its actions.*

The essential elements of accountability are:

1. An organization's commitment to accountability and adoption of internal policies consistent with external criteria;
2. Mechanisms to put privacy policies into effect, including tools, training, and education;
3. Systems for internal ongoing oversight and assurance reviews and external verification;
4. Transparency and mechanisms for individual participation; and
5. The means for remediation and external enforcement.

Responsibility: The definition references a program that consists of ongoing Privacy Management Activities within the five essential elements of accountability.

Ownership: The definition clarifies that "accountability goes beyond responsibility by obligating an organization to be answerable for its actions."

Evidence: The definition references the need for supporting evidence and a "willingness to demonstrate" said evidence.

Definition C: Getting Accountability Right with a Privacy Management Program

The Office of the Privacy Commissioner of Canada and the Offices of the Information and Privacy Commissioners of Alberta and British Columbia in the 2012 paper, 'Getting Accountability Right with a Privacy Management Program'[13] define data privacy accountability as follows:

> *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.*

[13] Office of the Information and Privacy Commissioner of Alberta. (2012).*Getting Accountability Right with a Privacy Management Program.* Alberta, Canada.

Responsibility: The definition references a program that consists of ongoing Privacy Management Activities, also known as "appropriate **policies** and procedures that promote good practices".

Ownership: While the definition does not explicitly reference ownership, the paper states that "someone must be assigned responsibility for overseeing the organization's compliance with applicable privacy legislation. Other individuals may be involved in handling personal information, but the privacy officer is the one accountable for structuring, designing, and managing the program."

Evidence: The definition references the need for supporting evidence ("demonstrable") and the paper goes on to state that, "organizations will be able to demonstrate to customers, **employees**, partners, shareholders, and privacy commissioners that they have in place a robust privacy compliance program. They will be able to describe and document all of the elements outlined in this guidance document and show evidence of how they have implemented their program."

This chapter has outlined the key three elements of data privacy accountability, demonstrated how they align with common definitions, and established a foundation for a discussion on how to put these concepts into practice as discussed in the next chapter: Accountability in Practice.

Chapter 3. Accountability in Practice

This chapter discusses privacy management in the context of Responsibility, Ownership, and Evidence. Organizations with established privacy programs will likely discover that their existing programs are already closely aligned with the accountability approach described. Organizations with new or developing privacy programs may find greater benefit by first reading Chapter 7: Getting to Accountability.

Privacy Management Activities

The Nymity Privacy Management Accountability Framework ("Framework") was developed to communicate the status of the privacy program, in other words for "demonstrating accountability." The Framework is a comprehensive, jurisdiction- and industry-neutral listing of 150+ Privacy Management Activities within 13 **Privacy Management Processes**. It is based on extensive research conducted by Nymity, with input from organizations around the world across a spectrum of industries and sectors.

Privacy Management Processes

1. Maintain Governance Structure
2. Maintain Personal Data Inventory
3. Maintain Data Privacy Policy
4. Embed Data Privacy into Operations
5. Maintain Training and Awareness Program
6. Manage Information Security Risk
7. Manage Third-Party Risk
8. Maintain Notices
9. Maintain Procedures for Inquiries and Complaints
10. Monitor for New Operational Practices
11. Maintain Data Privacy Breach Management Program
12. Monitor Data Handling Practices
13. Track External Criteria

The Nymity Privacy Management Accountability Framework is:

- **Practical**: the framework is structurally aligned with how organizations build and maintain their privacy programs;
- **Flexible**: the activities within the framework can be tailored to meet the unique needs of any organization;

- **Global**: Privacy Management Activities are industry and jurisdiction neutral;
- **Dynamic**: the framework continues to evolve as quickly as the privacy landscape – Nymity's research is ongoing and the framework is continually updated to reflect new developments in privacy management.

Examples of Privacy Management Activities are provided later in this chapter. A complete list can be found in Appendix A: Nymity Privacy Management Accountability Framework™. To obtain the most recent version of the Privacy Management Activity Framework, contact Nymity.

Privacy Management Activities in the Context of Accountability

The following section expands on the three key elements of accountability: responsibility, ownership, and evidence to illustrate how Privacy Management Activities align with each element.

1. Responsibility

The organization maintains an effective privacy program consisting of ongoing Privacy Management Activities.

Responsible organizations manage their privacy programs via ongoing Privacy Management Activities. The activities may vary between different organizations as do the purposes for processing personal data and the types of personal data being processed.

Two Tiers of Privacy Management Activities: Core and Elective

In a privacy program, not all Privacy Management Activities are considered equal. Some activities are more important than others. Some activities can be categorized as fundamental, mandatory, or core. Other activities can be categorized as desired, ideal, surpassing compliance, optional, or elective.

To simplify the concept of responsibility, Nymity will discuss two tiers of activities: Core and Elective.

Core activities are defined by the privacy office as fundamental to privacy management. These fundamental activities will vary from one organization to the next and will be influenced by the industry/sector as well as jurisdiction. Core activities may even vary within an organization.

> *Some of the measures are 'staples' that will have to be implemented in most data processing operations. Drafting internal policies and procedures implementing the principles (procedures to handle access requests, complaints) may constitute examples of appropriate measures for some processing of data. The suitability of measures will need to be decided on a case-by-case basis. – Article 29 Working Party*[14]

Elective activities are desired activities defined and supported by the privacy office. These activities are encouraged, but not required. Elective activities are often considered 'above and beyond' the minimum requirements for the processing of personal data.

> *One could also imagine situations where the data controller wishes to exceed the minimum requirements that are embedded in the general legal framework. For example, a data controller may decide to appoint a data protection officer even though this is not mandatory under existing law… The Article 29 Working Party applauds these initiatives and encourages the new data protection legal framework to provide incentives for data controllers to do so. –Article 29 Working Party*[15]

Table 3.1 illustrates examples of Core and Elective Privacy Management Activities within various industries and sectors. As mentioned above, the activities are defined by the privacy office and are different for each organization.

Industry/Sector	Core Activity Examples	Elective Activity Examples
Public Sector	Register databases with data protection authority (where registration is required)	Integrate data privacy into social media practices
Healthcare	Maintain administrative and technical measures to encrypt personal data in transmission and at rest, including removable media	Maintain customer Frequently Asked Questions
Financial Services	Maintain a breach notification (to affected individuals) and reporting (to regulators, credit	Maintain data privacy incident/breach metrics (e.g.

[14] Article 29 Data Protection Working Party. (2010). *Opinion 3/2010 on the Principle of Accountability.* Belgium.
[15] Article 29 Data Protection Working Party. (2010). *Opinion 3/2010 on the Principle of Accountability.* Belgium.

Industry/Sector	Core Activity Examples	Elective Activity Examples
	agencies, law enforcement) and protocol	nature of breach, risk, root cause)
Pharmaceuticals	Integrate data privacy into research practices	Conduct assessments through use of an accountability agent or third-party verification
Retail	Integrate data privacy into e-mail marketing practices	Integrate data privacy into behavioural advertising practices
Manufacturing	Conduct due diligence around the data privacy and security posture of potential vendors/processors	Integrate data privacy into health & safety practices
Not for Profit	Provide data privacy notice at all points where personal data is collected	Attend/participate in privacy conferences, industry association, or think-tank events
Lottery & Gaming	Integrate data privacy into use of CCTV/video surveillance	Obtain data privacy breach insurance coverage
Education	Maintain procedures to respond to access requests	Require completion of data privacy training as part of performance reviews
Telecommunications	Maintain policies/procedures for secondary uses of personal data	Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures

Table 3.1 - Core and Elective Privacy Management Activities by Industry/Sector - Examples

Table 3.2 illustrates examples of Core and Elective Privacy Management Activities related to various legislative requirements and frameworks, within the context of both internal and external compliance requirements.

Compliance Requirement	Core Activity Examples	Elective Activity Examples
Legislative Requirements		
UK Data Protection Act 1998	Register databases with data protection authority (where registration is required) Appoint a representative in member states where the organization does not maintain a physical presence	Maintain ongoing awareness material (e.g. posters, intranet, and videos) Maintain backup and business continuity plans

Compliance Requirement	Core Activity Examples	Elective Activity Examples
Mexico Regulation of the Federal Law on Protection of Personal Data Held by Private Parties	Maintain policies/procedures for collection and use of sensitive personal data (including biometric data) Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) and protocol	Conduct a Privacy Risk Assessment Document that new requirements have been implemented (also document where a decision is made to not implement any changes, including reason)
Hong Kong Personal Data Privacy Ordinance	Maintain procedures to respond to access requests Maintain a data privacy notice that details the organization's personal data handling policies	Maintain policies/procedures for collection and use of sensitive personal data (including biometric data) Conduct one-off, one-time tactical training and communication dealing with specific, highly-relevant issues/topics
Self-Regulatory Frameworks		
US-EU Safe Harbor	Maintain procedures to execute contracts or agreements with all processors Maintain policy/procedure for secondary uses of personal data	Maintain data privacy incident/breach metrics (e.g. nature of breach, risk, root cause) Maintain job descriptions for individuals responsible for data privacy (e.g. data protection officers)
Binding Corporate Rules	Require employees to acknowledge and agree to adhere to the data privacy policies Maintain a core training program for all employees	Consult with stakeholders throughout the organization on data privacy matters Integrate data privacy into use of cookies and tracking mechanisms
APEC Cross Border Privacy Rules	Assign accountability for data privacy at a senior level Conduct assessments through use of an	Maintain subscription to compliance reporting service/law firm updates to stay informed on new developments

Compliance Requirement	Core Activity Examples	Elective Activity Examples
	accountability agent or third-party verification	Maintain certification for individuals responsible for data privacy, including continuing professional education
Control Frameworks		
AICPA/CPA Canada Generally Accepted Privacy Principles	Maintain an information security policy Allocate resources to adequately implement and support the privacy program (e.g. budget, personnel)	Maintain a Code of Conduct Conduct regular communication between individuals accountable and responsible for data privacy
NIST Guidelines Privacy Control Catalog SP800-53 Appendix J	Maintain a Privacy by Design framework for all system and product development Maintain an inventory of key personal data holdings (what personal data is held and where)	Maintain an internal data privacy intranet, privacy blog, or repository of privacy FAQs and information Engage a breach response remediation provider
Internal Compliance		
Data Privacy Policy	Conduct training for newly appointed employees upon assignment to privacy-sensitive positions Maintain a product sign-off procedure that involves the privacy office	Maintain ongoing awareness material (e.g. posters, intranet, and videos) Review long-term contracts for new or evolving data protection risks
Contracts with Business Partners/Vendors	Maintain human resource security measures (e.g. pre-screening, performance appraisals) Maintain policies/procedures for secure destruction of personal data	Integrate data privacy into e-discovery practices Report periodically on the status of the privacy program to external stakeholders, as appropriate (e.g. annual reports, third-parties, clients)

Table 3.2 - Example Core and Elective Privacy Management Activities by Compliance Requirement

Ongoing Privacy Management Activities

Responsible organizations do not treat privacy as a project, although in many cases the program may have started as a project. On the contrary, a responsible organization sufficiently allocates resources to its privacy program and continually revaluates its program needs to ensure that the Privacy Management Activities are aligned.

> *A privacy management program should never be considered a finished product; it requires ongoing assessment and revision in order to be effective and relevant. The building blocks must be monitored and assessed on a regular basis and be updated accordingly. – Getting Accountability Right*[16]

A privacy program is a set of processes, each made up of ongoing activities. These activities are performed either periodically or continuously.

- **Periodic activities** are performed on a set **Frequency**, e.g. quarterly or annually. These activities are treated as discrete projects or tasks with a defined start and end.
- **Continuous activities** are embedded into day-to-day operations. These activities often take a repetitive approach, wherein adjustments are made continuously toward the desired outcome.

Table 3.3 reviews of Privacy Management Activities and how the two approaches for the frequency of activities might differ:

Privacy Management Activity	Periodic	Continuous
Maintain flow charts for key data flows	On an annual basis, require that key stakeholders review the flow charts for accuracy and update the diagrams as necessary	Implement as part of the project management requirements that proposed changes to data flows are identified and the flow charts are updated as a condition of project sign-off

[16] Office of the Information and Privacy Commissioner of Alberta. (2012).*Getting Accountability Right with a Privacy Management Program.* Alberta, Canada.

Privacy Management Activity	Periodic	Continuous
Measure participation in data privacy training activities	Each quarter, review reports generated by the e-Learning system to determine whether all employees have completed the requirements	Configure the e-Learning system to generate alerts when an employee has not completed the training by the required date and send a message to the employee's manager suggesting he or she follow up immediately
Consult with stakeholders throughout the organization on data privacy matters	Establish a cross-functional committee of privacy stakeholders (e.g. IT, Marketing, Legal, HR, etc.) who meet on a quarterly basis to discuss data privacy matters	Create an email alias or group discussion for data privacy stakeholders, to facilitate communication on data privacy matters
Maintain procedures to restrict access to personal information (e.g. role-based access, segregation of duties)	On a monthly basis, review reports of active system users to ensure their access is still appropriate and sign- off to indicate approval	Configure the HR system to send alerts to Information Security when employees are terminated or when there are changes to the job title, department, or reporting structure

Table 3.3 - Examples of Periodic and Continuous Approaches to Privacy Management Activities

Whether the activity should be performed periodically or continuously depends on a number of factors. Periodic activities may encourage structure, whereas continuous activities may provide more thorough coverage and risk prevention.

2. Ownership

An individual is answerable for the management and monitoring of the Privacy Management Activities.

In responsible organizations, the concept of ownership is typically embedded into the governance structure of a privacy program. Roles are clearly defined and all key players understand where they fit within the overall organizational structure, as well as, how their actions and decisions impact the privacy program as a whole.

Various organizational structures of a privacy program are as follows:[17]

- **Centralized**: One team or person is responsible for privacy-related affairs; often this point of contact is the Chief Privacy Officer or privacy office.
- **Local or Decentralized**: Decision making authority is delegated to lower levels in an organization, and there is a bottom-to-top flow of decision making and flow of ideas.
- **Hybrid**: Combination of centralised and local governance where the organization assigns a main individual or group responsible for issuing policies and directives to the rest of the organization, and local entities fulfil and support the policies and directives.

Ownership within the Privacy Office

In any structure, the privacy office is accountable for data privacy. However, the privacy office itself processes very little personal data, if any. Although the privacy office has little direct control over the processing of personal data, it is their responsibility to manage and monitor the Privacy Management Activities that ensure the processing is done responsibly.

> *…someone must be assigned responsibility for overseeing the organization's compliance with applicable privacy legislation. Other individuals may be involved in handling personal information, but the Privacy Officer is the one accountable for structuring, designing and managing the program, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up. - Getting Accountability Right*[18]

Ownership within Operational Units

The effectiveness of the privacy program relies on the appropriate Privacy Management Activities being performed at all points of the personal data life cycle, from the point of collection to the point of destruction. Ownership of some Privacy Management Activities will reside within the **operational units**, as that is where the data is being collected and processed.

---

[17] Densmore, R, R. (2013). *Privacy Program Management: Tools for Managing Privacy within Your Organization.* An IAPP Publication. United States.
[18] Office of the Information and Privacy Commissioner of Alberta. (2012).*Getting Accountability Right with a Privacy Management Program.* Alberta, Canada.

Table 3.4 provides examples of Privacy Management Activities within each of the 13 Privacy Management Processes which are performed by various stakeholders within the organization.

