

# Nymity Privacy Accountability Charts

## Three Charts to Assist Privacy Professionals with Explaining Privacy Accountability

Nymity produced these charts to assist privacy professionals in explaining accountability, compliance and an effective privacy program.

### STEP 1 Privacy Compliance Criteria

This chart assists privacy professionals in explaining the sources of compliance expectations that they must:

1. monitor to ensure the organization maintains compliance
2. research when the organization embarks on a new operational initiative

Accountable organizations can demonstrate they do both.

### What is Privacy Accountability?

Nymity views privacy accountability as an organization being responsible for privacy by implementing an effective privacy program, maintaining compliance and being able to demonstrate they are doing both.

### Privacy Accountability

<p><b>Organizations are responsible for:</b></p> <ul style="list-style-type: none"> <li>• Compliance</li> <li>• Maintaining an effective privacy program</li> </ul>	<p><b>Organizations account to:</b></p> <ul style="list-style-type: none"> <li>• Senior Management</li> <li>• Regulators/DPAs/Commissioners</li> <li>• Customers/Public/Business Partners</li> </ul>
---	--

### STEP 2 Privacy Program Mechanisms

This chart assists when explaining the components of an effective privacy program. The chart is structured to show core mechanisms found in many privacy programs and what mechanisms are found in a mature privacy program. It can be used to explain the current status of an organization's privacy program and discuss what the program should look like in the future.

Accountable organizations can demonstrate they have implemented and are maintaining an effective privacy program.

### Supporting Appendixes

1. Estimating Accountability Benefits
2. Privacy Office Demonstrating Accountability
3. Privacy Framework History
4. Accountability Principles from Frameworks
5. Privacy by Design - Accountability in Practice
6. How Nymity Helps
7. About Nymity

### STEP 3 Demonstrating Accountability

This chart assists privacy professionals in explaining the options organizations have when assessing their privacy program and producing reports as to the status of the privacy program and any inherent risks.

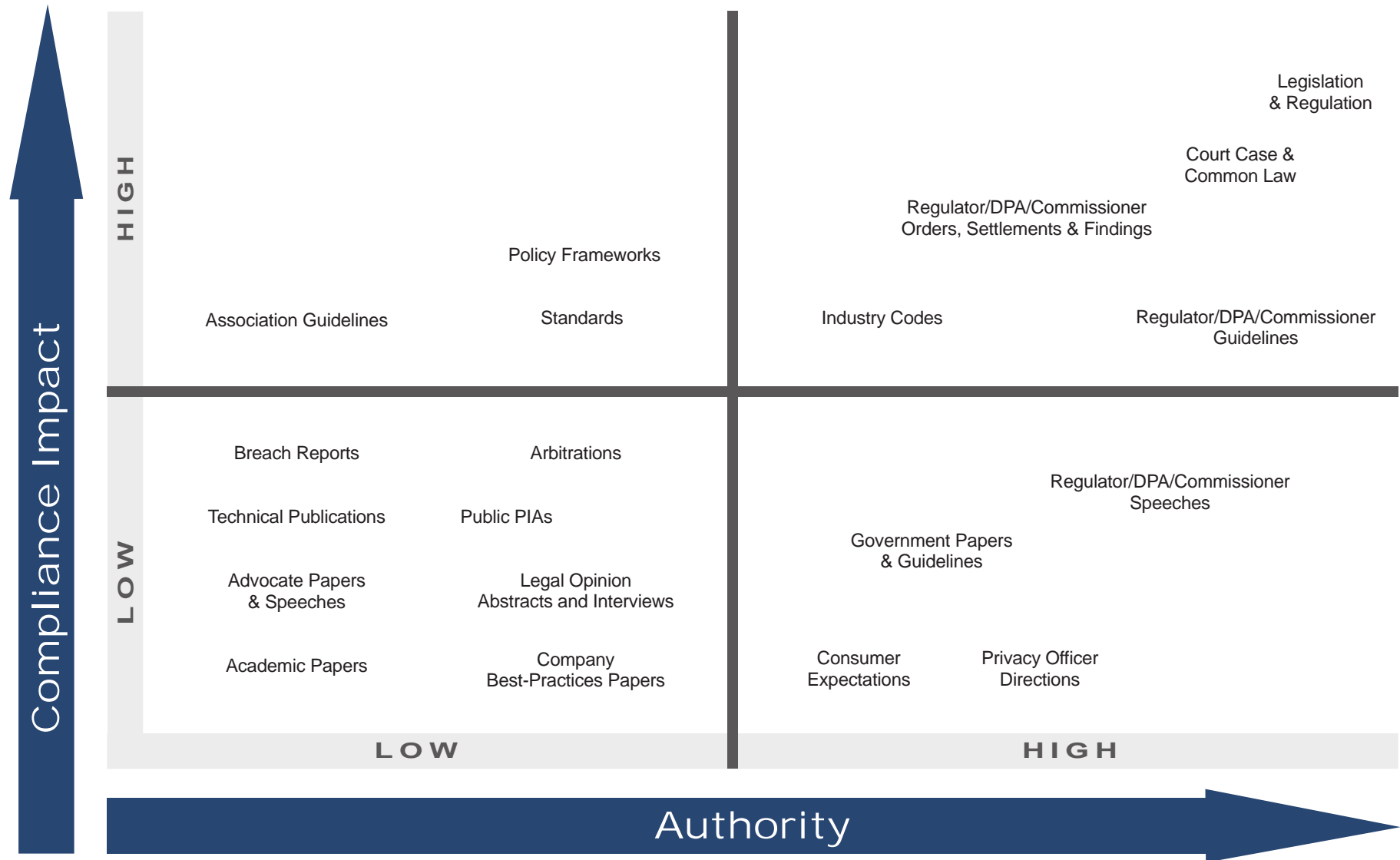
Accountable organizations can report the status of their privacy program and its effectiveness.

