Nymity Demonstrating Compliance Manual: A Structured Approach to Privacy Management Accountability
# Table of Contents

Introduction .................................................................................................................................................. 3  
Section 1: Demonstrating Compliance ........................................................................................................ 4  
Drivers for Demonstrating Compliance ........................................................................................................ 4  
Objectives for Demonstrating Compliance .................................................................................................... 5  
Accountability Approach to Demonstrating Compliance .................................................................................. 5  
How to Demonstrate Compliance using the Accountability Approach .......................................................... 7  
Section 2: Demonstrate Accountability and Compliance .................................................................................. 11  
Section 3 Accountability Scorecard Configuration Guide ............................................................................... 14  
Scorecard Structure ....................................................................................................................................... 14  
Identify and Categorize Privacy Management Activities .................................................................................. 14  
Configure the Evidence Worksheet .................................................................................................................... 16  
Collect Evidence from Owners ........................................................................................................................... 17  
Automatically Calculated Data Privacy Accountability Score ........................................................................ 18  
Ongoing Scorecard Management ....................................................................................................................... 19  
Appendix A: Fundamentals of Structured Privacy Management ...................................................................... 20
To demonstrate data privacy compliance is to show that the organization has the capacity to comply with requirements of a law, regulation, policy, or other commitment such as a privacy notice or code of conduct ("Rule Source"). This manual will introduce the Nymity accountability approach to demonstrating a compliance infrastructure, in other words, the organization’s capacity to comply, and provides detailed instructions for how to implement this approach. Demonstrating a compliance infrastructure through an accountability approach goes a step further than simply showing that compliance requirements have been met; it enables the organization to demonstrate how the requirements are met. It also shows that there is structured privacy management in place to enable ongoing compliance. In other words, that privacy compliance is a proactive and strategic outcome as opposed to an exercise in “checking boxes”.

For several years, Nymity has conducted formal research and observed privacy management programs in organizations across the world, of various sizes, and in every sector. Much of our research on privacy management has focused on measuring and reporting on the status of data privacy accountability and compliance. We have spoken with privacy officers, policy makers and regulators to identify the critical success factors for demonstrating compliance. A key outcome of this research is that among several approaches, the most effective, structured, and scalable approach is for the privacy office to use an accountability approach to demonstrate compliance.

Demonstrating privacy compliance is most effective when it is a dialogue rather than a binary statement of “compliant” or “non-compliant”. This is because unlike many types of compliance, privacy requires a contextual understanding. There is no simple answer. Effective privacy management relies on the interpretation of requirements, an assessment of risk, and other subjective factors. That isn’t to say there is no right answer; there is. However, providing it requires a dialogue about context. Nymity’s research has found that the best way to demonstrate compliance is for the privacy officer to articulate the subjective and objective factors influencing decisions and outcomes. The privacy officer is in the best position to understand, and be able to articulate, compliance in the context of:

- the rules of privacy law;
- the organization’s business and data processing practices;
- how privacy management is embedded throughout the organization; and
- the risk of harm to individuals and the organization.

This manual details how a privacy office can demonstrate compliance by contextualizing Evidence to Rules. It also provides guidance for effectively demonstrating a compliance infrastructure that results in Evidence and reporting quantitative metrics using a Microsoft Excel® spreadsheet called the Nymity Data Privacy Accountability Scorecard™.
Drivers for Demonstrating Compliance

Modern privacy laws and regulatory schemes require the demonstration of compliance to the Rules⁴ and it is expected that this trend will continue as the global regulatory landscape becomes increasingly aligned. There are a number of drivers for organizations to demonstrate compliance including:

1. **EU General Data Protection Regulation⁵**
   
   Demonstrating compliance appears multiple times in the EU Regulation:

   **Article 5: Principles relating to personal data processing**
   
   Paragraph 1 outlines the data privacy principles which the processing of personal data must adhere to: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. Paragraph 2 states that "the controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ("accountability")."

   **Article 24: Responsibility of the Controller**
   
   "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."

   The GDPR will be applicable from 25 May 2018, at which time organizations operating in Europe, or processing the personal data of European citizens, will be required to comply with the Regulation.

2. **Cross Border Data Transfer Mechanisms**
   
   Where the transfer of personal data across borders is restricted by law or regulation, organizations have a number of options for transferring the data. As transfers become more complex, many companies opt to enroll in voluntary schemes such as Binding Corporate Rules (BCR), APEC Cross Border Privacy Rules (CBPR), and the EU-US Privacy Shield. These programs require that the organization commit to processing personal data in accordance with requirements of the transferring country or jurisdiction, even when transferring to countries with less restrictive or no legal requirements. The programs vary on acceptable methods for demonstrating compliance but in all cases the organization must be able to show it is adhering to the commitments.

3. **Self-Regulatory Codes**
   
   Self-regulation systems (e.g. European Advertising Standards Alliance (EASA), Children’s Advertising review Unit (CARU) in the U.S.) set voluntary rules and standards of practice that go beyond legal obligations. Self-regulatory organizations (“SROs”) are responsible for enforcing industry’s commitment to these rules. In response to complaints from individuals respecting an organization’s non-compliance with commitments the organization made in relation to a Code, the organization must demonstrate compliance with the Code or be subject to sanction mechanisms.

