This paper provides an in-depth understanding of a methodology for baselining privacy management/accountability in any organization regardless of size, sector/industry, jurisdiction, or maturity of the privacy program. It also enables organizations to compare privacy management with others using this methodology. This paper includes all necessary tools to baseline and benchmark privacy management for free as well as provides an understanding of the underlying methodology for the software tool, Nymity Benchmarks™.
Nymity Privacy Accountability Baselining and Benchmarking Methodology™

This paper provides an in-depth understanding of the Nymity Privacy Accountability Baselining and Benchmarking Methodology™ - a methodology that enables organizations of any size, sector/industry, jurisdiction, or privacy program maturity to: (1) baseline privacy management in their organization; and (2) compare privacy management to others using this methodology. Reviewing this paper will provide:

1. A free framework to baseline privacy management;
2. A worksheet template to baseline privacy management (refer to Appendix A);
3. Resource considerations when implementing Privacy Management Activities (refer to Appendix B);
4. The ability to compare privacy management at your organization with others; and
5. An in-depth understanding of the underlying methodology used in Nymity Benchmarks™, a subscription-based software tool for benchmarking privacy management.

Needs of the Privacy Office

An integral part of the privacy office’s role is to design, implement, mature, and manage an effective privacy program, in other words, to be accountable. Regardless of the level of the privacy program maturity, most privacy offices at some point face the challenge of answering the following questions:

What is the status of privacy management in our organization? Documenting the status of privacy management at an organization is not a simple undertaking. Identifying privacy management activities outside of the privacy office can be time consuming, especially without a framework to assist in this initiative.

Where do we start? Whether starting with a blank slate or overhauling an existing privacy program, getting started can be a daunting task. A baseline of privacy management within the organization is helpful at all stages of implementing and maturing a privacy program.

What should we put in place? What are accountability best-practices or common practices? Is there an existing framework of privacy management activities?

Organizations typically create a privacy office, the individual or individuals responsible for privacy, with the primary objective to ensure compliance with privacy laws. The role and responsibility of the privacy office include:

- Advising Stakeholders – liaising with operational units to ensure compliant practices and responsible personal data processing;
- Maintaining the Privacy Program – maintaining a governance structure, policies, procedures, notices, training and awareness, data security, vendor management, breach response protocol, and much more;
- Responding to Data Breaches – leading the team through incident responses and privacy breaches;
- Responding to Inquiries and Complaints - handling interactions with customers, employees, lawful authorities, and regulators;
- Personal Development - increase the knowledge and skills of the individual or individuals in the privacy office.
What are others doing?
What privacy management activities are other privacy offices implementing to be accountable? How do I compare?

**Accountability = Privacy Management = Privacy Management Activities**
Fundamentally, privacy management is made up of privacy management activities (“Activities”) which are distinct activities affecting positive impact for the processing of personal data. Privacy management activities go beyond the privacy office and the privacy program and they reflect Activities found throughout the organization where privacy has been embedded into operational practices. Nymity’s Research on accountability has identified over 150 privacy management activities which are outlined in the Nymity Privacy Accountability Management Framework™ in Appendix A. It is these Activities that are the foundation for this methodology.

**Privacy Management goes Beyond the Privacy Office**
Privacy management goes beyond the Activities performed by the privacy office. It consists of all activities conducted throughout the organization that affect the processing of personal data. From the perspective of the privacy office, these Activities can be considered:

1. **Implemented by the Privacy Office:** The privacy office has direct responsibility for maintaining several privacy management activities, for example, managing a privacy management policy or maintaining PIA guidelines and templates.

2. **Influenced by the Privacy Office:** In some cases, the privacy office helps other parts of the organization embed privacy into their operational practices. Examples of these privacy management activities would include the privacy office working with customer services to maintain procedures to address complaints or working with marketing to ensure privacy is embedded in notices to customers.

3. **Independent of the Privacy Office:** In some cases, the privacy office observes organizational privacy management activities without having much influence. For example, purchasing will have sophisticated procedures for onboarding of new vendors, or legal will have integrated Elective privacy controls into contracts, or Human Resources may have already been treating employee personal data with confidentiality. In these cases, the privacy office can leverage other organizational privacy management activities in the privacy program.