**Explaining Privacy Accountability – Video Training**  
 Visit [www.nymity.com](http://www.nymity.com) to review the Accountability Chart Video. (April 2011)

**Get Latest Version of Charts**  
 Visit [www.nymity.com](http://www.nymity.com) to get the latest version of the Accountability Charts.

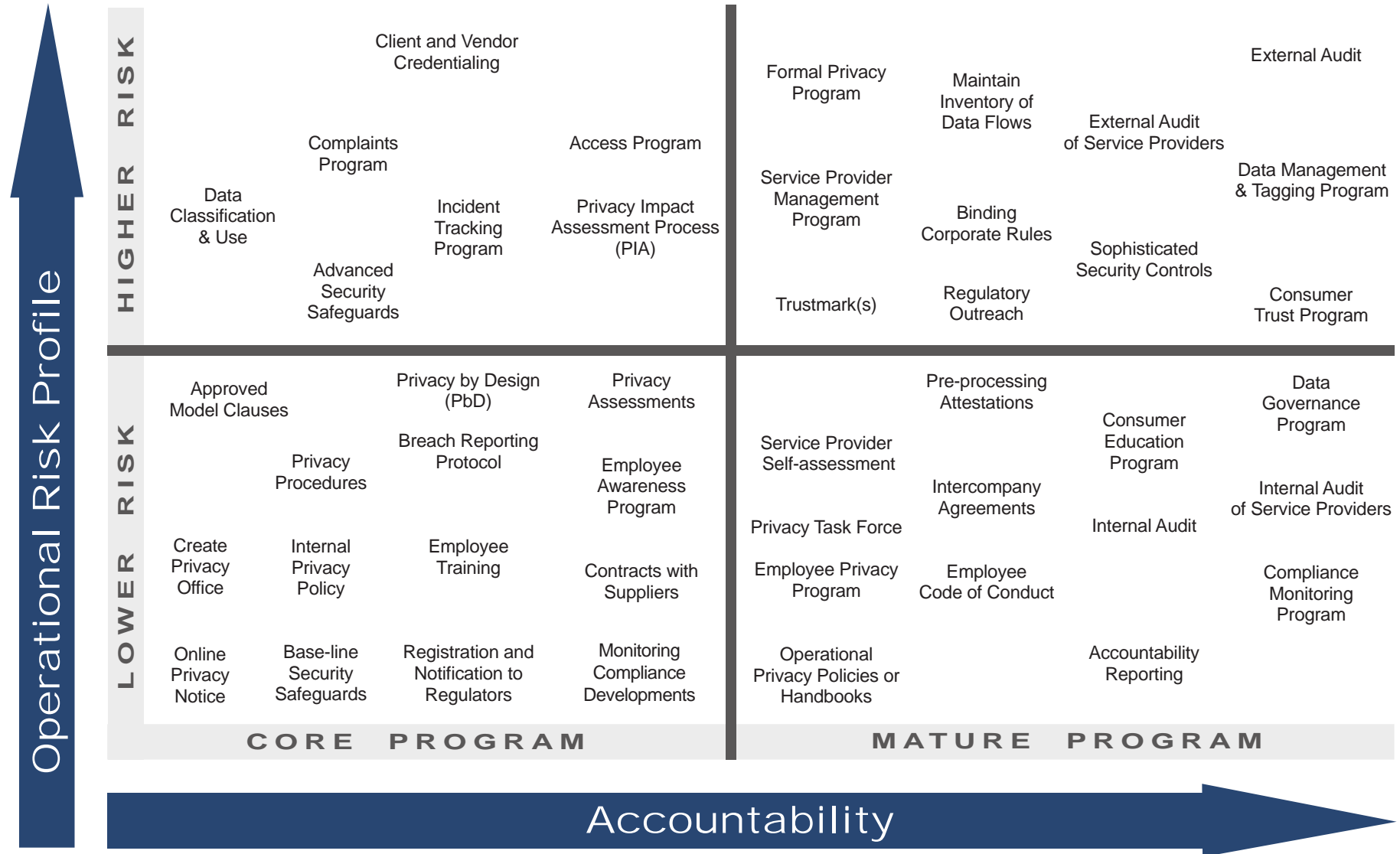
# Privacy Compliance Criteria

## Sources of Rules, Expectations and Best-Practices



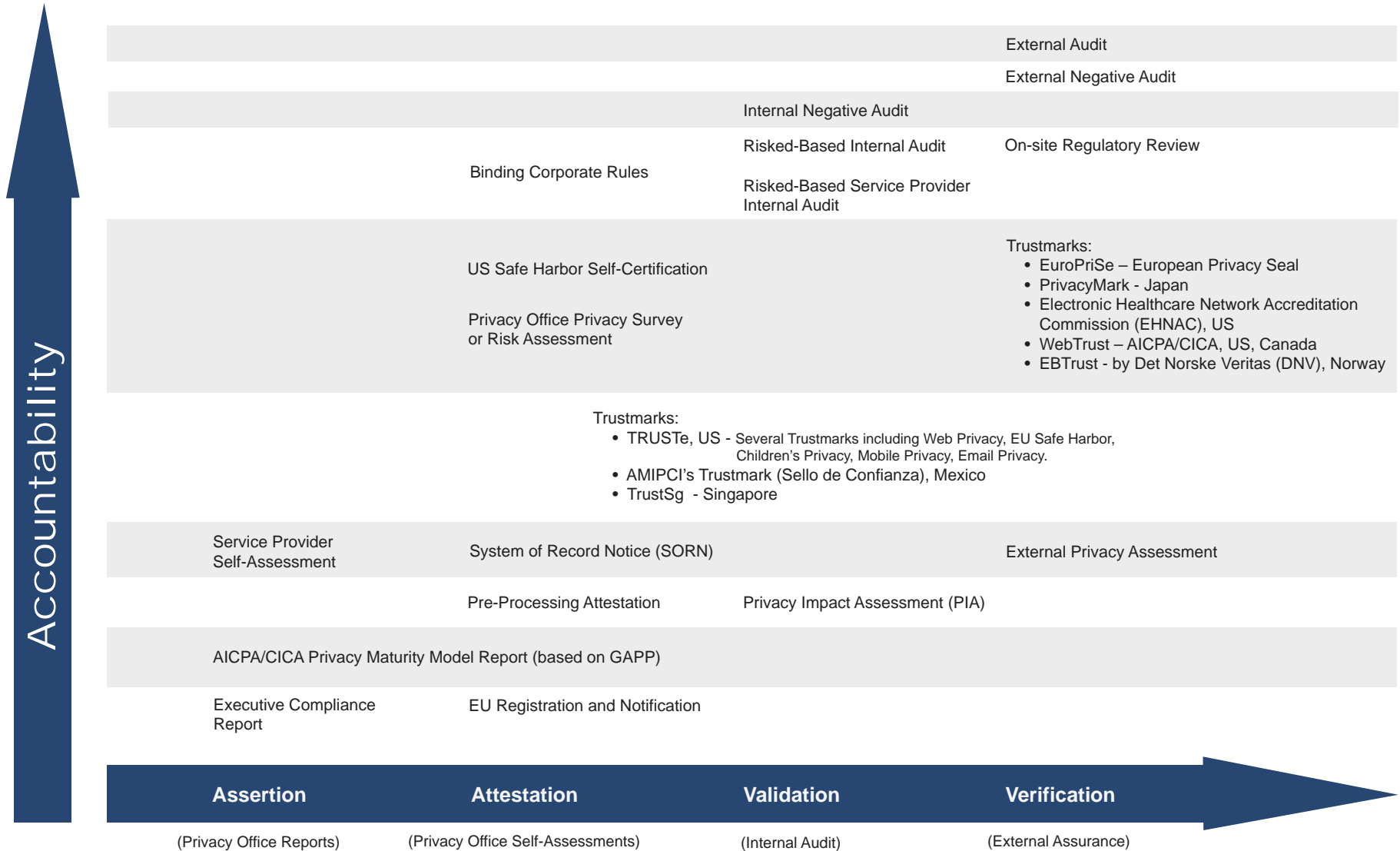
# Privacy Program Mechanisms

Common Components of Privacy Programs






# Demonstrating Accountability

## Common Mechanisms for Assessing and Demonstrating Compliance



# Appendix 1: Estimating Accountability Benefits

## Accountability benefits and drivers for senior management, Regulators/DPAs/Commissioners and Customers/Public/Partners

	Accountability Benefits	Applicable	Value