Privacy Management Process	Activities Owned by the Privacy Office – Examples	Activities Owned by Operational Units – Examples
1. Maintain Governance Structure	Maintain a Privacy Strategy	Owner: Human Resources Require employees to acknowledge and agree to adhere to the data privacy policies
2. Maintain Personal Data Inventory	Maintain an inventory of key personal data holdings (what personal data is held and where)	Owner: Corporate Records Management Classify personal data holdings by type (e.g. sensitive, confidential, public)
3. Maintain Data Privacy Policy	Maintain a data privacy policy	Owner: Human Resources Maintain a separate employee data privacy policy
4. Embed Data Privacy Into Operations	Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)	Owner: Marketing Integrate data privacy into direct marketing practices
5. Maintain Training and Awareness Program	Maintain a core training program for all employees	Owner: Customer Service Integrate data privacy into other training programs, such as HR, security, call centre, retail operations training
6. Manage Information Security Risk	Maintain an acceptable use of information resources policy (likely performed in conjunction with Information Security)	Owner: Information Security Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
7. Manage Third Party Risk	Maintain a vendor data privacy risk assessment process	Owner: Legal Maintain internal guidelines for contract templates that establish data privacy obligations in all contracts and agreements

Privacy Management Process	Activities Owned by the Privacy Office – Examples	Activities Owned by Operational Units – Examples
8. Maintain Notices	Maintain a data privacy notice that details the organization's personal data handling policies	Owner: Facilities/Corporate Security Provide notice by means of on-location signage, posters
9. Maintain Procedures for Inquiries and Complaints	Maintain procedures to investigate root causes of data protection complaints	Owner: Call Centre Maintain procedures to address complaints
10. Monitor for New Operational Practices	Maintain PIA guidelines and templates	Owner: Information Technology Conduct PIAs for new programs, systems, processes
11. Maintain Data Privacy Breach Management Program	Maintain a documented data privacy incident/breach response protocol	Owner: Legal: Engage a forensic investigation team
12. Monitor Data Handling Practices	Maintain privacy program metrics	Owner: Internal Audit: Conduct audits/assessments of the privacy program outside of the privacy office (e.g. Internal Audit)
13. Track External Criteria	Maintain subscription to compliance reporting service/law firm updates to stay informed on new developments	Owner: Compliance: Document that new requirements have been implemented (also document where a decision is made to not implement any changes, including reason)

Table 3.4 – Examples of Activities Owned by the Privacy Office and Operational Units

Ownership Cannot be Outsourced

Ownership for each Privacy Management Activity ultimately resides within the organization and cannot be **outsourced** to third party data processors. When the activities are performed by a third party, the organization must maintain oversight as it is the organization that is accountable to the data subjects, regulators, and business partners.

3. Evidence

Documentation supports the completion of Privacy Management Activities.

When Privacy Management Activities are performed on an ongoing basis, evidence is produced. As we will see in the next chapter, this evidence is required for demonstrating accountability.

Documentation Serves as Evidence

Evidence is documentation which can be provided in two forms: formal and informal. Refer to Table 3.5 for the characteristics of formal and informal documentation and corresponding examples:

Documentation	Characteristics	Examples
Formal	Typically published, maintained, and communicated to designated groups	Policies, Procedures, Reports
Informal	May show an example of an activity having occurred, such as an e-mail conversation between two key individuals or record of participation in a webinar	Email communication, meeting agendas, system logs

Table 3.5 – Characteristics of Formal and Informal Documentation

There are various sources of documentation available for the privacy office to monitor, and often the privacy office will have a role in the production of the documentation.

Table 3.6 describes the role that the privacy office plays depending on the source of the documentation, as well as corresponding examples of the document types:

Source	Privacy Office Role	Example Documents
Produced Generated by the privacy office with input from other key stakeholders	The privacy office performs the activity	Data Privacy Policy Privacy Notice Data Privacy Training Curriculum Privacy Impact Assessment Guidelines Policy/procedure for secondary uses of personal data

Source	Privacy Office Role	Example Documents
Influenced Influenced by the privacy office but created by other stakeholders	Input or opinions are provided by the privacy office	Direct Marketing Procedures Privacy Impact Assessments Employment Policies Records retention schedules
Collected Provided to the privacy office by other stakeholders	The privacy office is kept up-to-date on progress, often only upon completion	Internal Audit Results IT Security Assessment Results Business Continuity Plans

Table 3.6 – The Privacy Office's Role in Production of Documentation

Table 3.7 outlines how formal and informal documentation can be produced, influenced, or collected by the privacy office as evidence of the Privacy Management Activities.

Privacy Management Activities	Evidence/ Documentation	Source/ Role	Formal/ Informal
Maintain a data privacy policy	Data Privacy Policy	Produced by privacy office	Formal
Integrate data privacy into e-mail monitoring practices	E-mail monitoring policy and procedure	Influenced by privacy office Produced by Information Technology	Formal
Measure comprehension of data privacy concepts using exams	System generated report of data privacy exam scores	Collected by privacy office Produced by Human Resources	Informal
Provide notice in all marketing communications (e.g. emails, flyers, offers)	Examples of e-mail marketing communications	Influenced by privacy office Produced by Marketing	Informal

Table 3.7 - Formal and Informal Documentation

An organization that has embedded responsibility, ownership, and evidence into the privacy program has implemented accountability and is now equipped to demonstrate accountability.

Chapter 4. Demonstrating Accountability Using a Scorecard

Increasingly organizations with established privacy programs seek a practical, scalable approach to monitor, measure, and report ongoing Privacy Management Activities, in other words to demonstrate accountability. This chapter introduces the Nymity Data Privacy Accountability Scorecard ("Scorecard"), a framework which enables responsible organizations to demonstrate accountability. This chapter provides an overview of this approach, as well as an illustrative example. Throughout the chapter "Implementation Notes" will highlight lessons learned from successful implementations of the Scorecard.

Nymity Data Privacy Accountability Scorecard

The Scorecard is a pragmatic, scalable, evidence-based framework that allows organizations to demonstrate accountability by monitoring, measuring, and reporting ongoing Privacy Management Activities. The Scorecard is based on the three key elements of accountability outlined in previous chapters: responsibility, ownership, and evidence.

This section provides an overview of the steps to implement the Scorecard in any organization. The steps are the same regardless of whether it is a small entity using Nymity's free Microsoft Excel® based Scorecard template[19] ("Scorecard

[19] Free templates, guidelines, and other resources are available at www.scorecard.nymity.com or by contacting Nymity.

Spreadsheet") or a large organization using Nymity's automated software solution, Nymity Attestor™[20] ("Attestor").

1. Setup Scorecard

A) Identify and Categorize Privacy Management Activities

The privacy office first needs to identify all the Privacy Management Activities currently being completed and those that are desired or planned. Each Privacy Management Activity is then categorized as either Core or Elective.

- **Core**: Core activities are defined by the privacy office and are fundamental to privacy management within that organization. These fundamental activities vary between organizations and will be influenced by the industry/sector, as well as jurisdiction.
- **Elective**: Elective activities are encouraged, but not required. Elective activities are often considered 'above and beyond' the minimum requirements for the responsible processing of personal data.

Core and Elective Privacy Management Activities are discussed in greater detail in the previous chapter, Accountability in Practice.

B) Determine Ownership and Frequency

For each Privacy Management Activity, an Owner and Frequency must be defined.

- **Owner**: The Owner may be the privacy office, or an operational unit. Note that the Owner does not necessarily complete the Privacy Management Activity, but is ultimately responsible or answerable for it.
- **Frequency**: Note that all Privacy Management Activities must be performed on an ongoing basis – either periodic or continuous. For each Privacy

[20] The Attestor solution is a privacy management platform that enables an organization to demonstrate privacy accountability and compliance. For additional information, please refer to Chapter 5 or contact Nymity.

Management Activity, the privacy office determines the appropriate Frequency at which Evidence should be provided. The frequency at which evidence is provided is not necessarily the frequency at which the activity is performed. For example, for activities which are performed continuously it may be sufficient to provide summary evidence on a monthly or quarterly basis.

C) Create Evidence Collection Questions

For each Privacy Management Activity, the privacy office creates one or more **Evidence Collection Questions**. These are closed questions that would best compel the Evidence from Owners. Closed ended questions must be answered with 'yes' or 'no' to enable quantitative analysis.

IMPLEMENTATION NOTE

The best Evidence Collection Questions are simple, straightforward, and written in the language of the Owner who is to respond.

A benefit of the Scorecard is that it enables the privacy office to engage with stakeholders throughout the organization, even if they are not privacy experts. For example, if the goal is to compel Evidence to support the Privacy Management Activity "Conduct regular communication between individuals accountable and responsible for data privacy" it is better to specify the desired outcome within the question rather than rephrasing the activity as a question. Asking "Do individuals accountable and responsible for data privacy communicate regularly?" is not nearly as effective as "Do the Privacy Liaisons meet with the Central Privacy Team on a quarterly basis?" The individual responding will know exactly what is expected and the task of providing evidence will be much less onerous.

2. Collect Evidence

After the Scorecard is set up by the privacy office, the next step is to collect Evidence. The privacy office gathers responses to the Evidence Collection Questions, and Evidence to support the Responses.

- **Response**: The **Response** contains two parts: (1) – a 'yes' or 'no' response to the Evidence Collection Question, and (2) a comment to provide additional context.

IMPLEMENTATION NOTE

Often Scorecard users' initial reaction to the 'yes/no' requirement is concern that the responses 'partially' or 'not applicable' are not available.

When it seems the response should be 'not applicable', re-evaluate why the question is being asked in the first place. If it seems the answer should be 'partially' or 'sometimes', consider asking two separate questions or adding a qualifier. For example, 'Do all employees complete data privacy training?' may be more valuable when worded as 'Do employees with access to personal information complete data privacy training?'

- **Evidence**: All 'yes' responses require Evidence. As mentioned in the previous chapter, there are a number of sources of Evidence available, both informal and formal. The privacy office may log the Evidence via a link to a URL or a description as to where that document can be found.

IMPLEMENTATION NOTE

In order to demonstrate accountability, Evidence must be available to support the Responses – but it does not necessarily have to be attached. In the Attestor solution, only meta-data is captured (e.g. Title, Description, URL) in the Evidence Library. In the Scorecard Spreadsheet template, it may be sufficient to simply note the filename so that users can find it later if necessary.

3. Calculate Data Privacy Accountability Score

The **Data Privacy Accountability Score** represents the status of the privacy program as a percentage of the Core and Elective Privacy Management Activities which are being completed and evidenced on an ongoing basis. The Score is calculated by dividing the number of activities for which the Owner has provided Evidence (i.e. the Response is "Yes"), by the number of activities identified by the privacy office. The result equals the percentage of activities that are evidenced as of that specific date.

% Managed = # of Core Activities Evidenced ÷ # of Core Activities

When all Core activities are evidenced, the privacy program is considered 100% Managed and has thus reached the **target score**. A privacy program that performs

Elective activities above and beyond the minimum requirements for responsible data processing achieves a % Advanced score.

% Advanced = # of Elective Activities Evidenced ÷ # of Elective Activities

IMPLEMENTATION NOTE

Configuring the Scorecard (identifying activities, formulating questions, assigning ownership, etc.) requires the expertise of the privacy professional familiar with the organization's program objectives. Calculating the score, however, does not.

As such, it is easy to compare different areas of the organization, as well as review performance over time. An 80% Managed score in one area can be compared "apples to apples" to an 80% Managed score in a completely different jurisdiction or business area.

Until the target of 100% Managed is reached, the percentage Advanced is depicted as a **Potential Score**. In other words, Elective activities do not affect the Data Privacy Accountability Score until all Core activities are completed. Even though the Elective activities do not affect the overall score, the privacy office can still account for them and collect Evidence. This allows the privacy office to gain a holistic view of the privacy program.

IMPLEMENTATION NOTE

Nymity has obtained feedback from many privacy professionals from organizations, law firms, regulators and others to validate the concept and obtain feedback which has been consistently positive. One individual was particularly pleased with the concept of the Potential Score, to paraphrase: "You can't hand out 'I Love Privacy' balloons to make up for the fact that you don't have good procedures in place, but you still get credit for trying."

4. Scorecard Management

As stated in earlier chapters, Privacy Management Activities must be ongoing and Evidence needs to be updated or reaffirmed. As such, the Scorecard must be maintained - it may be updated on a periodic basis (e.g. monthly, quarterly or annually) or in the interim when the response changes (i.e. a new activity is evidenced).

IMPLEMENTATION NOTE

Scorecard implementations have been successful in organizations ranging from large, mature multinationals to privacy programs in the early stages. Nymity hears repeatedly that Scorecard users experience benefits that reach beyond the ability to monitor, measure, and report on their privacy program.

One benefit is that the process of managing the Scorecard increases engagement amongst the broader team and helps to embed privacy throughout the organization. The Scorecard encourages regular communication and collaboration between the privacy office and individuals responsible for Privacy Management Activities within the operational units. Activity Owners obtain a better understanding of the expectations, and having access to a centralized resource allows them to collaborate and learn from one another.

Given that the Privacy Management Activity has a Frequency assigned, the Owners need to provide new Evidence or verify with existing Evidence that the activity was completed. If the individual completes and provides Evidence for this activity within the Frequency set by the privacy office, then the Score remains the same, but if the individual does not the Score will decrease.

Demonstrating Accountability – An Illustrative Example

The following section illustrates how to put the Scorecard into practice. For additional resources including a training video and a sample of a completed Scorecard Spreadsheet, visit www.scorecard.nymity.com

1. Setup Scorecard

Setting up the Scorecard requires collaboration between the Privacy Office and Owners throughout the operational units. Stakeholders should be engaged throughout the process of identifying and categorizing Privacy Management Activities, developing Evidence Collection Questions, and assigning an Owner and Frequency.

Selected Privacy Management Activity	Category	Evidence Collection Question	Owner	Frequency
Maintain a data privacy policy	Core	Is the Data Privacy Policy reviewed based on legislative and operational changes?	Privacy Office	Annual

Selected Privacy Management Activity	Category	Evidence Collection Question	Owner	Frequency
Maintain internal guidelines for contract templates that establish data privacy obligations in all contracts and agreements	Core	Do third party contracts contain organizational standard privacy language?	Legal	Annual
Conduct PIAs for new programs, systems, processes	Core	Are Privacy Impact Assessments (PIAs) completed for all new uses of personal data?	Marketing	Semi-Annual
Attend/participate in privacy conferences, industry association, or think-tank events	Elective	Does the privacy office attend conferences and other events to learn about new developments in data privacy?	Privacy Office	Annual

Table 4.1 – Example of How to Setup the Scorecard

2. Collect Evidence

The figure below provides a snapshot of the Evidence Collection Worksheet completed with Responses, Comments, and an Evidence Log.

NYMITY Data Privacy Accountability Scorecard™

Evidence Worksheet
www.scorecard.nymity.com

1
3/15/2013

% Managed (core activities completed and evidenced) 64% Managed - 7 out of 11 core activities
% Advanced (elective activities completed and evidenced) 29% Advanced - 2 out of 7 elective activities

Core Activities

ID#	Question	Owner	Frequency	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.	
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.
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).

Figure 4.1 - Collecting Evidence using the Scorecard Spreadsheet

The Attestor collects the same information, but allows meta-data about the Evidence to be indexed and re-used for additional purposes, such as attesting compliance (discussed further in Chapter 5: Attesting Compliance).