**Introducing Nymity Privacy Accountability Baselining and Benchmarking Methodology**
Whether an organization already has an established program, or is just starting, it is advantageous to baseline the privacy program. Even if the privacy office is new, the organization has activities in place that will positively impact privacy; these activities can be considered privacy management activities and can be incorporated into the privacy program. The following outlines a methodology for baselining and benchmarking privacy management.

Appendix A includes a template that can be used to baseline privacy management. This editable template is available in MS Excel worksheet at [www.scorecard.nymity.com](http://www.scorecard.nymity.com).
Baselining Privacy Management/Accountability

The privacy office does not need to start with a blank page when identifying Activities. Instead, the privacy office can simply use the Nymity Privacy Management Accountability Framework in Appendix A as a starting point. Using this Framework, the privacy office will likely find that there is much more privacy management taking place in the organization than expected. To do this, the privacy office simply approaches other areas within the organization to identify all existing privacy management activities, for example, Activities found in Marketing, IT, HR, Legal, and business and operational units.

Assign Status

To baseline privacy management, assign a status to each of the Activities found in the Nymity Privacy Management Accountability Framework (refer to Appendix A). Each Activity will fall into one of four status categories:

1. **Implemented**: Core or Elective privacy management activity is in place.
2. **Planned**: Privacy management activity is planned in the next 12 months.
3. **Desired**: Privacy management activity is desired but currently not planned.
4. **Not Applicable N/A**: Privacy management activity is not applicable to our organization or this part of the organization.

When using this methodology it may be beneficial to use status sub-categories that provide additional information to more effectively communicate the status to others. When assessing status these sub-categories can be used if desired.

---

1 When baselining privacy management, the status Implemented has two statuses, Core and Elective.
**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 was unlikely that many organizations had documented policies for cloud computing or bring-your-own-device (BYOD); however, they are becoming increasingly more 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 Activity 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 Privacy Management Accountability Framework found in Appendix A 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; 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 is simply 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 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
Not only does each privacy management activity have a Status, it also has Attributes. The Attributes, as defined in this methodology, are straight-forward and often used for demonstrating accountability.
The Attributes are:

1. Core or Elective (mandatory)
2. Owner (optional)
3. Frequency (optional)

For example, when demonstrating accountability using the Data Privacy Accountability Scorecard, found at www.scorecard.nymity.com, there are benefits of taking the extra step of assigning one or more of these attributes. However, the selection of Core or Elective for the status of Implemented is important for benchmarking purposes. The following describes the methodology on how they are to be assigned:

1. **Core or Elective**
   
   Each of the Implemented Activities needs to be assigned as either Core or Elective. This is a mandatory step for benchmarking.

   **Core Activities** are defined by the privacy office as fundamental to privacy management. These fundamental privacy management 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 privacy management 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 simply non-core, in other cases they may be leading edge, such as measuring comprehension of privacy training and adjusting the curriculum to reflect learning needs. Other times, Elective Activities are considered nice to have, but not critical to privacy management, such as maintaining posters and videos related to privacy awareness.

2. **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 (found in the Privacy Accountability Management Framework in Appendix A) 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.
3. **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**

The table below illustrates how an organization may baseline its privacy program across three different Operational Units (OUs):

<table>
<thead>
<tr>
<th>OU</th>
<th>Privacy Management Activity</th>
<th>Status</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Measure participation in data privacy training activities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td></td>
<td>N/A</td>
<td>Desired</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Planned</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Implemented</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Core</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Elective</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Frequency</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Owner</td>
</tr>
<tr>
<td>B</td>
<td>Measure participation in data privacy training activities</td>
<td>Update Planned</td>
<td>Elective</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Quarterly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OU B</td>
</tr>
<tr>
<td>C</td>
<td>Measure participation in data privacy training activities</td>
<td>Scheduled</td>
<td>Core</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HR</td>
</tr>
</tbody>
</table>

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 the completion of the entire 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 Accountability Baselining and Benchmarking Methodology enables organizations to build upon the baseline in order to implement and benchmark the program.
Benchmarking Privacy Management/Accountability

Capturing the status and attributes of Activities using the structured methodology enables the comparison of privacy management (including components of the privacy program\(^3\)). Two or more programs can be compared over time on the basis of whether Activities are Implemented as Core or Elective, Planned, Desired, or Not Applicable. This information can be useful when the privacy office is communicating the status of privacy management, identifying strengths and weaknesses, or establishing priorities.