	<b>Being Accountable to Senior Management</b> Reduced risk of data breach Reduced risk of being found non-compliant Simplified compliance strategy Enhanced product innovation Enhanced management reporting	Y / N Y / N Y / N Y / N Y / N	\$ _____ \$ _____ \$ _____ \$ _____ \$ _____
	<b>Being Accountable to Regulators/DPAs/Commissioners</b> Reduced likelihood of investigations or fines Ability to demonstrate compliance due-diligence Enhanced regulatory outreach	Y / N Y / N Y / N	\$ _____ \$ _____ \$ _____
	<b>Being Accountable to Customers/Public/Partners</b> Enhanced transparency Enhanced brand (or brand protection) Reduced risk of harm for consumers	Y / N Y / N Y / N	\$ _____ \$ _____ \$ _____

## Accountability Drivers

<b>Senior Management</b> Lower compliance costs, brand protection, data breach reduction, governance over increased regulatory expectations and increased enforcement and risk mitigation in general.	<b>Regulators/DPAs/Commissioners</b> Increased expectation from enforcement bodies that an organization should be able to demonstrate accountability.	<b>Customers/Public/Partners</b> Due to complexities in: privacy notices, technology, and uses of personal data there is a shift from a reliance on consent to an organization being more responsible when using personal data.
--	--	--

# Appendix 2: Privacy Office Demonstrating Accountability

## Accountability Assertions and Attestations by the Privacy Office



### Privacy Office Reporting

Nymity's view is that a privacy office can cost-effectively demonstrate accountability through an assertion (report from the privacy office) or an attestation (self-assessment from the privacy office). The results can be shared with internal, and in some cases, external stakeholders.