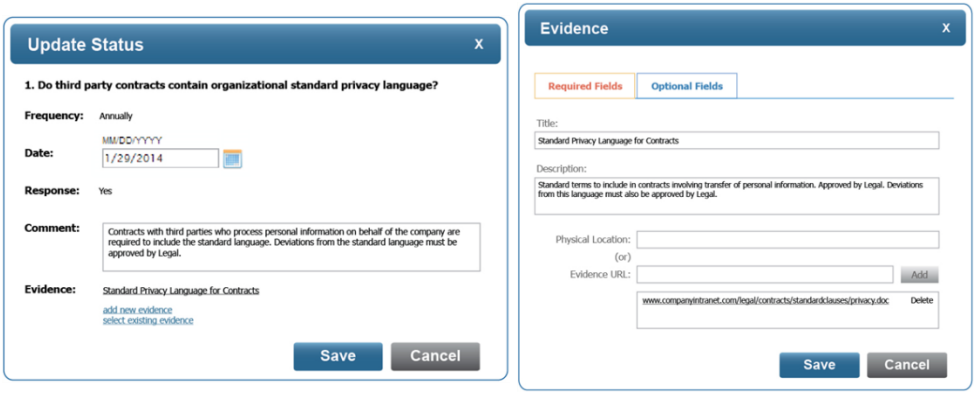


Figure 4.2 - Collecting Evidence using Nymity Attestor

3. Calculate Data Privacy Accountability Score

The Data Privacy Accountability Score is automatically calculated based on the percentage of Core and Elective activities completed and evidenced.

The Scorecard Spreadsheet allows up to 25 Core and 25 Elective activities and automatically calculates and plots the Score. For more complex implementations, the Attestor allows for weighting of each Privacy Management Activity.

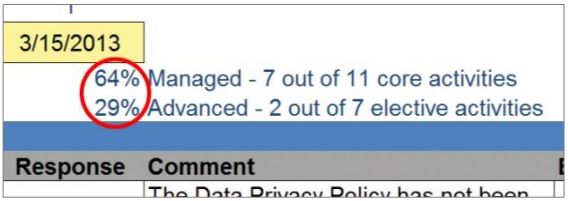


Figure 4.3 Data Privacy Accountability Score

IMPLEMENTATION NOTE

The Scorecard allows the privacy office to answer the question 'do you know if your privacy program is effectively implemented throughout the organization?' with confidence, on demand. Because the Score is calculated empirically and Responses must be supported by Evidence, the results stay up to date and accurate, providing a level of comfort that cannot be found in an annual assessment.

4. Scorecard Management

One of the key benefits of the Scorecard is the ability to monitor the privacy program over time.

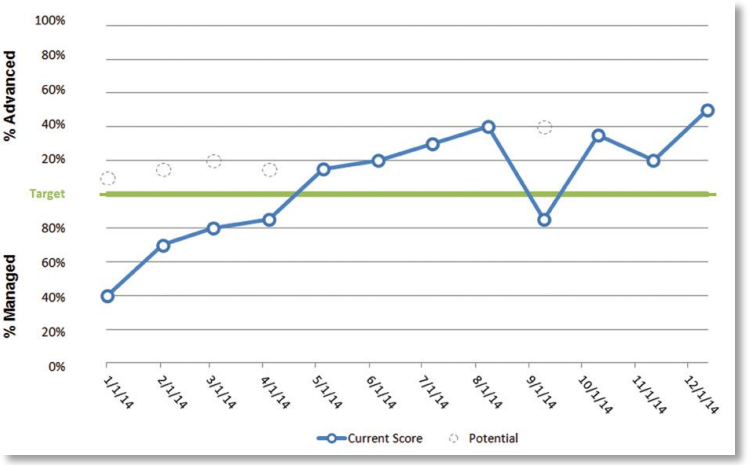


Figure 4.4 Data Privacy Accountability Scorecard Example

In the example above, the Data Privacy Accountability Score steadily increases and then suddenly drops below the target. This change is because the Owner did not provide Evidence within the assigned Frequency. As soon as the individual provides Evidence, the Score immediately returns to the previous % Advanced.

IMPLEMENTATION NOTE

The Scorecard allows the privacy office and stakeholders throughout the organization to see immediate impact of their own activities and the activities of their counterparts on the status of the privacy program overall. This can be a very strong motivator to proactively monitor the status and provide Evidence before the Frequency expires. One organization even found that users engaged in a bit of friendly competition to see who could get the higher score.

Scorecard Deployment Strategies

Most organizations deploy the Scorecard to measure, monitor, and report on the activities of the privacy office, as a 'proof of concept' before rolling it out into the entire organization. In order to move forward with a wider deployment, the organization must determine how to organize the activities and reports.

Answering the following questions will help guide the privacy office regarding the most appropriate deployment option(s) for its organization:

- **What are the reporting needs of the organization?** If the privacy office would like to monitor, measure, and report the privacy program status to management, it may make the most sense to align the report with the structure of the organization chart. If the goal is to demonstrate accountability to regulators on demand, deploying the Scorecard by jurisdiction or country is likely a good option.

- **How is the privacy program structured?** Sometimes the most logical way to deploy the Scorecard is to align with the existing privacy program (e.g. responsible individuals assigned in each business unit). That way, ownership is already determined for the most part.

Based on Nymity's experience with a number of successful Scorecard deployments, the best approach is usually a hybrid of two or more of the following deployment approaches:

- **Operational Unit** (e.g. Division, Department, Legal Entity, Business Unit): deploying a Scorecard for each operational unit is recommended if the organization wishes to report on the governance structure of the organization. This enables the privacy office to efficiently gather evidence and compare accountability across operational units.

- **Jurisdiction/Region**: If the Privacy Management Activities required to maintain data privacy compliance differ greatly from one jurisdiction to the next, it might be practical to structure the Scorecard by jurisdiction/region and analyze each one independently.

- **Data Type/Purpose** (e.g. customer, employee, or patient): Many organizations have distinctly different Privacy Management Activities related to the processing of personal data for various purposes. For example, employee data processed for the purposes of managing human resources may be subject to different legislative compliance requirements and managed by different Owners inside the organization compared to processing customer data for marketing purposes or order fulfilment. Processing personal information in a healthcare environment is another example of an activity

performed by a responsible organization that is likely to be very different even within the same organization.

In summary, the Scorecard is scalable for any data privacy program within a responsible organization. It can be customized and configured to: (1) meet the needs of the smallest organization, or (2) meet the needs of a matrix structure within a large multinational organization.

For complex deployments, and for organizations that wish to demonstrate both compliance and accountability, the Nymity Attestor™ solution, described in Appendix E, includes more sophisticated functionality.

Chapter 5. Attesting Compliance

As outlined in Chapter 1, one of the primary motivators for investing in the privacy program and being able to demonstrate accountability is compliance with laws and regulations. Organizations are looking for solutions to demonstrate compliance to rules of law, regulations, codes, standards, and internal rule sources such as data privacy policies or Binding Corporate Rules ("**Rule Sources**").

Achieving Compliance

Privacy compliance is a complex challenge. Most organizations processing personal data are subject to dozens of Rule Sources: privacy laws and regulations, related rules such as employment or sector specific laws, internal policies and procedures, and contractual obligations. The number grows substantially for large international organizations.

Maintaining compliance with the myriad Rule Sources requires that all processing of personal data is done in accordance with the requirements, or **Rules**. In an organization with limited resources, this may seem impossible. However, if the privacy office leverages existing investments in the program and demonstrating accountability, compliance can be achieved even with limited resources.

Leveraging Accountability to Attest Compliance

Evidence collected via the Scorecard for the purpose of demonstrating accountability can be re-purposed in order to provide evidence of compliance, in other words, to attest compliance. To attest compliance, the privacy office must 1) show evidence that the requirements are met; and 2) show that compliance is embedded throughout the organization via an effective privacy program.

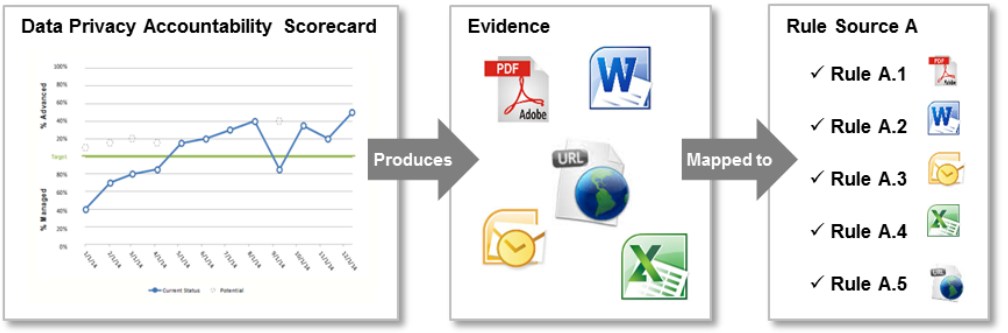


Figure 5.1 - Leveraging Accountability to Attest Compliance

To attest compliance, the privacy office needs to identify the Rules to which they are subject, and then map Evidence to the rules.

1. Identify Rules Requiring Evidence

Rule Sources often contain many provisions or sections that do not require action on the part of the organization and therefore do not require evidence. Examples of these include definitions, exemptions, regulator powers, and the preamble.

For example, the *UK Data Protection Act 1998* has 219 Rules to which 31 require action on the part of the organization and therefore require evidence.[21]

2. Map Evidence to Rules

A privacy office that can demonstrate accountability can attest compliance. Mapping the Evidence collected via the Data Privacy Accountability Scorecard to the appropriate compliance Rules demonstrates that the requirements are me The next step for attesting compliance is t that compliance is embedded throughout t organization via an effective privacy prog achieved through the use of the Scorecard

[21] Nymity Research has applied the Privacy Compliance Attestation Methodology™ to thousands of Rules from hundreds of Rule Sources.

Attesting Compliance Example

A company is processing personal data in Costa Rica and therefore must comply with the Rule Source *Protection of Individuals against the Processing of Personal Data, No. 8968.* The company has implemented the Data Privacy Accountability Scorecard, and therefore has a number of pieces of Evidence to demonstrate accountability.

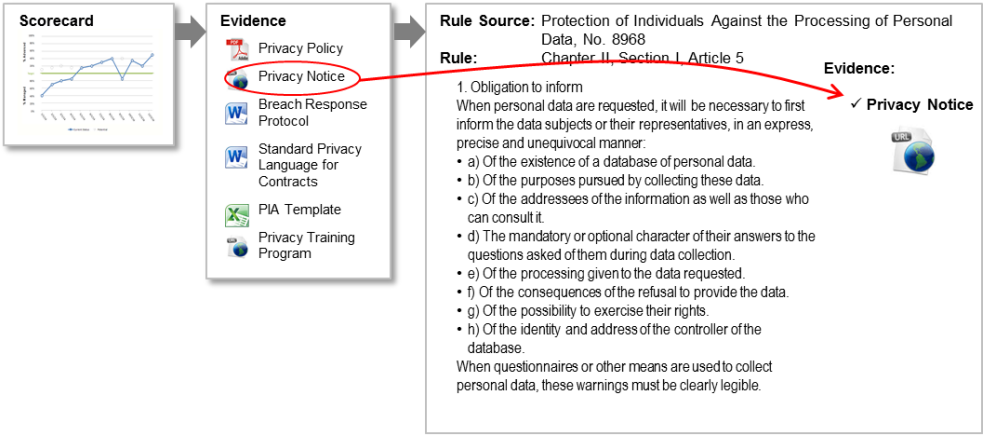


Figure 5.2 - Attesting Compliance Example

Chapter II, Section I, Article 5 of the Costa Rica law contains requirements regarding provision of notice to individuals. The privacy office reads the Rule and determines that they comply, and attaches the Privacy Notice as Evidence. This single piece of Evidence is now used to demonstrate accountability as well as to attest compliance.

Chapter 6. Case Study

Nymity has had the pleasure of partnering with a number of global organizations to successfully implement the Data Privacy Accountability Scorecard. These organizations range in size and type, but all have one thing in common: they wish to answer the question, 'how do we know that the privacy program is effectively embedded throughout the organization?' The most common factor driving these organizations to invest time and resources to answer this question (the driver for over half of Nymity's current Attestor implementations), is **Binding Corporate Rules** (BCR).[22] Whether monitoring existing BCR or conducting a readiness assessment, the Scorecard is proven effective at demonstrating accountability for the purposes of BCR.

This section describes how one organization, an international oil and gas company ("the Company"), utilized the Data Privacy Accountability Scorecard to successfully implement a BCR monitoring program, thereby demonstrating accountability.

Background

With over 75,000 employees, the Company processes a large volume of personal data – mostly that of employees and contractors, but some customer data as well. Maintaining compliance with data protection laws was a complex challenge, in particular with regard to restrictions in EU law around transferring personal data outside the European Economic Area (EEA). The Company has adopted BCR as a

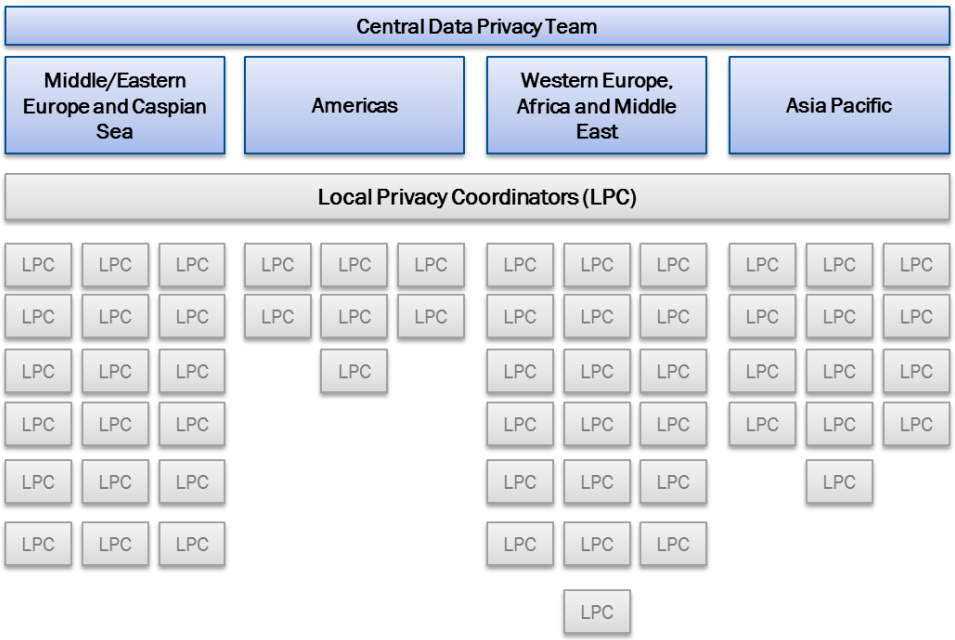
[22]BCRs are internal rules (such as a Code of Conduct) within a multinational organization, adopted by multinational groups of companies, which defines its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection. BCR is a voluntary framework for responsible organizations to demonstrate accountability to DPAs and obtain approval. Once approved, the organization is able to obtain benefits such as abandoning the requirement for standard contractual clauses each time the organization transfers data to a member of its group.

means to legally comply with the EU laws on intragroup transfers and to create a robust international compliance framework for the processing of personal data.

Privacy Program

The privacy function at the Company consists of a Central Data Privacy Team ("privacy office") of a Global Privacy Officer and 4 Regional Privacy Advisors. The privacy office reports into the Legal function. Its mission is "to promote best practices for managing personal information in compliance with the Code of Conduct, [BCR], and any local legal obligations."

Supporting the privacy office is a network of Local Privacy Coordinators (LPCs), one for each of the 80 countries - who are tasked with implementing and monitoring the BCR in their jurisdictions and providing advice to local stakeholders. The LPC role is assumed in addition to normal job responsibilities, with most within the Human Resources function.



The Objective: Monitoring Compliance with Binding Corporate Rules

The Company had implemented a robust privacy compliance framework and adopted BCR across 80 countries. Organizations utilizing BCR as a cross border transfer mechanism are required to commit to an "audit programme [which] covers all aspects of the BCRs…such audit must be carried out on a regular basis… [and] the Data Protection Authorities can receive a copy of such audits upon request."[23] The Company had a questionnaire- based mechanism in place to do so, however, it had limitations.