**Illustrative Example**

Continuing from the previous example, this table illustrates how an organization uses the information gathered during baselining to benchmark its privacy program:

<table>
<thead>
<tr>
<th>OU</th>
<th>Privacy Management Activity</th>
<th>N/A</th>
<th>Desired</th>
<th>Planned</th>
<th>Implemented</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Measure participation in data privacy training activities</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>B</td>
<td>Measure participation in data privacy training activities</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Measure participation in data privacy training activities</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

As with the baselining example above, for simplicity, this example examines 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\(^4\)).

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

---

\(^3\) For the purposes of methodologies, Nymity considers the privacy program as the activities under the control of the privacy office. Privacy management is considered a broader category of privacy management, that is, as activities throughout the organization that have a positive impact on the processing of personal data.

\(^4\) Operational Unit A and B both categorized the Activity as Implemented as part of the baselining exercise (refer to the table, Types of Benchmarking). 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 or Elective.
### Types of Benchmarking

<table>
<thead>
<tr>
<th>Benchmarking Outcome</th>
<th>Example Question</th>
<th>Example Responses°</th>
</tr>
</thead>
</table>
| **Comparison**       | How do the privacy programs compare between Operational Units X, Y, and Z? | - Unit X takes the minimal steps necessary based on a limited number of Core Activities  
- Unit Y has a more Elective 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**         | 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 and 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**           | 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 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. |

### External Benchmarking

Many organizations wish to compare their privacy program with the privacy program of a similar organization, 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 Accountability Baselineoing and Benchmarking Methodology, can be compared.

° Note that in order to answer the questions effectively, benchmarking would need to be carried out across the Privacy Management Activity 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.
Introducing Nymity Benchmarks

Nymity Benchmarks™ is a subscription-based software tool built for the privacy office based on the above methodology. Nymity Benchmarks is the only tool in the world that allows an organization to compare its privacy program and gain insight into what other organizations are doing, based on privacy management activities. Nymity Benchmarks enables the privacy office to baseline its organization’s privacy management, thereby allowing a statistical comparison. With this tool, the privacy office can benchmark over 150 privacy management activities.

Learn more by visiting www.nymity.com/benchmarks

---

6 Nymity Benchmarking is a paid subscription product available from Nymity. Contact Nymity for a free demonstration and trial at www.nymity.com/benchmarks
Appendix A: Nymity Privacy Management Accountability Framework™

The Nymity Privacy Management Accountability Framework (“Framework”) is a comprehensive listing of over 150 privacy management activities identified through Nymity’s global data privacy accountability research. The privacy management activities are structured in 13 privacy management processes, and are jurisdiction and industry neutral. Originally designed for demonstrating accountability, the Framework is now also used by organizations for other privacy management purposes:

**Demonstrating Accountability**
Demonstrate that an effective privacy program is in place, or in other words, demonstrate accountability, for:

- **BCR Implementation and Monitoring**
  Save time and resources with this Framework when implementing and monitoring Binding Corporate Rules (BCR) in your organization. Nymity provides additional free resources for organizations wishing to use the Framework for this purpose.

- **Evidencing Safe Harbor**
  Support the Safe Harbor Self-Certification process by using documentation as evidence of meeting Safe Harbor obligations. Nymity provides additional free resources for organizations wishing to use the Framework for this purpose.

- **Audit/Privacy Seal Preparation**
  Prepare for an internal or external assessment, such as a privacy seal - this Framework is effective for assembling the necessary documentation and facilitating more effective collaboration between the auditor and audited.

- **DPA Self-Reporting/Self-Attestation**
  Stand-ready to demonstrate accountability, on-demand, with evidence, to a Data Protection Authority (DPA). Some organizations currently use this Framework to be prepared to show due-diligence in the event of an investigation. Nymity is currently researching the possible role of DPA Self-Attestations.

- **Management Reporting**
  Report privacy management in a meaningful and simple way to senior management, C-Suite and Board level.