### Privacy Maturity Model

Nymity believes the Privacy Maturity Model (PMM) from the AICPA/CICA (internationally endorsed by ISACA) is an ideal accountability reporting framework for assertions and attestations. The following example is an organization documenting the status of criteria 3.2.2 Consent for New Purposes and Uses then reporting it on a Choice and Consent report.

### Step 1

**Organizations document the status of their privacy program as an assertion or after conducting a self assessment (attestation).**

**Consent for New Purposes and Uses (3.2.2)**

If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the individual is notified and implicit or explicit consent is obtained prior to such new use or purpose.

Criteria is Not Applicable	Current	Goal
<b>Non-Existent</b> Management processes are not applied at all.	<input type="checkbox"/>	<input type="checkbox"/>
<b>Ad Hoc</b> Individuals are not consistently notified about new proposed uses of personal information previously collected.	<input type="checkbox"/>	<input type="checkbox"/>
<b>Repeatable</b> Individuals are consistently notified about new purposes not previously specified. A process exists to notify individuals but may not be fully documented and consent might not be obtained before new uses.	<input type="checkbox"/>	<input type="checkbox"/>
<b>Defined</b> Consent is obtained and documented prior to using personal information for purposes other than those for which it was originally collected.	<input type="checkbox"/>	<input type="checkbox"/>
<b>Managed</b> Processes are in place to ensure personal information is used only in accordance with the purposes for which consent has been obtained and to ensure it is not used if consent is withdrawn. Monitoring is in place to ensure personal information is not used without proper consent.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>Optimized</b> Consent processes are periodically reviewed to ensure consent for new purposes is being appropriately recorded and acted upon and where necessary, improvements made. Automated processes are followed to test consent prior to use of personal information.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