4. **Enforcement Action**

---

⁴ Rules: Requirements of a law, regulation, policy, enforcement actions, or other commitments such as a privacy notice or code of conduct.
Regulatory investigation may result in consent orders or settlements that require the organization to comply with a number of remediating measures. The organization may be required to demonstrate compliance with the terms of the order or settlement through regular third-party or regulatory audits.

5. Meeting regulator expectations
As noted above, some privacy laws are evolving to require demonstrating compliance. In some cases, the law hasn’t changed but the regulator has published guidance and made it clear that they expect organizations to be prepared to demonstrate compliance. Regulators in Canada, Hong Kong, Colombia, and Australia have published guidance⁶ to that effect. Responsible organizations treat this guidance as a requirement, knowing that failure to do so may result in negative consequences.

As personal data becomes further embedded in all aspects of business operations, organizations are receiving attention from other regulators such as financial services and telecommunications authorities, as well as labour unions and works councils. Privacy officers now need to be able to demonstrate how their use of personal data not only complies with privacy law but also complies with related legislation as well.

Objectives for Demonstrating Compliance
This manual provides step by step instructions for demonstrating compliance based on a accountability approach. The objective of using the accountability approach is that the privacy office can answer the question: how does the organization comply with the requirements of a privacy law, regulation, policy, or other commitment such as a privacy notice or code of conduct? Note the subtle difference between “how does the organization comply” and “is the organization compliant with the requirements?” The former is a broader, open ended question about the compliance infrastructure of the privacy program (accountability), and the latter is a yes/no question about the current status.

Given the dynamic nature of business, technology, and law, it is not practical to approach privacy management with the goal of reporting on the definitive status of compliance at a point in time. Even traditional methods such as audits and assessments do not seek to determine the definitive state of compliance across the entire organization. Audits and assessments review a representative sample of past events, and a third party draws conclusions about the likelihood of compliance given the results within the sample. This type of monitoring is one component of the accountability approach (Privacy Management Category #12: Monitor Data Handling Practices), and when combined with the other twelve categories it provides a more comprehensive picture of ongoing privacy management.

Accountability Approach to Demonstrating Compliance
Demonstrating compliance through an accountability approach goes a step further than simply showing that compliance requirements have been met, it enables the organization to demonstrate how the requirements are met, and it shows that there is structured privacy management in place to enable ongoing compliance. It also enables the demonstration of a compliance infrastructure and the organization’s capacity to comply. In other words, that compliance is a proactive and strategic outcome as opposed to an exercise in “checking boxes”.

Data privacy accountability is embedded throughout an organization when there are three components present⁷:

- **Responsibility:** the appropriate privacy management activities⁸ have been implemented and are maintained on an ongoing basis. The appropriate privacy management activities are determined based on the organization’s

---

Canada, Getting Accountability Right with a Privacy Management Program https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf
Colombia, Guidelines for the Accountability Principle Implementation http://www.sic.gov.co/drupal/recursos_user/documentos/noticias/Guia_Accountability.pdf
⁷ For further discussion on the components of accountability, please refer to Appendix A: Fundamentals of Structured Privacy Management.
⁸ Nymity considers privacy management activities are ongoing procedures, policies, measures, mechanisms, and other initiatives that impact the processing of personal data or that relate to compliance with privacy and data protection laws.
compliance requirements, risk profile, business objectives, and the context of data processing (type of data processed, nature of processing, purpose for collection, use and disclosure, etc.).

- **Ownership**: the privacy management activities are embedded throughout the organization. In most cases, the privacy office processes very little, if any, personal data. As such, for privacy management to be effective it has to be implemented within each function or business unit that processes personal data.

- **Evidence**: when privacy management activities are being maintained, documentation is produced. That documentation can be used as Evidence of accountability and compliance. Evidence can be formal (e.g. policies, procedures) or informal (e.g. communications, workflows). When using an accountability approach, Evidence is always a by-product of a privacy management activity, i.e. Evidence is not produced for the sake of documentation, but as a result of an activity.

The following examples illustrate the difference between an accountability approach and a traditional compliance approach:

**Example: Data Breach**

Many jurisdictions now require that organizations report to regulators and notify data subjects in the event of a breach. In order to comply with breach laws, a breach must have occurred (otherwise it is not possible to report or notify). Technically, an organization can be compliant if they wait until they become aware of a breach and then react accordingly.