**Other Privacy Management Uses**
Organizations have found the Framework to be helpful when:

- **Structuring the Privacy Program**
  Structure your privacy program based on the 13 “Privacy Management Processes”. This process-based approach helps ensure privacy management is implemented not as a project, but on an ongoing process.

- **Baselining and Program Planning**
  Quickly baseline privacy management across your organization by simply removing the Not/Applicable privacy management activities and identifying which of the remaining activities have been implemented, are planned, or are desired.

- **Benchmarking**
  Use the baselining information to compare your program with others using the same structure of 'Not Applicable', 'Desired', 'Planned' or 'Implemented'. For the detailed process, obtain the free baselining and benchmarking paper, Nymity Privacy Accountability Baselining and Benchmarking Methodology at www.nymity.com/whitepapers.

- **Understanding Best Practices**
  Use the framework as a comprehensive, up-to-date, listing of privacy management activities. Gain insight into how other organizations are implementing activities to enhance privacy management and to demonstrate accountability.

A free demonstrating accountability toolkit, including a free spreadsheet, book, training videos, and other resources, is available at www.scorecard.nymity.com.
13 Privacy Management Processes

The privacy management activities in the Framework are categorized into 13 Privacy Management Processes which are:

1. **Maintain Governance Structure**
   Ensure that there are individuals responsible for data privacy, accountable management, and management reporting procedures.

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.

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

4. **Embed Data Privacy Into Operations**
   Maintain Operational policies and procedures consistent with the data privacy policy, legal requirements, and operational risk management objectives.

5. **Maintain Training and Awareness Program**
   Provide ongoing training and awareness to promote compliance with the data privacy policy and to mitigate operational risks.

6. **Manage Information Security Risk**
   Maintain an information security program based on legal requirements and ongoing risk assessments.

7. **Manage Third-Party Risk**
   Contracts and agreements with third-parties and affiliates are maintained to be consistent with the data privacy policy, legal requirements, and operational risk tolerance.

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

9. **Maintain Procedures for Inquiries and Complaints**
   Maintain effective procedures for interactions with individuals about their personal data.

10. **Monitor for New Operational Practices**
    Monitor Organizations practices to identify new processes or material changes to existing processes and ensure the implementation of Privacy by Design principles.

11. **Monitor for Data Privacy Breaches**
    Maintain an effective data privacy incident and breach management program.

12. **Monitor Data Handling Practices**
    Verify Operational practices comply with the data privacy policy and operational policies and procedures.

13. **Track External Criteria**
    Tracks new compliance requirements, expectations, and best practices.
Worksheet Template for Baselining Privacy Management/Accountability

The Privacy Management Accountability Framework worksheet template has been formatted to enable an organization to baseline a privacy program, in other words, to baseline accountability. To “baseline” means documenting the status of privacy management. An in-depth understanding for baselining organization privacy management is described above. To summarize, determine baseline status for each privacy management activity by selecting one of the following statuses:

1. Not Applicable (N/A): The advantage of using the Framework for baselining is that you can be confident that you have a comprehensive list of Activities regardless of your location or business environment in which you operate. As it is a comprehensive Framework, it is likely that many, in some cases most, of the Activities are selected as Not Applicable, which is expected.

2. Desired: When benchmarking, the privacy office may discover new Activities they had not previously considered or they may identify Activities that would be beneficial to the organization but are not currently planned.

3. Planned: Privacy management activity is planned in the next 12 months.

4. Implemented: Privacy management activity is in place, select status of either Core or Elective:

<table>
<thead>
<tr>
<th>Core</th>
<th>Elective</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>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 Elective, 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.</td>
</tr>
</tbody>
</table>

Benchmarks Template is available in MS Word and MS Excel worksheet format at www.scorecard.nymity.com

Ongoing Research

Nymity is a research company and, as such, continuously updates 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 request new privacy management activities related to effective privacy program management please submit them to Nymity at research@nymity.com. Nymity Research will review the privacy management activity and respond to your request.
This section lists the privacy management activities, as of April 2014. An up-to-date version is available in Appendix A in The Privacy Office Guide to Demonstrating Accountability, as well as other resources at www.nymity.com/demonstratingaccountability.
Appendix B: 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 Methodology 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, this illustrates how an organization may implement the privacy management activity:

<table>
<thead>
<tr>
<th>Privacy Management Process 5 – Maintain Training and Awareness Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity: Measure participation in data privacy training activities</td>
</tr>
</tbody>
</table>

**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
### 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, 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 according to 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

### Introducing Nymity Templates

Nymity Templates™ is a subscription-based software tool built for the privacy office based on the above methodology for the privacy office. Nymity Templates include hundreds of policies and procedures with annotations, checklists, guides, real-world examples, and expert instructions written and maintained by former chief privacy officers and Nymity Research. All resources are downloadable and ready to use, resulting in comprehensive how-to-guides for privacy management.

Nymity Templates are designed as guidance for the Privacy Office in implementing over 150 privacy management activities within a privacy program.

Nymity Templates are comprehensive guides that save time and enable the privacy office to confidently implement an effective privacy program – and reduce risk by getting it done right the first time.

---

7 Nymity Templates is a paid subscription product available from Nymity. Contact Nymity for a free demonstration and trial at [www.nymity.com/templates](http://www.nymity.com/templates).
Learn more by visiting [www.nymity.com/templates](http://www.nymity.com/templates).

**About Nymity**

Nymity is a global research company specializing in compliance tools for the privacy office. Established in 2002, Nymity is 100% dedicated to data privacy compliance and effective privacy management. Nymity empowers organizations to comply with confidence.

**Compliance Needs of the Privacy Office**

At Nymity, we appreciate that the roles and responsibilities of the privacy office within any organization are dynamic and challenging. Our research indicates that organizations create a privacy office for a number of reasons including laws and regulations, enforcement actions, data breach, competitive differentiation, and corporate culture. Regardless of where the privacy office resides within an organizational structure, the industry or jurisdiction, our research confirms that the roles and responsibilities of the privacy office are universal, and include:

- Advising Stakeholders – liaising with operational units to ensure compliant practices and responsible personal data processing;
- Maintaining the Privacy Program – maintaining a governance structure, policies, procedures, notices, training and awareness, data security, vendor management, breach response protocol, and much more;
- Responding to Data Breaches – leading the team through privacy incident and breach responses;
- Responding to Inquiries and Complaints – handling interactions with customers, employees, law enforcement authorities, and regulators; and
- Professional Development – increasing the knowledge and skills of the individuals in the privacy office.

**How Nymity Supports the Privacy Office**

Nymity has an established history of supporting the privacy office through its innovative research tool, Privaworks™. PrivaWorks is complemented by the following subscription-based software tools:

<table>
<thead>
<tr>
<th>Research Tools</th>
<th>Description</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nymity References™</td>
<td>Library of analyzed compliance research.</td>
<td>Quickly understand compliance obligations and best-practices.</td>
</tr>
<tr>
<td>Nymity LawReports™</td>
<td>Rule maps, charts, and tables.</td>
<td>Quickly report on rules of law based on specific needs.</td>
</tr>
<tr>
<td>Nymity MofoNotes™</td>
<td>Summary analysis of laws.</td>
<td>Understand obligations without reading the laws.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management Tools</th>
<th>Description</th>
<th>Benefits</th>
</tr>
</thead>
</table>
Nymity Research
As a global research company specializing in compliance software tools for the privacy office, Nymity approaches data privacy compliance scientifically. Nymity’s research team of privacy lawyers, privacy analysts, and former chief privacy officers continually creates innovative methodologies and frameworks, which serve as the foundation for Nymity’s compliance tools. Nymity’s research team encapsulates its structured, systematic analysis into Nymity’s compliance tools through continuous research and delivery of relevant content. As a complementary service, some of Nymity’s research is made available for free to the global privacy community.

Nymity Frameworks and Methodologies
Nymity’s frameworks and methodologies are available for free to support privacy management in organizations of any size, sector/industry, or in any jurisdiction. The primary audience for these documents is the organization’s privacy office and thus, some knowledge of privacy management and compliance is beneficial.