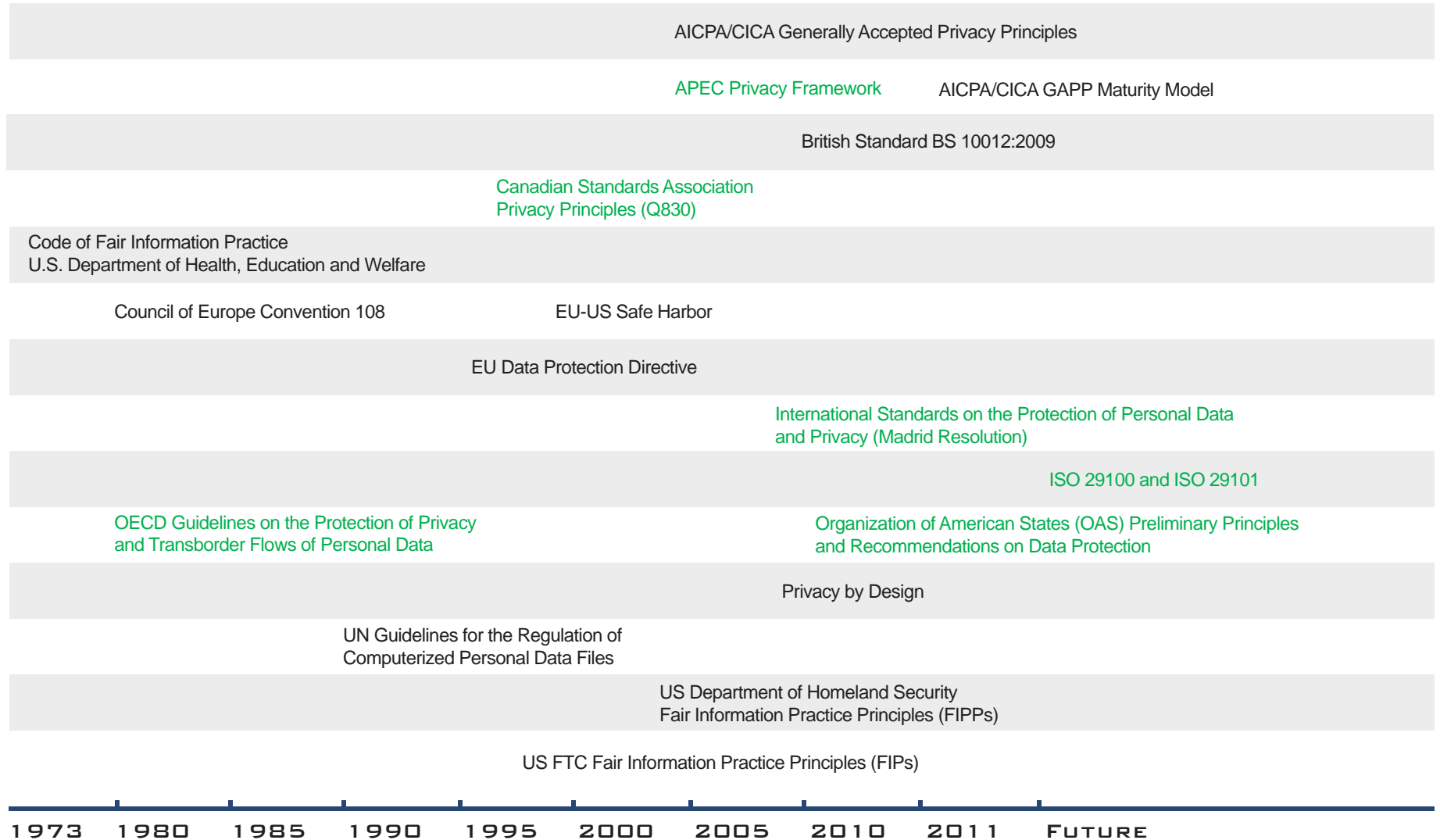
### Step 2

**Privacy office produces accountability reports.**

# Appendix 3: Privacy Framework History

## Frameworks Listed Alphabetically

■ Includes an Accountability Principle

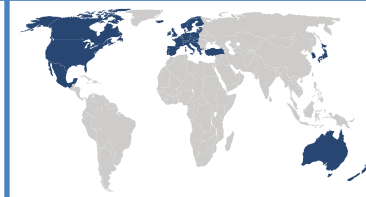


# Appendix 4: Accountability Principles from Privacy Frameworks

## OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

### Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

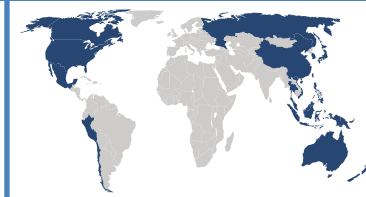


Countries: Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States.

## APEC Privacy Framework

### IX. Accountability

26. A personal information controller should be accountable for complying with measures that give effect to the Principles stated above.



When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

Countries: Australia, Brunei, Canada, Chile, China, Chinese Taipei, Hong Kong, Indonesia, Japan, South Korea, Malaysia, Mexico, New Zealand, Philippines, Papua New Guinea, People's Republic of China, Peru, Russia, Singapore, Thailand, United States, Vietnam

## International Standards on the Protection of Privacy (Madrid Resolution)

### 11. Accountability principle.

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 observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23.