When the first draft of the proposed EU General Data Protection Regulation (GDPR)[24] was released including an accountability principle, the Company realized they needed to take steps to better prepare for the possibility of 'a regulator knocking at the door'.

The Company sought a solution for ongoing monitoring of the status of the privacy program: to answer the question, 'how do we know the privacy program is effectively embedded throughout the organization?' and to be able to demonstrate that on demand.

Critical Success Factors

The privacy office identified three critical success factors for the solution – it had to be:

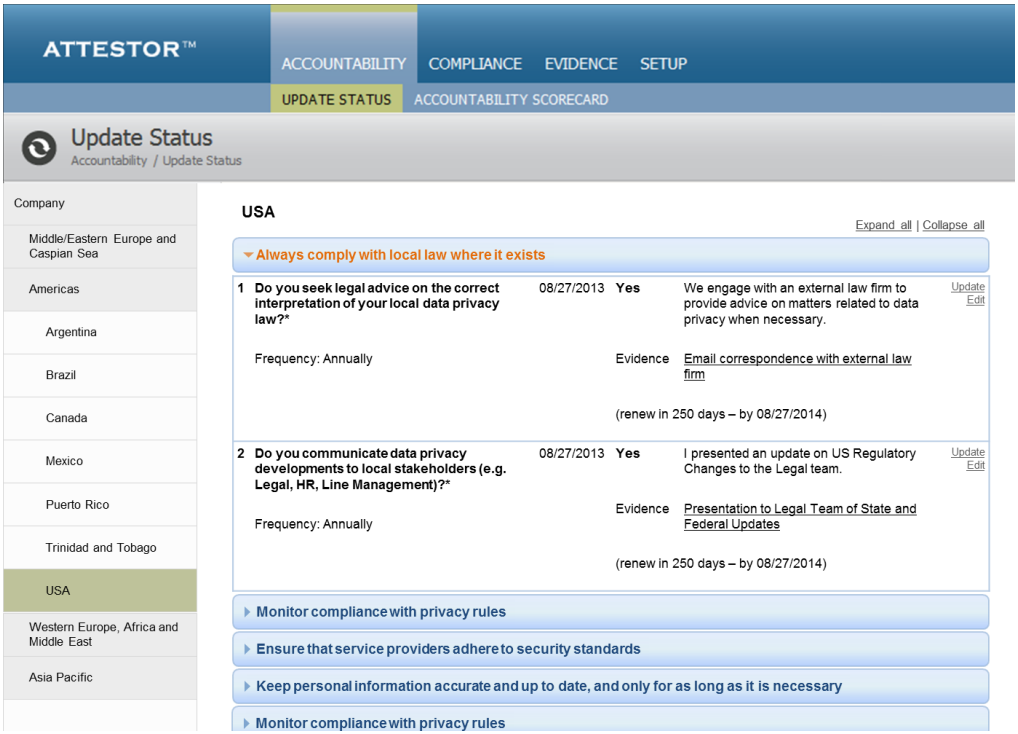
- **Pragmatic:** The Company needed the ability to demonstrate compliance to the BCR in a sustainable, ongoing way. The solution needed to be simple and straightforward for the LPCs - without placing undue burden or requiring them to become privacy experts. It also had to work with existing program resources;

[23] Article 29 Data Protection Working Party. (2008).*Working Document WP 154 Setting up a Framework for the Structure of Binding Corporate Rules*. Belgium.
[24] European Commission. (2012). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Brussels.

- **Scalable:** The Company wanted a global view of the program, with the ability to drill down to the region and country level, so they could understand how country-specific risks would impact the overall enterprise; and
- **Evidence based** to enable compliance with privacy laws and regulations locally and globally.

The Solution: the Data Privacy Accountability Scorecard using Attestor

Using the approach outlined in Chapter 4, the Company implemented the Scorecard approach to demonstrating accountability.



1. Setup Scorecard

First, the privacy office developed approximately 30 Evidence Collection Questions which would be standard across all countries and address all the requirements of the BCR. The Company opted to consider only Core activities for the first phase, to keep it simple and avoid confusing the LPCs for whom data privacy was not their primary job function.

First, each of the Regional Privacy Advisors completed the Scorecard. In doing so, they were able to understand the perspective of the LPCs and opted to revise the Evidence Collection Questions to make them even more straightforward. As discussed in Chapter 4, simple, clearly worded questions are the best.

2. Collect Evidence

The Company launched the Scorecard using a phased approach, beginning with countries with more mature local privacy programs, usually because the local laws were more rigorous. Prior to asking the LPCs to invest the time in completing the Scorecard, the privacy office took great care to properly socialize the project. Getting buy-in and support from senior management and the legal team was critical. To do so, the privacy office explained the background and reason for demonstrating accountability and pointed out ways the project would add value for each of the stakeholders.

It was important to the privacy office that the Scorecard did not place undue burden on the LPCs. These individuals were busy with their day to day job responsibilities; and the privacy office required their cooperation to make the project a success. To help minimize the impact on the LPCs, the Regional Privacy Advisors pre-loaded some commonly referenced documentation into the Evidence Library. The LPC was able to browse for Evidence, rather than search for it.

3. Calculate Data Privacy Accountability Score

The Regional Privacy Advisors had completed the Scorecard as part of the initial phase, and opted to share their results to the broader privacy team as part of the project. Not all respondents were comfortable sharing their results, so the privacy office configured permissions in Attestor to ensure that they were limited to those with a business need to know.

While socializing the Scorecard project, the Company found that it was important to present the Scorecard as a tool to help them manage the privacy program and improve it over time – not as a report card. Some countries were more sensitive than others to being given a ‘score’ for their local privacy program. However, the privacy office made it clear that demonstrating accountability is about communicating and working together to reach the target.

4. Scorecard Management

The Regional Privacy Advisors met with each of the LPCs during and after the completion of Evidence Collection Questions. They identified areas for improvement

and established plans to provide evidence where none was previously available. Going forward, on a quarterly basis the Scorecard is used as the basis for the conversation between the LPCs and Regional Advisors (in itself a Privacy Management Activity!).

The Result: Success!

The Company's Global Privacy Officer described the Scorecard implementation as follows, "in the event that a national privacy regulator requests or demands evidence that [we are] compliant with BCRs, local laws or regulations, we will be able to respond quickly and objectively [and] our responses will be backed by evidence. We can document our compliance status and any actions we are taking to make improvements."

The Scorecard met the Company's objectives for demonstrating accountability, and also resulted in benefits which were not anticipated but certainly welcome:

- Distributes the work of monitoring compliance across the organization, rather than being entirely the responsibility of the privacy office;
- Easy to demonstrate the impact that one country has on the program overall[25], and compare one country to another and to the organization overall;
- Encourages participation throughout the year, not just a 'mad dash' to respond to a compliance audit; and
- Serves as a resource for LPCs - they can learn from their counterparts in other countries and they better understand what is expected of them. When there is turnover in the role, the new LPC can see all of the relevant history of how things were done before.

Monitoring BCR is one of several ways to use the Scorecard. Organizations have used the Scorecard to help streamline and reduce the cost of privacy audits, conduct BCR readiness assessments, and perform internal gap analyses.

Contact Nymity to learn more about how the Scorecard can support privacy initiatives.

[25] This benefit is made possible by the organizational structure configuration functionality in Attestor and may not be as easily achieved using the Microsoft Excel® Spreadsheet version.

Chapter 7. Getting to Accountability

In order to demonstrate accountability, organizations must have an established privacy program in place and be processing personal data responsibly. For a variety of reasons, an organization may not have an established program. Many of the drivers outlined in Chapter 1: Drivers for Investing in a Privacy Program are reasons for an organization to create or change a privacy program.

This chapter outlines the Nymity Privacy Planning and Benchmarking Methodology (PPBM), a methodology for planning, implementing, maturing, maintaining, and comparing a privacy program.

Many privacy offices faced with the challenge of building or transforming a privacy program ask the following questions:

Where do we start?

Whether starting with a 'blank slate' or a program in need of an overhaul, getting started can be a daunting task for even the most seasoned privacy professional.

What should we put in place?

It can be difficult to determine the priorities of the program, as there are often competing interests from various other parts of the organization. Many also wonder, 'what are others in my industry doing?'

How do we implement the Privacy Management Activities?

If the privacy office knows where to start and what to put in place, the task of actually implementing the Privacy Management Activities is still required. They can learn how to implement the Activities themselves, or hire an expert; either way, resources are required.

This chapter will address the above questions, with a focus on the early stages of the privacy program life cycle: implementing, maturing, and managing the privacy program. The PPBM can also be used throughout the life cycle as a resource to get started with implementing accountability, and for ongoing maintenance in mature privacy programs.

Baselining the Privacy Program

Whether building a privacy program or working with an established program, it is pertinent to first identify the Privacy Management Activities ("Activities") that are already in place. From the perspective of the privacy office, these activities are either:

- **Implemented by privacy office:** The privacy office has direct responsibility for maintaining several Activities, for example maintaining a data privacy policy or maintaining PIA guidelines and templates;
- **Influenced by the privacy office:** The privacy office supports other parts of the organization in embedding privacy into operational practices. Examples of these Activities would include the privacy office working with customer service to maintain procedures to address complaints, or working with marketing to ensure a **privacy notice** is embedded in marketing materials sent to customers; or
- **Independent of the privacy office:** The privacy office observes some Activities with limited influence. For example, Procurement may have a sophisticated process for onboarding vendors, Legal may have embedded advanced privacy controls into the process for managing contracts, or Human Resources may have procedures for protecting the confidentiality of employee personal data.

Baselining Made Easy

The privacy office does not have to start with a blank page when identifying Activities; Nymity has already identified over 150 Activities that are common to privacy programs across jurisdictions and industries. See Appendix A: Nymity Privacy Management Accountability Framework.

Assign Status

Each Activity falls into one of four status categories:

- **Implemented**: Privacy Management Activity is in place.

- **Planned**: In progress or scheduled to be implemented in the next 12 months.
- **Desired**: Privacy Management Activity is desired but not currently planned to be implemented in the next 12 months.
- **Not Applicable** (N/A): Privacy Management Activity is not applicable to the organization (or the part of the organization being assessed).

Each status category has sub-categories that explain the necessary information to communicate the status to others.

Implemented Activities

Activities that are categorized as 'Implemented' fit into two sub-categories:

- **Up-to-Date**: The Activities are up-to-date and completed on an ongoing basis. The privacy office will likely discover that many Activities are Up-to-Date but do not require any interaction or support from the privacy office. For example, IT may conduct a security risk assessment which considers data privacy risk, or Procurement may conduct due diligence around the data privacy and security posture of potential vendors/processors. Some Up-to-Date Activities will be completed by the privacy office, such as an annual process to review the privacy policy.
- **Update Planned:** Some Activities will likely be identified as Implemented, but will require the attention of the privacy office to update or enhance the Activity. For example, the privacy office may have a training program in place but recognize the need to update the content; or the marketing department may have a privacy notice in place that requires a review to ensure it is consistent with data handling practices.

Planned Activities

As part of the baselining activity, most organizations will identify the need to implement new Activities. Even organizations with very mature privacy programs will make investments each year to continuously mature and evolve the program. Additionally, new Activities are often required as the privacy landscape changes over time. For example, five years ago it's likely that very few organizations had documented policies for cloud computing or bring-your-own-device (BYOD), however, they are becoming increasingly common as the technologies become ubiquitous. Planned Activities fit into two categories:

- **In Progress**: Some Activities take several months or even years to complete. For example, providing data privacy notice at all points where personal data is collected could take months and is likely executed in stages. Particularly this includes Activities which require coordination across multiple stakeholder groups, such as conducting PIAs for new programs, systems, and processes.

- **Scheduled**: Some Activities are planned but not yet initiated. For example, an Activity may be scheduled to take place in conjunction with an external event such as integrating data privacy into use of cookies and tracking mechanisms, scheduled to coincide with a change in law or regulation.

Desired Activities

For some organizations, although Activities may be desired, the program is not yet ready to schedule them. Often the reason a desired Activities is not ready to be scheduled is due to dependencies on other Activities or initiatives. Desired Activities fall into three categories:

- **Privacy Program Dependencies:** In some cases, the privacy office is not yet ready to schedule implementation of Activities because it is dependent on another Activity that is not yet implemented. For example, conducting periodic testing of the breach protocol would be dependent on the data privacy incident/breach response protocol being completely implemented.

- **Operational Dependencies:** In many, if not most cases, the privacy office is dependent on operational units for cooperation and resources. For example, maintaining a data-loss prevention strategy is likely the responsibility of IT Security. For a multitude of reasons, IT Security may not have done so; but the privacy office does not have direct control. Therefore, there is an operational dependency and the Activity is categorized as desired.

- **Awaiting Approval:** Some Activities are desired but have not yet been approved by management. Budget and resource constraints are often a factor in Activities awaiting approval. For example, it may be desired to hold an annual data privacy day/week, but it has not yet been approved.

Not Applicable Activities

The Nymity Privacy Management Accountability Framework is designed to reflect a comprehensive list of Activities undertaken by organizations across industries,

sectors, and jurisdictions with over 150 Activities listed across 13 Privacy Management Processes. It is highly unlikely that all of the Activities apply to any one organization, so most programs designate a number of Activities as Not Applicable (N/A) for one of three reasons:

- **Operationally Not-Relevant:** This could be because the organization simply is not involved in the underlying practices of processing personal data. For example, if the organization does not conduct telemarketing, then integrating data privacy into telemarketing practices is not applicable. Another example for an organization that is a third-party data processor – if the organization does not collect personal data directly from the individual, providing data privacy notice at all points where personal data is collected would not be applicable.

- **Jurisdictionally Not-Relevant:** While the Nymity Privacy Management Accountability Framework is designed to be jurisdictionally neutral, some Activities are aligned to common legislative requirements. For example, registering databases with data protection authorities is only relevant in jurisdictions that require this Activity. Also, in many jurisdictions, Activities related to cross-border transfers would be irrelevant. Many of the jurisdictional specific Activities are found in Privacy Management Process 2 – Maintain Personal Data Inventory.

- **Insufficient Business Case:** In some cases, a business case will not justify the investment of resources to conduct an Activity. For example, an organization that processes a low volume of customer data would not likely have the business case for some of the more advanced Activities such as maintaining procedures to investigate root causes of data protection complaints.

Categorizing the status of each Activity sets the foundation for planning and benchmarking, and enables a consistent structure for ongoing measurement and reporting. However, another layer is required to understand the context of the Activities in relation to the privacy program: attributes.

Assign Attributes

Assigning attributes sets the foundation for demonstrating accountability. For a comprehensive discussion on each of the attributes below, please refer to Chapter 1: Accountability in Practice.

Core or Elective

Core activities are defined by the privacy office as fundamental to privacy management. These fundamental activities will vary from one organization to the next and will be influenced by the industry/sector as well as jurisdiction. In some organizations, Core activities are considered the bare-minimum for processing personal data responsibly. Often the designation of Core is related to compliance requirements such as Safe Harbor, Binding Corporate Rules, or internal policies.

Elective activities are desired activities defined and supported by the privacy office. They are often considered 'above and beyond' the Core, or minimum, requirements for the processing of personal data. Sometimes Elective activities are advanced, such as measuring comprehension of privacy training and adjusting the curriculum to reflect learning needs. Other times, Elective activities are 'nice to have' but not critical to privacy management, such as maintaining posters and videos related to privacy awareness.