<table>
<thead>
<tr>
<th>Free Privacy Papers, Books, and Toolkits</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demonstrating accountability is more than reporting, even more than reporting with evidence. It is the ability to show that a privacy program is managed and monitored.</td>
<td></td>
</tr>
</tbody>
</table>

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 be able to demonstrate it. This book is a guide for the privacy office to demonstrate accountability using the free framework - Nymity Data Privacy Accountability Scorecard™ - available in the free Demonstrating Accountability Toolkit.

Free Download
<table>
<thead>
<tr>
<th>Free Privacy Papers, Books, and Toolkits</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Management Accountability Framework™ White Paper&lt;br&gt;Free Download</td>
<td>This paper provides an in-depth understanding of a methodology for baselining privacy management/accountability in any organization regardless of size, sector/industry, jurisdiction, or maturity of the privacy program. It also enables organizations to compare privacy management with others using this methodology. This paper includes all necessary tools to baseline and benchmark privacy management for free as well as provides an understanding of the underlying methodology for the software tool, Nymity Benchmarks™.</td>
</tr>
<tr>
<td>Privacy Accountability Baselining and Benchmarking Methodology™ White Paper&lt;br&gt;Free Download</td>
<td>This privacy framework is a comprehensive, jurisdiction- and industry-neutral listing of 150+ Privacy Management Activities within 13 Privacy Management Processes. The framework is structurally aligned with how privacy programs are maintained, and can be tailored to fit the unique circumstances of any organization. The Privacy Management Accountability Framework was originally developed for communicating the status of the privacy program, or in other words, for demonstrating accountability. The Framework is also being used by organizations for: baselining and planning the privacy program; structuring the privacy program; benchmarking; BCR implementation and monitoring; Safe Harbor self-attestations; audit preparation; and regulatory self-regulation/self-attestations.</td>
</tr>
<tr>
<td>Privacy Reference Analysis Methodology™ White Paper&lt;br&gt;Free Download</td>
<td>This white paper provides an in-depth understanding of the Nymity research methodology for analyzing privacy compliance documents such as regulatory authority documents, case law, and best-practices documents. The paper provides readers a proven process to analyze compliance documents and gain insight into the underpinnings of Nymity References™ and PrivaWorks™.</td>
</tr>
<tr>
<td>Privacy Rules Categorization Methodology™ White Paper&lt;br&gt;Free Download</td>
<td>This white paper provides an in-depth understanding of the Nymity research methodology for analyzing privacy laws, regulations, codes, and standards. The paper provides readers a proven process to analyze privacy laws plus gain insight into the underpinnings of Nymity LawReports™ and PrivaWorks™.</td>
</tr>
<tr>
<td>Privacy Compliance Attestation Methodology™</td>
<td>This white paper provides an in-depth understanding of a pragmatic methodology for attesting compliance to privacy laws, regulations, codes, and standards,</td>
</tr>
<tr>
<td>Free Privacy Papers, Books, and Toolkits</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>White Paper</td>
<td>providing readers with a proven approach to demonstrate compliance with evidence. The paper also provides insight into the underpinnings of Nymity’s software tool, Attestor™.</td>
</tr>
<tr>
<td>Privacy Risk Reporting Methodology™ White Paper</td>
<td>This white paper provides an in-depth understanding of a methodology for measuring external privacy risk and contextualizing it to internal organizational risk factors to produce relevant maps, charts, and tables; in addition, the paper provides insight into the underpinnings of Nymity RiskMaps™.</td>
</tr>
</tbody>
</table>

Deeply Rooted in Data Privacy Compliance
Through partnership with leading organizations including IAPP, CIPL, FPF, Ponemon Institute, the Information Accountability Foundation, USCIB, ICC, and LexisNexis, Nymity has an established foundation in data privacy. Through deep involvement in the privacy community, Nymity ensures that it remains at the forefront of research.

Award-Winning, Innovative Approach to Data Privacy Compliance
Nymity has an established history of innovating compliance – our customers over the past twelve years can attest to this. Renowned for its unique approach to compliance, Nymity delivers relevant, analyzed research via innovative technology. In 2011, Nymity was recognized as a Gartner Cool Vendor in Risk Management, Privacy & Compliance. In 2012, Nymity was selected as a Global Hot 100 Company by the World Summit on Innovation and Entrepreneurship for its innovative research methodology.

Innovating compliance is at the very core of Nymity. For more information, visit www.nymity.com.