Country: International

## Canadian Standards Association's Model Code for the Protection of Personal Information (Q830)

### Principle 1 - Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

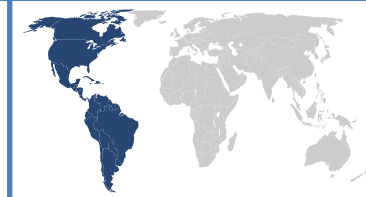


Country: Canada

## Organization of American States (OAS) PRELIMINARY PRINCIPLES AND RECOMMENDATIONS ON DATA PROTECTION (THE PROTECTION OF PERSONAL DATA)

Principle 5: Accountability. 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. The latter should include how the data controller manages requests for access to personal data information and what kind of personal information the data controller processes.

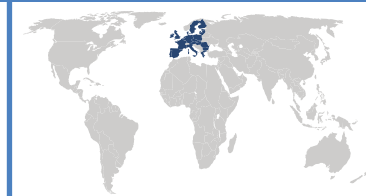


Countries: Antigua and Barbuda, Argentina, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba, Dominica (Commonwealth of), Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, The Bahamas (Commonwealth of), Trinidad and Tobago, United States, Uruguay, Venezuela (Bolivarian Republic of)

## Proposed Amendments to EU Data Protection Directive

Article X - Implementation of data protection principles

- a) The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.
- b) The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request.



Countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom



# Appendix 5: Privacy by Design, Accountability in Practice

Accountability in Practice	Privacy by Design
Accountable organizations privacy office proactively implements effective privacy programs plus monitor for changes in rules, expectations and best-practices.	<p><b><i>Proactive not Reactive; Preventative not Remedial</i></b>                      The <i>Privacy by Design</i> (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events <i>before</i> they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, <i>Privacy by Design</i> comes before-the-fact, not after.</p>
Accountable organizations privacy programs include processes that ensure privacy is a default setting for all practices that involve an individual's personal data.	<p><b><i>Privacy as the Default</i></b>                      We can all be certain of one thing – the default rules! <i>Privacy by Design</i> seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, <i>by default</i>.</p>
Accountable organizations ensure the privacy office is a key player of any new product, service or process involving personal data.	<p><b><i>Privacy Embedded into Design</i></b>                      Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.</p>
Accountable organizations privacy office is equipped to consult with the operational units to optimize privacy without restricting operations.	<p><b><i>Full Functionality – Positive-Sum, not Zero-Sum</i></b>  <i>Privacy by Design</i> seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. <i>Privacy by Design</i> avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.</p>
Accountable organizations maintain appropriate safeguards during the collection, use, disclosure and destruction of personal data.	<p><b><i>End-to-End Security – Lifecycle Protection</i></b>  <i>Privacy by Design</i>, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, <i>Privacy by Design</i> ensures cradle to grave, lifecycle management of information, end-to-end.</p>
Accountable organizations demonstrate the effectiveness of the organization's privacy program to internal stakeholders, and when appropriate, external stakeholders.	<p><b><i>Visibility / Transparency</i></b>  <i>Privacy by Design</i> seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.</p>
Accountable organizations believe they are custodians of an individual's personal data and have a responsibility to use, disclose, maintain, protect and delete the individual's personal data without the need for the individual's participation, or upon their request.	<p><b><i>Respect for Users</i></b>                      Above all, <i>Privacy by Design</i> requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.</p>

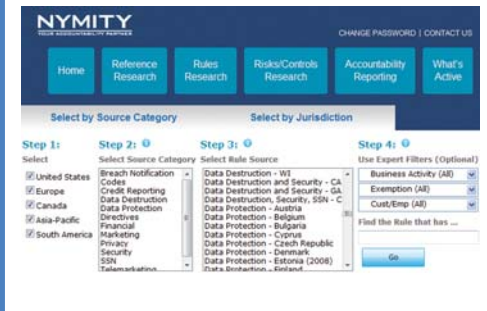
# Appendix 6: How Nymity Helps

## Your Accountability Partner

### Nymity Compliance and Accountability Solutions

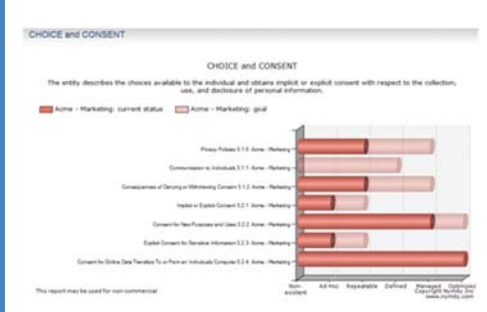
Nymity provides a comprehensive privacy solution that includes three research tools that provide knowledge on demand; plus four software tools that provide ongoing resources for compliance and accountability.