Owner

Roles should be clearly defined so that all key players understand where they fit within the overall organizational structure, as well as how their actions and decisions impact the privacy program as a whole. For many Activities, particularly in Privacy Management Processes 1 - Maintain Governance Structure, 3 - Maintain Data Privacy Policy, and 13 – Track External Criteria, the privacy office is the owner.

Ownership of some Activities will reside within the operational units, as that is where the data is being collected and processed. Activities in Privacy Management Process 4 – Embed Data Privacy into Operations are likely to reside in operational units. IT Security is likely the owner for many of the Activities in Privacy Management Process 6 – Manage Information Security Risk.

Frequency

Privacy Management Activities must be performed on an ongoing basis – either periodic or continuous. For each Activity, the privacy office determines the appropriate frequency. Typically, the minimum frequency is annually, and the maximum is monthly.

Illustrative Example

Table 7.1 illustrates how an organization may baseline its privacy program across three different Operational Units (OUs).

OU	Privacy Management Activity	Status				Attributes		
		N/A	Desired	Planned	Implemented	Core/ Elective	Frequency	Owner
A	Measure participation in data privacy training activities				Up-to-Date	Core	Quarterly	OU A
B	Measure participation in data privacy training activities				Update Planned	Elective	Quarterly	OU B
C	Measure participation in data privacy training activities			Scheduled		Core	Annually	HR

Table 7.1 - Illustrative Example of Baselining the Privacy Program

Status and Attributes are captured for each Activity, for each Operational Unit. For simplicity, this example looks at the same Activity across all three Units. In practice, baselining requires completion of the entire Nymity Privacy Management Accountability Framework for each Unit.

- Operational Units A and B both measure participation in data privacy training. In Unit A, the Activity is Up-to-Date and a Core or mandatory element of the privacy program.
- In Unit B, the Activity is Implemented but there is an update planned. It is an Elective activity, likely due to the type of personal information processed by employees in that Unit being lower risk.
- In Unit C, the Activity is not currently performed, but is scheduled to be implemented in the next 12 months. When in place, the Activity will be performed annually on the Operational Unit's behalf by Human Resources – possibly due to a shared services model or resource constraints within Unit C.

The Nymity Privacy Planning and Benchmark Methodology enables organizations to build upon the baseline in order to implement and benchmark the program.

Implementing Privacy Management Activities

The benchmarking exercise will identify areas of focus for the privacy office – either to move the Activity status along (e.g. from Desired to Planned) or to move from one

sub-category to another (e.g. Implemented Activity moving from Update Planned to Up-to-Date). The PPBM provides the following structure for the information required to implement or enhance any Activity:

- **Scope**: Defining the scope helps to identify the specific elements of an Activity, and those that fall outside the scope, possibly in another related Activity. There are two factors to consider in the scope of an Activity:
    - Role of the Activity within the context of the entire organization; and
    - Role of the privacy office in ensuring that the Activity reflects organizational policies and values.

  For example, the organization will maintain an information security policy for the purpose of safeguarding personal data. The role of the privacy office in this Activity is to embed data privacy considerations into the policy. This distinction is important in helping the privacy office to manage implementation of the Activities, ensuring their own responsibilities are appropriately assigned and other stakeholders are involved as necessary.

- **Business Case**: Privacy Management Activities require resources to implement and maintain, and sometimes require justification. For every Activity in the Desired status, a business case (formal or informal) will likely be required to justify the investment and move it to Planned status.

- **Pre-requisites**: Often an Activity is in Desired status because other Activities need to be completed first. For example, almost all Activities are dependent on the pre-requisite of maintaining a data privacy policy.

- **Resources**: Resources for implementing Activities may be produced by the privacy office, with the assistance of an external firm or counsel, or be conducted internally. The privacy office may wish to leverage guidance, checklists, and templates to help implement the Activities.

Illustrative Example

Continuing from the previous example, Table 7.2 illustrates how an organization may implement the Privacy Management Activity:

Privacy Management Process 5 – Maintain Training and Awareness Program	
Activity: Measure participation in data privacy training activities	
Scope	Measuring the participation of data privacy training demonstrates an organization's commitment to data privacy. The measure of participation could be achieved through participants taking a test containing data privacy questions or recording the names of participants attending data privacy training. Each of these methods proves that data privacy training has taken place. Organizations consider recording attendance for core training and refresher training.
Business Case	Training is one of the most effective ways to change and align staff behavior with the organization's policies. The privacy office must clearly indicate the impact of privacy training on achieving the organization's objectives, identifying: what needs to be trained based on the current environment, what training procedures, methods, etc. are most likely to affect this training, and the evidence that the training has occurred and that staff have internalized the training objectives. Measuring the participation in training activities fulfills part of the last piece of the puzzle – it provides evidence that training has occurred. Such measurements also help identify any training gaps, i.e. which staff/departments/vendors still require training.
Pre-requisites	▪ Conduct data privacy training needs analysis by position/job responsibilities ▪ Maintain a core training program for all employees ▪ Conduct training for newly appointed employees upon assignment to privacy-sensitive positions ▪ Conduct regular refresher training to reflect new developments
Resources	▪ E-Learning system outputs showing percentage of employees completing data privacy training ▪ Form for manager attestation that direct reports have completed training ▪ Data privacy training sign-in sheet

Table 7.2 - Required Information for Implementing a Privacy Management Activity

Benchmarking the Privacy Program

Capturing the status and attributes of Activities using the structured methodology enables the comparison of privacy programs (or components of a program). Two or more programs can be compared over time on the basis of whether Activities are Core, Elective, Planned, Desired, or Not Applicable. This information can be useful when the privacy office is communicating the status of its program, identifying strengths and weaknesses, or establishing priorities.

Illustrative Example

Continuing from the previous example, Table 7.3 illustrates how an organization uses the information gathered during baselining to benchmark its privacy program.

OU	Privacy Management Activity	N/A	Desired	Planned	Implemented	
					Core	Elective
A	Measure participation in data privacy training activities				X	
B	Measure participation in data privacy training activities					X
C	Measure participation in data privacy training activities			X		

1. Main status category is carried over directly from baselining exercise

2. Implemented Activities categorized Core/Elective

Table 7.3 - Illustrative Example of Benchmarking

As with the baselining example above, for simplicity this example looks at the same Activity across three Operational Units. In practice, benchmarking typically involves evaluating multiple Activities in each Operational Unit.

Benchmarking combines the status with the attributes defined in baselining. The main status categories (i.e. not the sub-categories) are carried over directly from the baselining (see point 1 in the table above). For each of the Activities categorized as Implemented, the attribute of Core or Elective is recorded (status sub-categories and other attributes are not required for benchmarking, refer to point 2 in the table above)[26].

The privacy office can now compare the privacy programs of two or more Operational Units to one another, or over time. The table below provides examples of questions which can now be answered using insights gained from the benchmarking results.

[26] Operational Unit A and B both categorized the Activity as Implemented as part of the baselining exercise (refer to Table 7.1 above). When assigning attributes, the Activity was determined Core for Operational Unit A, and Elective for Operational Unit B. In Operational Unit C, the Activity status was Planned; as such the benchmarking does not take into account the attribute of Core/Elective.

Benchmarking Outcome	Example Question	Example Responses[27]
Comparison Compare two or more privacy programs	How do the privacy programs compare between Operational Units X, Y, and Z?	▪ Unit X is takes the minimal steps necessary based on a limited number of Core Activities. ▪ Unit Y has a more advanced privacy program based on the number of Elective Activities implemented ▪ Unit Z has identified a number of gaps but has a plan in place to implement more Activities over the next 12 months
Progress History of one privacy program over time	Last year, the privacy office sought to improve our third party risk management program – how have we progressed?	▪ All but one of the Activities identified as Desired at the outset of the project have moved forward. Of those, 30% are Implemented and 70% are Planned for the next 12 months.
Hybrid Compare two or more programs over time.	Based on data privacy breach metrics, it appears there has been an increase in breaches occurring in Unit D, but a decrease in breaches in Unit F– what could contribute to these trends?	▪ Unit F has increased their focus on training and awareness over the past 12 months; perhaps fewer mistakes are made because employees are more educated on how to protect personal data. ▪ Unit D uses several third party data processors and has procedures to ensure that contracts are in place with all vendors. However, Activities related to conducting due diligence for vendors are all noted as Desired. Perhaps more investment is warranted in getting those Activities planned.

Table 7.4 - Types of Benchmarking

[27] Note that in order to answer the questions effectively, benchmarking would need to be carried out across the Framework for each Operational Unit, i.e. insights based on a limited number of Activities are not accurate. However, as depicted in the second example (benchmarking over time) the organization may wish to examine one of the 13 Privacy Management Processes to obtain more focused results.

External Benchmarking

Many organizations wish to compare their privacy program with similar organizations, i.e. external benchmarking. This data can be important input into decisions on how and where to invest resources in privacy management. Any privacy program, internal or external, baselined using the Nymity Privacy Planning and Benchmark Methodology, can be compared.

Nymity Benchmarks™ is a tool built on the methodology which allows users to compare their privacy program to others, conduct ongoing planning, and track progress over time.

For more information please refer to Appendix D: About Nymity or contact Nymity.

Appendix A: Nymity Privacy Management Accountability Framework™

The Nymity Privacy Management Accountability Framework™ ("Framework") was originally developed for communicating the status of the privacy program, in other words a framework for demonstrating accountability. The Framework was designed to report on any privacy program, no matter how it is structured. For example, it works well with privacy programs structured around privacy principles, rationalized rules, standards and codes.

The Framework is a comprehensive, jurisdiction- and industry-neutral and works with privacy programs that are relatively new or very mature. Organizations around the world are using the framework to structure their privacy programs. The Nymity Privacy Management Accountability Framework is made up of 13 Privacy Management Processes each containing multiple Privacy Management Activities (over 150 in total).

One Framework: Multiple Purposes

Although originally designed as a framework for demonstrating accountability, organizations are now using it for other purposes including:

- **Structuring the privacy program:** Some organizations, often those with a new privacy program or enhancing their existing program, have found this Framework effective for structuring the privacy program. The may use all 13 Privacy Management Processes or a subset. For example, a North American service provider/data processor many not implement many of the activities within Privacy Management Processes 2) Maintain Personal Data inventory, or 8) Maintain Notices as they are not relevant given the nature of their data processing activities.

- **Baselining and planning:** Some organizations use the Framework as a checklist to identify existing Privacy Management Activities and for planning the implementation of new ones.
- **Benchmarking:** This Framework provides an effective mechanism to compare the privacy program across different areas of the organization, or between two organizations.
- **Regulatory Reporting:** Reporting to a regulator is a form of demonstrating accountability. Some organizations are using this Framework to show due-diligence, for example in the event of a data breach to demonstrate that the event was an exception that occurred despite a robust program in place to prevent it, as opposed to a systemic issue.

Nymity is a research company and as such is continuously updating the Privacy Management Activities. The Framework will continue to evolve as the privacy landscape changes and more organizations adopt it as an approach to communicating the status of their privacy programs.

Should you wish to submit or request new Privacy Management Activities, please share them with Nymity at info@nymity.com.

This section lists the Privacy Management Activities as of April 2015. An up to date version and other resources are available for free on Nymity's website (www.nymity.com).

1. Maintain Governance Structure

Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures

Privacy Management Activities

- Conduct an Enterprise Privacy Risk Assessment
- Maintain a Privacy Strategy
- Maintain a privacy program charter/mission statement
- Maintain job descriptions for individuals responsible for data privacy (e.g. data protection officers)
- Assign accountability for data privacy at a senior level
- Allocate resources to adequately implement and support the privacy program (e.g. budget, personnel)
- Assign responsibility for data privacy throughout the organization
- Appoint a representative in member states where the organization does not maintain a physical presence
- Conduct regular communication between individuals accountable and responsible for data privacy
- Consult with stakeholders throughout the organization on data privacy matters
- Report, on a scheduled basis, on the status of the privacy program (e.g. board of directors, management board)
- Integrate data privacy into business risk assessments/reporting
- Integrate data privacy into a Code of Conduct
- Integrate data privacy into ethics guidelines
- Maintain a strategy to align activities with legal requirements (e.g., address conflicts, differences in standards, creating rationalized rule sets)
- Require employees to acknowledge and agree to adhere to the data privacy policies
- Report periodically on the status of the privacy program to external stakeholders, as appropriate (e.g. annual reports, third parties, clients)

Notes:

Activities relating to maintaining a data privacy policy are discussed on PMP 3 – Maintain a Data Privacy Policy

2. Maintain Personal Data Inventory

Maintain an inventory of the location of key personal data storage or personal data flows with defined classes of personal data

Privacy Management Activities

- Maintain an inventory of key personal data holdings (what personal data is held and where)
- Classify personal data holdings by type (e.g. sensitive, confidential, public)
- Obtain approval for data processing (where prior approval is required)
- Register databases with data protection authority (where registration is required)
- Maintain documentation for all cross-border data flows (e.g. country, mechanism used as a basis for the transfer such as Safe Harbor, model clauses, binding corporate rules, or approvals from data protection authorities)
- Maintain flow charts for key data flows (e.g. between systems, between processes, between countries)
- Use Binding Corporate Rules as a data transfer mechanism
- Use Standard Contractual Clauses as a data transfer mechanism
- Use APEC Cross-Border Privacy Rules as a data transfer mechanism
- Use the Safe Harbor framework as a data transfer mechanism
- Use Data Protection Authority approval as a data transfer mechanism
- Use adequacy or one of the derogations from adequacy (e.g. consent, performance of a contract, public interest) as a data transfer mechanism

Notes:

All activities related to notification of processing and registration of databases should be included in this management process

All activities related to cross border transfer should be included in this management process.