**Research Tools**



On-Demand Expertise

---



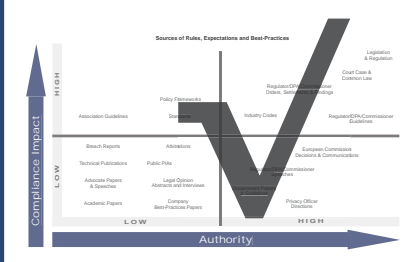
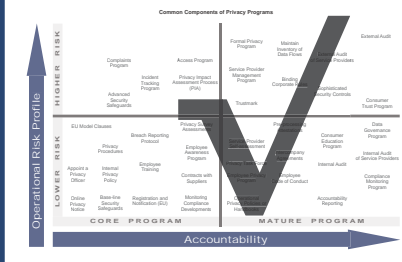
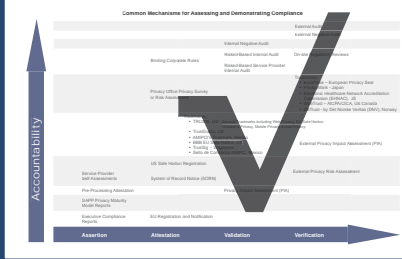
On-Going Resources

RESULTS



### Customer Compliant and Accountable

Customers can cost-effectively and proactively understand compliance criteria, maintain an effective privacy program and demonstrate they do both.

	<p>Understand Your Compliance Criteria</p>
	<p>Maintain Effective Privacy Program</p>
	<p>Report the Status of Your Privacy Program</p>

Contact Nymity for a Free Demonstration and Trial at [info@nymity.com](mailto:info@nymity.com)

# Appendix 7: About Nymity

Nymity provides a comprehensive global compliance and accountability solution that assists organizations in maintaining compliance, implementing an effective privacy program, and being able to demonstrate both. Nymity's solution consists of three research tools that provide knowledge on demand; plus four software tools that provide ongoing compliance and accountability resources.

## In-House Team of Dedicated Privacy Experts

Nymity has an expert team of privacy lawyers and former chief privacy officers that are 100% dedicated to producing the content for Nymity's Research Tools (Nymity does not offer consulting). The expert team utilizes Nymity's controls-based research methodology that has been proven to provide customers the information they need to gain the knowledge they want and saves them huge amounts of time doing so.

## Worldwide Group of Research Contributors

Nymity works with a worldwide group of research contributors to provide an on-the-ground version of what is happening. These individuals are also expert in their various disciplines and help us understand the local nuances that are as important as the written compliance requirements themselves.

## Global, Regional, Country, State/Province

Nymity compliance and accountability solutions provide flexible and scalable configuration options that works well for organizations operating in a single state/province/region/country as well as multi-national organizations.

## 10 Years - Over 1000 Subscribers

2012 will mark the 10<sup>th</sup> year of Nymity providing compliance solutions to privacy professionals. Starting in Canada in 2002, Nymity has grown into the global premier privacy compliance solution provider with over 1000 subscribers around the world. Nymity customers represent all sectors and all industries – small companies to large multinational corporations, healthcare providers, regulators and government.

## History in Accountability

Since 2002, Nymity's expert team have analyzed hundreds of privacy laws and thousands of legal documents in all jurisdictions of the world against the accountability principle. In 2011, Nymity launched its accountability reporting tool.

## Customer Service

Subscribers of Nymity work directly with a business development manager who provides custom configurations, custom training and phone/email support. Every call returned, every email responded to.