Activities relating to maintaining a listing of third-parties and affiliates are discussed in PMP 7 – Manage Third Party Risk

PMP 10 – Monitor for New Operational Practices includes the requirement to update the personal data inventory

3. Maintain Data Privacy Policy

Maintain a data privacy policy that meets legal requirements and addresses operational risk

Privacy Management Activities

- Maintain a data privacy policy
- Maintain a separate employee data privacy policy
- Obtain board approval for data privacy policy
- Document legal basis for processing personal data
- Document guiding principles for consent

Notes:

The privacy policy is not synonymous with the privacy notice – the policy communicates the organization's guiding principles internally, while the notice communicates the organization's data handling practices externally (see PMP 8 – Maintain Notices)

Operational policies and guidelines are discussed in PMP 4 – Embed Data Privacy into Operations

Training and Awareness policies are included in PMP 5 – Maintain Training and Awareness Program

Security policies are included in PMP 6 – Maintain Security Controls

Policies relating to outsourcing (by third-parties or affiliates) are included in PMP 7 – Manage Third Party Risk

Policies for processing access requests are discussed in PMP 9 – Manage Procedures for Inquiries and Complaints

Data Breach response policies are included in PMP 11 – Maintain Data Privacy Breach Management Program

4. Embed Data Privacy into Operations

Maintain operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives

Privacy Management Activities

- Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)
- Maintain policies/procedures for maintaining data quality
- Maintain policies/procedures for pseudonymization/anonymization of personal data
- Maintain policies/procedures to review processing conducted wholly or partially by automated means
- Maintain policies/procedures for secondary uses of personal data
- Maintain policies/procedures for collecting consent preferences
- Maintain policies/procedures for secure destruction of personal data
- Integrate data privacy into use of cookies and tracking mechanisms
- Integrate data privacy into records retention practices
- Integrate data privacy into direct marketing practices
- Integrate data privacy into e-mail marketing practices
- Integrate data privacy into telemarketing practices
- Integrate data privacy into behavioural advertising practices
- Integrate data privacy into hiring practices
- Integrate data privacy into employee background check practices
- Integrate data privacy into social media practices
- Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures
- Integrate data privacy into health & safety practices
- Integrate data privacy into interactions with works councils
- Integrate data privacy into practices for monitoring employees
- Integrate data privacy into e-mail monitoring practices
- Integrate data privacy into use of CCTV/video surveillance
- Integrate data privacy into use of geo-location (tracking and or location) devices
- Integrate data privacy into delegate access to employees' company e-mail accounts (e.g. vacation, LOA, termination)
- Integrate data privacy into e-discovery practices
- Integrate data privacy into conducting internal investigations
- Integrate data privacy into practices for disclosure to and for law enforcement purposes
- Integrate data privacy into customer/patient/citizen facing practices (e.g. retail sales, provision of healthcare, tax processing)
- Integrate data privacy into back office/administrative procedures (e.g. facilities management)
- Integrate data privacy into financial operations (e.g. credit, billing, processing transactions)
- Integrate data privacy into research practices

5. Maintain Training and Awareness Program

Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks

Privacy Management Activities

- Conduct data privacy training needs analysis by position/job responsibilities
- Maintain a core training program for all employees
- Conduct training for newly appointed employees upon assignment to privacy-sensitive positions
- Maintain a second level training program reflecting job specific content
- Conduct regular refresher training to reflect new developments
- Integrate data privacy into other training programs, such as HR, security, call centre, retail operations training
- Measure participation in data privacy training activities (e.g. numbers of participants, scoring)
- Require completion of data privacy training as part of performance reviews
- Deliver a privacy newsletter, or incorporate privacy into existing corporate communications
- Maintain ongoing awareness material (e.g. posters, intranet, and videos)
- Maintain an internal data privacy intranet, privacy blog, or repository of privacy FAQs and information
- Hold an annual data privacy day/week
- Measure comprehension of data privacy concepts using exams
- Provide data privacy information on system logon screens
- Maintain certification for individuals responsible for data privacy, including continuing professional education
- Conduct one-off, one-time tactical training and communication dealing with specific, highly-relevant issues/topics
- Provide ongoing education and training for the privacy office (e.g. conferences, webinars, guest speakers)

6. Manage Information Security Risk

Maintain an information security program based on legal requirements and ongoing risk assessments

Privacy Management Activities

- Conduct a security risk assessment which considers data privacy risk
- Maintain an information security policy
- Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)
- Maintain administrative and technical measures to encrypt personal data in transmission and at rest, including removable media
- Maintain an acceptable use of information resources policy
- Maintain procedures to restrict access to personal information (e.g. role-based access, segregation of duties)
- Maintain a corporate security policy (protection of physical premises and hard assets)
- Maintain human resource security measures (e.g. pre-screening, performance appraisals)
- Maintain backup and business continuity plans
- Maintain a data-loss prevention strategy
- Maintain procedures to update security profile based on system updates and bug fixes
- Conduct regular testing of data security posture
- Maintain a security verification

Notes:

Training related to security is included in PMP 5 – Maintain Training and Awareness Program

7. Manage Third Party Risk

Maintain contracts and agreements with third parties and affiliates consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain data privacy requirements for third parties (e.g. vendors, processors, affiliates)
- Maintain procedures to execute contracts or agreements with all processors
- Maintain a vendor data privacy risk assessment process
- Conduct due diligence around the data privacy and security posture of potential vendors/processors
- Maintain a policy governing use of cloud providers
- Maintain procedures to address instances of non-compliance with contracts and agreements
- Conduct ongoing due diligence around the data privacy and security posture of vendors/processors based on a risk assessment
- Review long-term contracts for new or evolving data protection risks

8. Maintain Notices

Maintain notices to individuals consistent with the data privacy policy, legal requirements, and operational risk tolerance

Privacy Management Activities

- Maintain a data privacy notice that details the organization's personal data handling policies
- Provide data privacy notice at all points where personal data is collected
- Provide notice by means of on-location signage, posters
- Provide notice in marketing communications (e.g. emails, flyers, offers)
- Provide notice in all forms, contracts, and terms
- Maintain scripts for use by employees to provide the data privacy notice
- Maintain a data privacy notice for employees (processing of employee personal data)
- Maintain a privacy Seal or Trustmark to increase customer trust
- Provide data privacy education to individuals (e.g. preventing identity theft)

9. Maintain Procedures for Inquiries and Complaints

Maintain effective procedures for interactions with individuals about their personal data

Privacy Management Activities

- Maintain procedures to address complaints
- Maintain procedures to respond to access requests
- Maintain procedures to respond to requests to update or revise personal data
- Maintain procedures to respond to requests to opt-out
- Maintain procedures to respond to requests for information
- Maintain customer Frequently Asked Questions
- Maintain escalation procedures for serious complaints or complex access requests
- Maintain procedures to investigate root causes of data protection complaints
- Maintain metrics for data protection complaints (e.g. number, root cause)

10. Monitor for New Operational Practices

Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles

Privacy Management Activities

- Maintain a Privacy by Design framework for all system and product development
- Maintain Privacy Impact Assessment guidelines and templates
- Conduct PIAs for new programs, systems, processes
- Maintain a procedure to address data protection issues identified during PIAs
- Maintain a product sign-off procedure that involves the privacy office
- Maintain a product life cycle process to address privacy impacts of changes to existing programs, systems, or processes
- Maintain metrics for PIAs (e.g. number completed, turnaround time)

Notes:

All activities related to audits and assessments of existing operational practices are included in PMP 12 – Monitor Data Handling Practices

11. Maintain Data Privacy Breach Management Program

Maintain an effective data privacy incident and breach management program

Privacy Management Activities

- Maintain a documented data privacy incident/breach response protocol
- Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) and protocol
- Maintain a breach incident log to track nature/type of all breaches
- Maintain data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)
- Conduct periodic testing of breach protocol and document findings and changes made
- Engage a breach response remediation provider
- Engage a forensic investigation team
- Obtain data privacy breach insurance coverage
- Maintain a record preservation protocol to protect relevant log history

12. Monitor Data Handling Practices

Verify operational practices comply with the data privacy policy and operational policies and procedures

Privacy Management Activities

- Conduct self-assessments managed by the privacy office
- Conduct ad-hoc audits/assessments based on complaints/inquiries/breaches
- Conduct audits/assessments of the privacy program outside of the privacy office (e.g. Internal Audit)
- Benchmark results of audits/assessments (e.g. comparison to previous audit, comparison to other business units)
- Conduct ad-hoc walk-throughs
- Conduct assessments through use of third party verification
- Maintain privacy program metrics

Notes:

Activities such as Privacy Impact Assessments used for new operations are included in PMP 10 – Monitor for New Operational Practices

13. Track External Criteria

Track new compliance requirements, expectations, and best practices

Privacy Management Activities

- Conduct ongoing research on developments in law
- Maintain subscription to compliance reporting service/law firm updates to stay informed on new developments
- Maintain records or evidence that alerts are read and actions are taken (e.g. read daily and forwarded to key individuals as required)
- Attend/participate in privacy conferences, industry association, or think-tank events
- Record/report on the tracking of new Rule Sources or amendments to Rule Sources
- Seek legal opinions regarding recent developments in law
- Document that new requirements have been implemented (also document where a decision is made to not implement any changes, including reason)
- Review or participate in studies related to best practices in data privacy management

Appendix B: Demonstrating Accountability to Data Protection Authorities

Demonstrating accountability[28] to Data Protection Authorities (DPAs) is an increasingly popular topic within the global privacy community and in some jurisdictions it either is or will become a requirement and/or a policy expectation as set by the DPA.

This section includes a global scan of recent activity such as comments from DPAs, and newly issued directives and guidelines, and changes to legislation which indicate the shift toward the requirement for organizations to be prepared to demonstrate accountability on demand.

The principle of accountability first appeared over 30 years ago in the 1980 OECD Guidelines,[29] the first internationally agreed-upon set of privacy principles which have influenced legislation and policy in OECD Member countries and beyond. The guidelines were revised in September 2013 with input from a group of experts chaired by Jennifer Stoddart, Privacy Commissioner of Canada. The group included participants from governments, privacy enforcement authorities, academics, business, civil society, and the Internet technical community; as well as representatives of the Council of Europe and the European Union, as well as experts active in APEC.

[28] For the purpose of this discussion, demonstrating accountability to a DPA is defined as proactively (i.e. self-initiated) reporting to the DPA on the status of the privacy program or on-demand reporting to a DPA. Examples of mechanisms for demonstrating accountability may include audits or assessments conducted by the organization or a third party. For the purpose of this discussion, mechanisms for demonstrating accountability do not include responses to investigations conducted by the regulator in response to a complaint or incident.

[29] OECD. (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The changes to the guidelines reflect the conversations happening globally around the importance of accountability and specifically demonstrating accountability to DPAs. Paragraph 15(b) provides that a data controller should be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority… giving binding effect to these Guidelines. Establishing the capacity and effectiveness of a privacy management programme, even in the absence of a personal data security breach or allegation of noncompliance, enhances the accountability of data controllers.

This OECD development is aligned with other developments in demonstrating accountability to DPAs around the world. The following discussion will speak to some of these developments.

The discussion will start in Canada as there are many examples of the Canadian Privacy Commissioners' expectations of organizations being able to demonstrate accountability on demand.

Canada

Data privacy in Canada is regulated at the federal and provincial level, depending on sector. The Federal Office of the Privacy Commissioner and the provincial Offices of the Information and Privacy Commissioners of Alberta and British Columbia are increasingly focused on collaboration and alignment, recently formalizing their approach to cooperation in a number of areas including enforcement, policy, public education and compliance resources, and information sharing.[30]

One example of this is a recent collaboration on the paper 'Getting Accountability Right with a Privacy Management Program, by the above mentioned Commissioners, in which the Commissioners' state:

> *…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…There will be times when mistakes are made. However, with a solid privacy management program, organizations will be able to identify their weaknesses, strengthen their good practices, demonstrate due diligence, and*

[30] Office of the Privacy Commissioner of Canada. (November 2011). *Provincial and Territorial Privacy Commissioners and Ombuds Offices. Canada.*

> *potentially raise the protection of personal information that they hold to a higher level than the bare minimum needed to meet legislative requirements.* [31]

The paper goes on to provide additional guidance on best approaches for developing a sound privacy management program.

Federal Private Sector

In Canada, accountability is not only expected, it is required by the federal private-sector law. Canada was among the first jurisdictions to establish Accountability as a data privacy principle as it is in the *Personal Information and Electronics Document Act* (PIPEDA) which came fully into effect on January 1, 2004. Although PIPEDA does not mandate demonstrating accountability, accountability is a legal obligation which the Commissioner's office oversees.

In May 2013, The Office of the Privacy Commissioner of Canada released a document entitled 'The Case for Reforming the Personal Information Protection and Electronic Document Act,[32] which recommended that "the law should be amended to require organizations to demonstrate, at the Commissioner's request, that they have a privacy program in place." Should the recommendations be implemented, demonstrating accountability would become law.

Provincial Public Sector

British Columbia

In the Province of British Columbia, Canada, the Privacy Commissioner, Elizabeth Denham, has spoken on the topic of demonstrating accountability to DPAs:

> *Organizations, public or private, that collect personal information from their customers and citizens…assume legal and ethical responsibility for privacy protection. And they should stand ready to demonstrate to citizens, customers, and to the privacy commissioners in the event of a complaint, investigation or audit.*[33]

---

[31] Office of the Information and Privacy Commissioner of Alberta. *Getting Accountability Right with a Privacy Management Program.* Alberta, Canada.
[32] Office of the Privacy Commissioner of Canada. (May 2013). *PIPEDA Review: The Case for Reforming the Personal Information Protection and Electronic Documents Act. Canada.*
[33] Commissioner Elizabeth Denham's Keynote Address to the 13th Annual Privacy and Security Conference Victoria, British Columbia February 17, 2012

Ontario

The public sector in the province of Ontario, Canada is regulated by the Information and Privacy Commissioner (IPC) of Ontario, Dr. Ann Cavoukian. The IPC is well known on the global privacy stage for award-winning work toward establishing the Privacy by Design principles. The framework was approved unanimously by the international Data Protection and Privacy Commissioners at the 32nd International Conference of Data Protection and Privacy Commissioners in Jerusalem, Israel, 2010 as an "essential component of fundamental privacy protection."[34]

In the paper 'Privacy by Design, Essential for Organizational Accountability and Strong Business Practices'[35], the IPC speaks to demonstration of accountability to DPAs:

> *The need for organizational accountability remains constant – indeed, it has become more urgent today than ever before. What is changing are the means by which accountability may be demonstrated, whether to individuals, regulators or to business partners. Beyond policy statements, what is needed now are more innovative and more robust methods for assuring that personal data is, in fact, being managed responsibly.*

Alberta

In Alberta, Canada's Health Information Act requires that a Privacy Impact Assessment (PIA) must be reviewed by the Privacy Commissioner before the organization can implement proposed administrative practices and information systems related to the processing of health information. The PIA submission must also include evidence such as policies and procedure documents.

Since the Commissioner examines the organization-wide practices as part of the PIA, the result of this requirement is that the demonstration of accountability is mandated.[36]

---

[34] 32nd International Conference of Data Protection and Privacy Commissioners. (2010) *Resolution on Privacy by Design.* Jerusalem, Israel.
[35] Abrams, M. E., Cavoukian, A., Taylor, S. (November 2009) *Privacy by Design: Essential for Organization Accountability and Strong Business Practices.* Toronto, Canada.
[36] Office of the Information and Privacy Commissioner of Alberta. (2009-2012). *PIAS: Description.* Alberta, Canada. Retrieved from: http://www.oipc.ab.ca/pages/PIAs/Description.aspx. Date Accessed: January 23, 2014.

> *While PIAs are focussed on specific projects, the process should also include an examination of organization-wide practices that could have an impact on privacy. Organizational privacy policy and procedures, or the lack of them, can be significant factors in the ability of the organization to ensure that privacy protecting measures are available for specific projects.*

A presentation delivered by the Office of the Privacy and Information Commissioner of Alberta noted that the regulators can benefit from the organizations' ability to demonstrate accountability.[37] The presentation cited an Order issued by the Office which noted that "an organization has the burden of proving that it had made reasonable security arrangements to protect personal data…. as it is in the best position to provide evidence of the steps it has taken."

European Union

In the European Union, the Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data is an independent advisory body on data protection and privacy, set up under Article 29 of the Data Protection Directive 95/46/EC. It is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. In July 2010, the Working Party published Working Paper 173 which suggested:

> *…a new provision requiring data controllers to implement appropriate and effective measures and to demonstrate this to authorities upon request.*[38]

In 2011, Peter Hustinx, European Data Protection Supervisor, echoed this working party paper's position:

> *Data controllers should be mandated to take all necessary measures to ensure that the data protection rules are complied with. This is the 'principle of accountability' that would require data controllers to be able to demonstrate that they have taken all appropriate measures to ensure compliance.*[39]

---

[37] McLeod-McKay, Diane. (2013). *The Meaning of "Accountability" in the Privacy Law Context.*
[38] Article 29 Data Protection Working Party. (2010). *Opinion 3/2010 on the Principle of Accountability.* Belgium.
[39] Graham, C., Hustinx, P., Vitaliev, D. (2011 June 13). Data Protection and Privacy Issues. *Engineering and Technology Magazine.*

The European Commission acknowledged the opinion, and the Proposal for a Regulation of the European Parliament and the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, commonly called the General Data Protection Regulation (GDPR)[40], addressed the principle of accountability by detailing the obligation of responsibility to comply with the Regulation and to demonstrate compliance in recital (60).

> *Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and **be obliged to** demonstrate the compliance of each processing operation with this Regulation. [Emphasis added]*

The European Parliament's draft report[41] on the Commission's proposal included the following amendment, with the justification that "the concept of accountability should be mentioned explicitly, and it should be clarified that this includes only an obligation to be able to demonstrate compliance on request."

> *Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established in order to ensure accountability. In particular, the controller should ensure and **be able to** demonstrate the compliance of each processing operation with this Regulation.*

The Committee of Civil Liberties, Justice and Home Affairs (LIBE) then submitted amendments[42] to the GDPR that removed the word "accountability" but more explicitly stated the requirements and introduced third party verification.

> *Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the*

---

[40] European Commission. (2012). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Brussels.
[41] European Parliament. (2012). *Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).*Brussels.
[42] Committee on Civil Liberties, Justice, and Home Affairs. (2013). *Draft Report on the proposal for a Regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* Brussels.

> *controller's behalf should be established, in particular with regard to documentation, data security, impact assessments, the data protection officer and oversight by data protection authorities. In particular, the controller should ensure and* ***be able to*** *demonstrate the compliance of each processing operation with this Regulation... [Emphasis added]*

The three versions of the GDPR differ on the level of obligation, but all are aligned on the need for organizations to be accountable and be able to demonstrate that. At the time of printing, the final text of the General Data Protection Regulation had not yet been determined.

International Standards on the Protection of Privacy (Madrid Resolution)

The 2009 International Conference of Data Protection and Privacy Commissioners led to a joint effort by the privacy guarantors from fifty countries, coordinated by the Spanish Data Protection Agency, toward integrating data protection legislations on five continents. The outcome of this initiative was published in the 'Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data,' which included within the Accountability principle:

> *[H]ave the necessary internal mechanisms in place for demonstrating such observances both to data subjects and to the supervisory authorities in the exercise of their powers.*[43]

Binding Corporate Rules (BCR)

BCRs are internal rules (such as a Code of Conduct) within a multinational organization, adopted by multinational groups of companies, which defines its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection.

BCR is a voluntary framework for responsible organizations to demonstrate accountability to DPAs and obtain approval. Once approved, the organization is able to obtain benefits such as abandoning the requirement for standard contractual clauses each time the organization transfers data to a member of its group.

[43] International Conference of Data Protection and Privacy Commissioners. (2009). *International Standards on the Protection of Personal Data and Privacy, The Madrid Resolution.* Madrid, Spain.

The framework for the structure of Binding Corporate Rules[44] requires multinational organizations to demonstrate accountability as it includes:

> *Requirement to submit for DPA approval a detailed application form outlining the organization's program and evidence to show that commitments in the BCRs are being respected (e.g. policies, procedures, training program).*
>
> *An audit program which must be carried out on a regular basis and covers all aspects of the BCRs.*
>
> *Requirement that the DPAs can receive a copy of such audits upon request.*

Council of Europe Data Protection Convention ("Convention 108")

The Convention ETS No 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (of 1981) - which was the first legally binding international instrument with worldwide significance on data protection (commonly referred to as Convention 108). It has served as the backbone of international law in over 40 European countries and has influenced policy and legislation far beyond Europe. It is the only legally binding international treaty dealing with privacy and data protection.[45]

In 2011 the Convention celebrated its 30th anniversary with an initiative toward modernising the treaty by inviting input on the evolving data protection issues. Council of Europe acknowledges the growing prevalence of the discussion around demonstrating accountability by asking commenters: "Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?[46]" The results were:[47]

> *Most of those who replied to this question favour the idea of introducing an obligation to comply with the accountability principle as a guarantee of*

---

[44] Article 29 Data Protection Working Party. (2008).*Working Document WP 154 Setting up a Framework for the Structure of Binding Corporate Rules.* Belgium.
[45] Bygrave, L.A., & Greenleaf, G., & Kierkegaard, S., & Llyod, I., & Saxby, S., & Waters, N. (2011, November 2). 30 Years on- The Review of the Council of Europe Data Protection Convention 108. *Computer Law and Security Review (CLSR), Vol. 27, pp. 223-231.*
[46] Council of Europe. (2011). *Modernisation of Convention 108.*
[47] Molny, J., & Terwangne, C, D. (2011). *Report on the Consultation on the Modernisation of Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data.* Belgium.

improving the protection afforded. Accountability mechanisms should be clearly defined; they should not be excessive and should be implemented by all signatories in the same way.

Some contributors are opposed to the introduction of an obligation to demonstrate compliance because it would constitute a burden, especially for small and medium- sized enterprises.

Iceland

Iceland's Act on the Protection of Privacy as regards the Processing of Personal Data, No. 77/2000 requires that organizations not only monitor their privacy program, but document the results and make them available to DPAs upon request:

The controller shall conduct internal audits on the processing of personal information to ensure that they are processed in accordance with prevailing laws and regulations and the security measures that are to be implemented… They shall none the less be conducted at least annually.

The controller shall see to it that a report is written on each of the measures that the internal audit is comprised of. In such a report, the results of each part of the audit shall be described. Internal audit reports shall be preserved in a secure manner. The Data Protection Authority has the right to review these reports at any time.

Finland

In Finland, the Data Protection Ombudsman advocates the use of a Data Balance Sheet and the concept of accountability reporting as a tool for more efficient, effective, and competitive data processing procedures, as well as for improved operations and reporting, for either internal or external purposes.[48]

The data balance sheet also complies with the principle of accountability, according to which an organization itself demonstrates its compliance with legislation and good practice in data processing and information management. In the future, data protection legislation may require the introduction of practices complying with the accountability principle. Before

[48] The Office of the Data Protection Ombudsman. (2012). *Prepare a Data Balance Sheet.* Finland.

this happens, organizations may nevertheless proactively introduce the data balance sheet at any time.

United Kingdom

While the UK Data Protection Act 1998 does not mandate demonstrating accountability, the UK Information Commissioner's Office (ICO) has a mechanism for organizations to voluntarily demonstrate accountability to the supervisory authority at their own request.

> *The Information Commissioner's Office (ICO) undertakes a programme of consensual audits across the public and private sector to assess their processing of personal information and to provide practical advice and recommendations to improve the way organizations deal with information rights issues.*[49]

Each year, the ICO conducts a number of audits with organizations who have voluntarily approached the ICO and would like to benefit from the knowledge and skills of the ICO's audit team.

United States of America

U.S. Private Sector

In February 2012, the Obama Administration published a paper calling on Congress to pass legislation that applies the Consumer Privacy Bill of Rights in commercial sectors not currently subject to Federal data privacy laws.[50] The paper specifically addresses the Accountability principle and states:

> *Companies that can demonstrate that they live up to their privacy commitments have powerful means of maintaining and strengthening consumer trust.*

The Bill of Rights includes a privacy principle that includes demonstrating accountability:

[49]UK Information Commissioner's Office. (2013). *Auditing Data Protection, A Guide to ICO Data Protection Audits.* United Kingdom.
[50] The White House. (2012). *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.* Washington, DC.

> *Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights. Companies should be accountable to enforcement authorities and consumers for adhering to these principles.*

U.S.-E.U. Safe Harbor

The U.S.–E.U. Safe Harbor framework requires that organizations implement procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented, either through self-assessment or outside compliance reviews[51] and that they should retain their records and make them available upon request in the context of an investigation or a complaint about non-compliance:[52]

> *Organizations should retain their records on the implementation of their Safe Harbor privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction.*

U.S. Public Sector

In the US Public Sector, the National Institute of Standards and Technology (NIST), establishes standards and minimum requirements for federal information systems. In April 2013 NIST published the Privacy Control Catalog, which became Appendix J to the Security and Privacy Controls for Federal Information Systems and Organizations.[53] The NIST standard incorporates the principle of accountability and the requirement to demonstrate accountability in the following control guidance:

> *The development and implementation of a comprehensive governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy.*
>
> *Through internal and external privacy reporting, organizations promote accountability and transparency in organizational privacy operations. Reporting also helps organizations to determine progress in meeting privacy*

[51] Export.gov. (2013). *U.S.-EU Safe Harbor Overview*. United States. Retrieved from: http://export.gov/safeharbor/eu/eg_main_018476.asp. Date Accessed: March 12, 2014.
[52] U.S.-E.U. Safe Harbor FAQ #7
[53] National Institute of Standards and Technology. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations.* United States.

compliance requirements and privacy controls, compare performance across the federal government, identify vulnerabilities and gaps in policy and implementation, and identify success models.

Colombia

Colombia`s data protection Law 1581 *Which Establishes General Provisions for the Protection of Personal Data* and Regulation Decree Number 1377 of 2013 *whereby Law 1581/2012 is partially regulated* mandates demonstrating accountability.[54] In addition, it incorporates the concept of proportionality which may be related to the concerns voiced in response to questions from Convention 108 mentioned above, regarding scalability. The regulation states:

> *The persons Responsible for personal data Processing must be able to demonstrate, at the request of the Superintendence of Industry and Trade, that they have implemented the appropriate and effective measures to comply with the obligations stipulated in Law 1581/2012 and this Decree, in a manner that is proportional… to the responsible person's legal nature and, when applicable, his business size, taking into account if it deals with a micro, small, medium or large business, according to the regulation in force.*

It is expected that more countries will enact laws that require organizations to be able to demonstrate accountability as it is expected that more DPAs will call for organizations to be able to do so as a policy.

Organization of American States

The Organization of American States (OAS) is the world's largest regional forum, established for the purposes of regional solidarity and cooperation among its 35 member states and 67 permanent observer states including the EU.[55]

In November of 2011, the OAS published the Preliminary Principles and Recommendations on Data Protection (The Protection of Personal Data) which

[54] Colombian Ministry of Trade, Industry and Tourism. (2013). *Decrees Number 1377/2013 "Whereby Law 1581/2012 is Partially regulated.* Bogota, Colombia.
[55] Organization of American States. (2014). *About the OAS: Who we Are.* Washington, DC. Retrieved from: http://www.oipc.ab.ca/pages/PIAs/Description.aspx. Date Accessed: January 23, 2014.

included the Accountability Principle with explicit references to demonstrating accountability to DPAs:[56]

> *The data controller is responsible for taking all the necessary steps to follow personal data processing measures imposed by national legislation and other applicable authority. In addition, the responsibility lies with the data controller to show individuals and the appropriate supervisory authority that the data controller is complying with necessary measures, as established by national legislation or other authority to protect the individual's personal data.*
>
> *In short, the law should hold all organizations accountable for how the data entrusted to it is processed. In an accountability regime, data protection standards and requirements are enshrined in law and individual organizations must determine how to meet those standards in practice. The law also should recognize that the particular measures to be taken in implementing these elements should "scalable" – that is, dependent on the nature and volume of the personal information that is processed, the nature of such processing, and the risks to the individuals involved.*

Asia Pacific

Australia

The amendments to the Australia Privacy Act came into effect in March 2014, and include 13 Australian Privacy Principles (APPs). In August 2013 the Office of the Australian Information Commissioner issued a series of guidelines which help to interpret the APPs. APP 1 requires the "Open and transparent management of personal information." The guideline states that the principle enhances the accountability of entities for their personal information handling practices and can build community trust and confidence in those practices.

In addition to being a general statement of organizations' obligation to comply with other principles, APP 1 requires entities to take proactive steps to establish and maintain internal practices, procedures, and systems that ensure compliance with the principles. Entities are also advised to keep a record of the steps taken to ensure that personal information is managed in an open and transparent way. The guidelines state

[56] Organization of American States. (2011). *Preliminary Principles and Recommendations on Data Protection (The Protection of Personal Data).* United States.

that organizations should consider implementing governance mechanisms such as designated privacy officers and regular reporting to the entity's governance body.

Hong Kong

In February 2014, the Office of the Privacy Commissioner for Personal Data in Hong Kong issued a Best Practice Guide[57] for privacy management programmes. Although there is currently no legislative requirement under the Personal Data Privacy Ordinance ("Ordinance"), the paper reflects the Commissioner's expectation for organizations to be able to demonstrate accountability:

> *Data users should embrace personal data privacy protection as part of their corporate governance responsibilities and apply them as a business imperative throughout the organisation, covering business practices, operational processes, product and service design, physical architecture and networked infrastructure.*
>
> *Organisations should establish some form of internal audit and assurance programmes to monitor compliance with their personal data protection policies…Should the organisation be subject to an enquiry, an inspection or an investigation under the Ordinance, these reports may be helpful in demonstrating the organisation's compliance with the Ordinance.*

[57] Office of the Privacy Commissioner for Personal Data, Hong Kong. (2014). *Privacy Programme Management, A Best Practice Guide.* Hong Kong.

Appendix C: Evolution of Nymity's Research on Demonstrating Accountability

In the fall of 2009, at the 30th International Conference of Data Protection and Privacy Commissioners in Madrid, Spain, a joint effort by the privacy guarantors from 50 countries led to the 'Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data' ("Madrid Resolution").[58] The Madrid Resolution contained an accountability principle that stated:

> *The responsible person shall a. Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and b.* ***have the necessary internal mechanisms in place for demonstrating such observances*** *both to data subjects and to the supervisory authorities in the exercise of their power. [Emphasis added]*

As a result, Nymity began to research a pragmatic framework to demonstrate accountability and a workable solution for the privacy office. This book marks five years of Nymity's research in the area of demonstrating accountability, culminating in the release of the Data Privacy Accountability Scorecard™ and ultimately, the Attestor™ solution for demonstrating accountability and compliance.

This section outlines the evolution of Nymity's research on demonstrating accountability.

[58] International Conference of Data Protection and Privacy Commissioners. (2009). *International Standards on the Protection of Personal Data and Privacy, The Madrid Resolution.* Madrid, Spain.

Demonstrating Accountability Success Factors

To achieve Nymity's goal of a pragmatic framework for demonstrating accountability, substantial research was conducted including interviews with DPAs, privacy leaders, and customers. The initial success factors were:

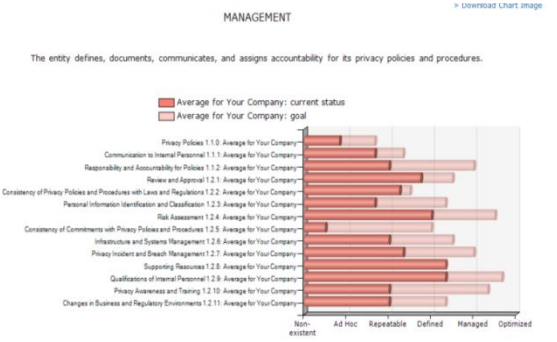
- Must report privacy program status;
- Must be evidence based;
- Must be free.

Demonstrating Accountability using the AICPA/CICA Privacy Maturity Model (2011)

Nymity initially sought to demonstrate accountability using the AICPA/CICA Privacy Maturity Model (PMM). The PMM is a free framework published by the accounting associations in the US and Canada and is based on the 73 criteria found in the Generally Accepted Privacy Principles. The PMM contained five levels of maturity: Ad Hoc, Repeatable, Defined, Managed, and Optimized.

Nymity conducted a research study with several organizations that documented the status of their privacy programs using the PMM, and presented their privacy programs in a workshop to DPAs. The results met the initial success factors:

- ✓ Reported the privacy program status
- ✓ Evidence based
- ✓ Free

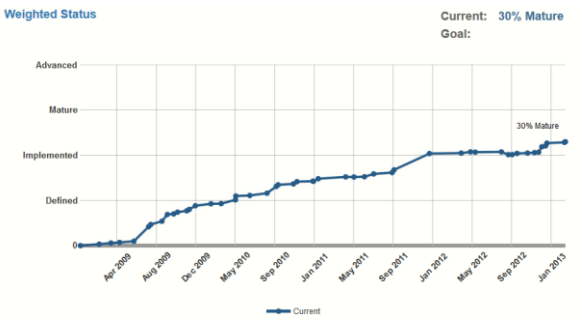


However, the research presented some challenges related to reporting and workability. It was discovered that the 73 criteria are somewhat complicated and are not scalable to all organizations. Also, DPAs wanted to understand the history of the program, and the PMM did not incorporate a timeline. In addition, participants in the study reported that when there was an "optimized" level on the scale, much of the discussion was focused on why an area was not optimized, rather than on the actual status of the program.

Claims Based Self Attestation Methodology (2012)

The outcomes of the research on the PMM led to a second research initiative for demonstrating accountability with additional success factors:

- Easy to use
- Scalable
- Timeline based



Nymity created a claims-based, self-attestation methodology for demonstrating accountability based on four stages of implementing a privacy program. The model enabled organizations to self-report their privacy program over time and provide evidence. All six success factors were met:

- ✓ Reported the privacy program status
- ✓ Evidence based
- ✓ Free
- ✓ Easy to use
- ✓ Scalable
- ✓ Timeline based

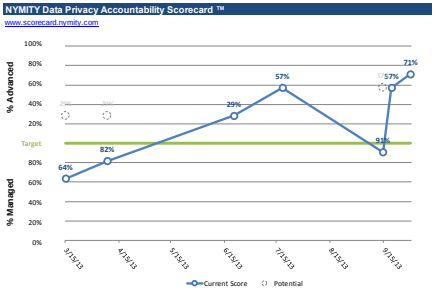
However, when Nymity worked with 11 organizations to conduct proof of concept implementations, two workability challenges emerged: plotting the results was highly subjective (i.e. one person's opinion of "defined" was not consistent with the next), and the evidence collection based on self-attestations was time consuming. As such, Nymity did release this claims based self-attestation methodology, but instead sought a framework which would meet the original six success criteria, with two additional criteria:

- Objective results
- Efficient evidence collection

The Data Privacy Accountability Scorecard™ (2013)

Nymity built upon the claims based methodology to develop the Data Privacy Accountability Scorecard ("Scorecard") featured in Chapter 4. The Scorecard is an evidence-based, easy to use, scalable approach for the privacy office to report the

status of a privacy program over time. Results are calculated objectively and evidence collection is simple and efficient. Nymity tested this framework through pilot projects and found that it met all of the success criteria, and did not observe any more workability challenges.



In the fall of 2013, at the 35th International Conference of Data Protection and Privacy Commissioners in Warsaw, Poland, Nymity announced a feedback draft of the Scorecard as a free resource for privacy offices to monitor, measure, and report on the status of their privacy program, in other words to demonstrate accountability. Microsoft Excel® based templates, training videos, an instruction manual, and additional resources were made available for free at www.scorecard.nymity.com

Nymity Attestor™ Solution for Demonstrating Accountability and Compliance (2014)

In the spring of 2014, at the IAPP Global Privacy Summit in Washington, DC, Nymity will be proud to announce Attestor, a privacy management platform that enables the privacy office to demonstrate accountability and compliance (described in detail in Appendix E).

Appendix D: About Nymity

Nymity is a global research company specializing in accountability, risk, and compliance software solutions for the privacy office. Nymity helps organizations attain, maintain, and demonstrate data privacy compliance, in all jurisdictions, industries, and sectors. Organizations all over the world rely on Nymity's solutions to proactively and efficiently manage their privacy programs – empowering them to comply with confidence. Learn more at www.nymity.com

Appendix E: Nymity Attestor

Attestor is a data privacy program management platform that enables organizations to demonstrate accountability and compliance.

Nymity has partnered with a number of global organizations to successfully implement Attestor to demonstrate accountability and compliance with laws and regulations, codes and standards, and often for reasons related to Binding Corporate Rules (BCR): readiness assessments, implementation, and monitoring. Other business cases include helping to streamline and reduce the cost of privacy audits, assessments such as SOC-2[59], Safe Harbor self-certification, and internal gap analyses.

These organizations range in size and type, but all have one thing in common: they wish to answer the question, 'how do we know that the privacy program is effectively embedded throughout the organization?' They wish to:

- effectively **implement and monitor cross border transfer mechanisms** such as Safe Harbor or Binding Corporate Rules;
- **shift privacy accountability into Operational Units** while **maintaining effective oversight**, in line with enterprise compliance initiatives;
- establish meaningful **accountability metrics** that tell the story of the privacy program and demonstrate, with evidence, that the program is managed effectively; and

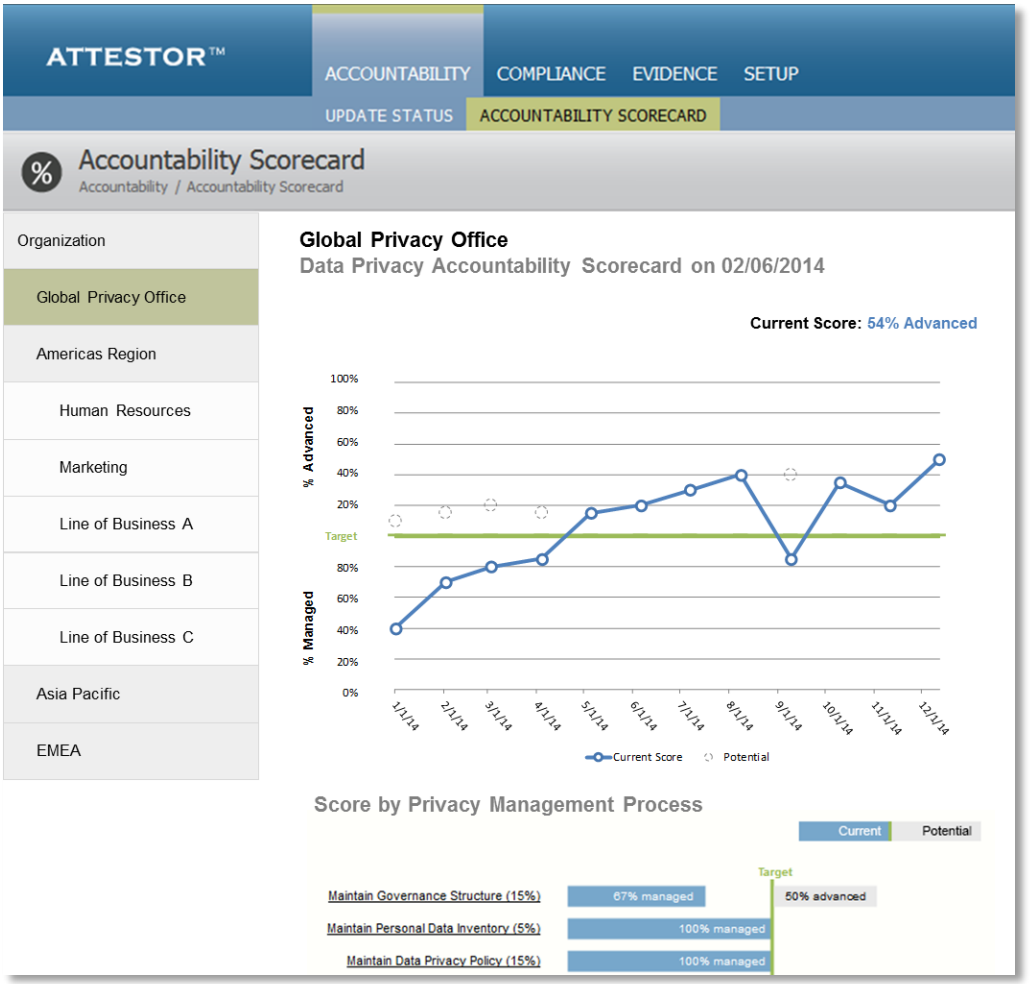
[59] SOC-2 is an attestation report performed by an independent auditor on the controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. Many organizations require third party data processors to provide SOC-2 reports as part of vendor due diligence.

- **attest compliance** to laws and regulations, codes, and/or enforcement actions.

Attestor enables the privacy office to accomplish these objectives.

Demonstrating Accountability using Attestor: Automating the Scorecard

Attestor automates the Data Privacy Accountability Scorecard described in Chapter 4.



In addition to providing a structured approach to evidence collection and automatic calculation of the Data Privacy Accountability Score, Attestor provides advanced functionality to meet the needs of organizations requiring more complex deployments:

- Attestor incorporates the **organizational structure and hierarchy** functionality to support **more complex monitoring and reporting**. Users enter data for a **Reportable Unit**[60] and can view the results as a whole, or drill down into the 13 Privacy Management Processes. A hierarchy structure allows reporting based on region or division. For example, there may be Reportable Units for Canada, United States, and Mexico - Attestor generates an aggregate view of all three countries presented as the Scorecard for North America (an **Aggregate Unit**).

- **Privacy Management Activities** **are assigned a weighting** which is used to calculate the Data Privacy Accountability Score. The Score is no longer as simple as the number of Activities evidenced/number of Activities identified, but it is possible to reflect that not all Activities are equal in a privacy program.

- Reportable Units and Privacy Management Processes can also be weighted to **reflect their importance to the overall program**. An example of weighting the Reportable Units is that the UK might be weighted higher within the EMEA region than others due to volume of data processed there. Another way to utilize weighting is within the Privacy Management Processes – an Operational Unit that relies heavily on third party processors might assign higher weight to Privacy Management Process 7 – Manage Third Party Risk.

- The element of **Frequency is automated**. Users are warned when Evidence is about to expire. If the Evidence does expire, the Score automatically adjusts.

- Attestor collects meta data about Evidence (e.g. title, description, URL, owner) and stores it in an easily searchable **Evidence Library**. Documents

[60] Reportable Units are components of the organization or the privacy program that the privacy office wishes to manage, monitor and report. Reportable Units may be structured as Operational Units, legal entities, countries, functions, lines of business, or a hybrid of several.

reside on customer systems, reducing information security risk and avoiding complications related to version control.

- Users can record **plans** to complete Privacy Management Activities. If a Response is 'no' but the individual is working toward a solution, he or she can enter a comment, a date it is planned for completion, and evidence of progress.

Attesting Compliance using Attestor: Leveraging Accountability Evidence

As outlined in Chapter 7, attesting compliance is accomplished by mapping the Evidence (documentation collected for demonstrating accountability) to the appropriate Rule Source (law, regulation, framework, code internal policy, etc.). The only thing the privacy office needs to do is collect the Evidence; the patent pending methodology underlying Attestor automatically maps the organization's documentation to the Rules.

The privacy office then determines whether the existing documentation satisfies the requirement and either attests compliance or identifies a gap and creates an action plan. This analysis can be supported by Nymity References. For example, when trying to understand if the organization's procedures meet specific jurisdictional requirements, the privacy office may wish to review regulatory guidance or case law to boost their understanding.

Attestor supports over 300 privacy laws, regulations, codes and standards and can accommodate custom rule sources such as an organizations data privacy policy or Binding Corporate Rules.

Glossary

Aggregate Unit: a parent organizational unit that combines the results of the data entered into its child Reportable Units

Article 29 Working Party: independent European advisory body. The Working Party's mission is to ensure the uniform application of Directive 95/46/EC, providing opinions and making recommendations or drafting working documents that are all available on the Internet. The Article 29 Working Party's members are representatives of the different national data protection authorities, the European Data Protection Supervisor and representatives of the European Commission[61]

Attestor: a privacy management platform that enables the privacy office to demonstrate accountability and compliance

Binding Corporate Rules (BCR): legal tool that can be used by multinational companies to ensure an adequate level of protection for the intra-group transfers of personal data from a country in the EU or the European Economic Area (EEA) to a third country[62]

Consent Decree: enforcement mechanism in the United States which is a binding, voluntary agreement of a person or company to take specific actions (such as ceasing the conduct that is the subject of the suit/case) without admitting fault or guilt

Continuous Activities: Privacy Management Activities that are embedded into day-to-day operations

[61] Belgian Commission for the Protection of Privacy
[62] European Data Protection Supervisor

Core Activities: Privacy Management Activities defined by the privacy office as fundamental to privacy management

Data Breach: unauthorized collection, use, access, retention, or disclosure of personal data

Data Privacy Accountability Score: status of the privacy program represented as a percentage of the Core (% Managed) and Elective (% Advanced) Privacy Management Activities which are being completed and evidenced on an ongoing basis

Data Protection Authority (DPA): regulatory body which is in charge of monitoring the processing of personal data within its jurisdiction[63]

Demonstrating Accountability: being able to show that the organization has an established privacy program in place

Elective Activities: Privacy Management Activities defined and supported by the privacy office, but not mandatory

Employees: internal personnel, including employee, contractors, agents, and others acting on behalf of the organization[64]

Enforcement Action: action by a regulatory body or organization to make sure that its rules are being followed, e.g. fines or sanctions, consent decrees, settlements

Evidence: formal or informal documentation to support that a Privacy Management Activity was completed

Evidence Collection Question: closed (i.e. yes/no) questions that are designed to compel Evidence from Owners

Frequency: the rate at which a Privacy Management Activity should occur (e.g. annually, semi-annually, quarterly, monthly)

Individual: the person about whom personal data is being collected (sometimes referred to as the data subject)[65]

---

[63] European Data Protection Supervisor
[64] AICPA/CPA Canada Generally Accepted Privacy Principles
[65] AICPA/CPA Canada Generally Accepted Privacy Principles

Nymity Privacy Management Accountability Framework (Framework) comprehensive, jurisdiction-neutral, and industry-neutral listing of 150+ Privacy Management Activities within 13 Privacy Management Processes

Operational Unit: Department, division, business unit, legal entity or function within an organization (e.g. customer service, sales, marketing, human resources, information security, finance)

Owner: the individual responsible for the management and monitoring of a Privacy Management Activity

Outsourcing: the use and handling of personal data by a third party that is acting on behalf of the organization

Periodic Activities: Privacy Management Activities that are discrete projects or tasks with a defined start and end, performed on a set Frequency

Policy: a written statement that communicates management's intent, objectives, requirements, responsibilities, and standards[66]

Potential Score: percentage of Elective Privacy Management Activities (% Advanced) completed and evidenced, where the Target Score has not yet been reached

Privacy Management Activities ("Activities"): ongoing activities that have a positive impact on the processing of personal data

Privacy Management Process: category of Privacy Management Activities that are structurally aligned with how privacy programs are maintained

Privacy Notice: statement provided to Individuals detailing the organization's personal data handling practices, the rights and obligations of the organization and the individuals, and mechanisms for redress

Privacy Office: the individual or individuals responsible for privacy

Privacy Officer: official charged with ensuring that an organization develops and adheres to a Privacy Policy. This person, appointed by a designated approving

[66] AICPA/CPA Canada Generally Accepted Privacy Principles

authority, oversees employees who have access to and responsibility for the organization's privacy infrastructure[67]

Privacy Program: the policies, communications, procedures, and controls in place to manage and protect personal information in accordance with risk and compliance requirements[68]

Reportable Units: an organizational unit of the company that represents a scope - such as a legal entity, Operating Unit, product line, business area, department, or function

Response: 'yes' or 'no' answer to the Evidence Collection Question, and comment to provide additional context

Rule: specific provision found in a Rule Source, such as a requirement, clause, provision, or term

Rule Sources: rules of law, regulations, codes, standards, and internal rule sources such as data privacy policies or Binding Corporate Rules

Target Score: Data Privacy Accountability Score of 100% Managed, when all Core activities are completed and evidenced

Third Party Processors: service provider that is not affiliated with the organization that collects or processes personal data on its behalf

[67] International Association of Privacy Professionals.
[68] AICPA/CPA Canada Generally Accepted Privacy Principles