However, most organizations understand the risk and impact of a breach and therefore accountable. They implement privacy management activities such as data breach response plans, test the plans, engage breach response providers, and implement other activities. They maintain these activities even in the absence of a breach having occurred. They also train employees on how to identify breaches, and maintain metrics of breaches and the risks/root causes in order to identify patterns and trends which may indicate a broader issue. The accountable organization is better prepared to effectively deal with the breach and minimize impact to data subjects and the organization. For example, an accountable approach to data breach management may include:

- Responsibility/Ownership: The privacy office establishes breach response plans, tests the plan, provides employee training, records metrics, and helps to manage the process for reporting and notification. Operational units identify and escalate breaches in accordance with the plan, and assist with response and remediation.
- Evidence: data privacy breach response plan, records of testing the plan, data breach logs, data breach reports, data breach metrics, evidence of reporting/notification

**Example: Data Retention**

Most privacy frameworks contain the requirement that personal data should be retained only as long as appropriate based on the purpose for which it was collected. A relatively young organization can easily comply with this requirement. For example, if the organization has only been collecting personal data for two years, they can justify retaining the data for that amount of time for most purposes.

---

9 Nymity Benchmark statistics for "Maintain a data privacy incident/breach response plan" as of July 22nd, 2016 is 55% Implemented, 25% In-Progress, 19% Desired and 1% Not Applicable.

10 Nymity Benchmark statistics for "Conduct periodic testing of data privacy incident/breach plan" as of July 22nd, 2016 is 26% Implemented, 20% In-Progress, 45% Desired and 9% Not Applicable.

11 Nymity Benchmark statistics for "Engage a breach response remediation provider" as of July 22nd, 2016 is 34% Implemented, 7% In-Progress, 23% Desired and 36% Not Applicable.

12 Nymity Benchmark statistics for "Conduct privacy training" as of July 22nd, 2016 is 60% Implemented, 27% In-Progress, 13% Desired and 0% Not Applicable.

13 Nymity Benchmark statistics for "Maintain a log to track data privacy incidents/breaches" as of July 22nd, 2016 is 53% Implemented, 17% In-Progress, 27% Desired and 3% Not Applicable.
An accountable organization, however, maintains policies, procedures, and mechanisms to proactively manage data retention schedules\(^ {14} \). This helps them to comply on an ongoing basis, as well as rationalize their decisions for when to retain or destroy data\(^ {15} \). It makes them accountable. For example, an accountable approach to data breach management may include:

- **Responsibility/Ownership**: The privacy office analyzes the requirements of privacy laws and regulations, understands the purpose for which personal data was collected as well as related retention requirements such as employment, financial/tax, or others, and provides input into retention schedules which are likely managed by system/data owners. Operational units execute the schedule by configuring systems to archive/delete data based on its classification, or manually manage records by securely destroying them based on the schedule.

- **Evidence**: privacy policies, data classification procedures, data retention schedule, evidence of system configuration, and archive schedule

The data breach and data retention examples above illustrate the relationship between accountability strategy and traditional approach to privacy management and compliance. The examples show that implementing structured privacy management is a strategic approach and is the best way to enable ongoing compliance.

**How to Demonstrate Compliance using the Accountability Approach**

**Step 1: Demonstrate Accountability by Gathering Evidence of Ongoing Privacy Management Activities**

**Responsibility** (maintaining the appropriate privacy management activities) and **Ownership** (embedding privacy management activities throughout the organization) are components of structured privacy management. When these two components are in place, **Evidence** is produced as a by-product of maintaining privacy management activities, and the privacy office has everything it needs to demonstrate accountability and then go a step further to demonstrate compliance.

The privacy office demonstrates accountability by gathering Evidence of ongoing privacy management activities and it demonstrates compliance by contextualizing the Evidence to Requirements (requirements of a law, regulation, policy, or other commitments such as a privacy notice or code of conduct).

The privacy office can use the **Evidence Worksheet**\(^ {16} \) to streamline the process of gathering Evidence from the privacy management activity Owners throughout the organization.

Please refer to **Section 3: Accountability Scorecard Configuration Guide** for details on how to use the Evidence Worksheet and the Nymity Data Privacy Accountability Scorecard™ which is automatically generated when the Evidence Worksheet is complete and can be used to report the status of privacy management.

**Step 2: Demonstrating Compliance by Contextualizing Evidence**

Using the Evidence Worksheet, the privacy office has created an index of the documentation needed to demonstrate compliance. The next step is to contextualize the Evidence to requirements.

Data privacy is not simple, it is contextual in nature and sometimes subject to interpretation and judgement. There is no standard checklist that an organization can point to and say “we are compliant”, it depends on a number of factors, i.e. context. In order to articulate how the organization’s data processing activities are carried out in compliance with the Rules (to demonstrate compliance), one must understand the activities themselves, the motivations behind them, how the Rules apply, and a number of other factors. Nymity’s research has shown that privacy officers are uniquely positioned to demonstrate compliance. This is because privacy officers have the expertise to interpret the requirements and the knowledge to understand how they apply to each type of processing, in other words, they understand and can communicate the context of compliance.

\(^ {14} \) Nymity Benchmark statistics for “Integrate data privacy into records retention practices” as of July 22\(^ {nd} \), 2016 is 37% Implemented, 25% In-Progress, 37% Desired, and 1% Not Applicable.

\(^ {15} \) Nymity Benchmark statistics for “Maintain policies/procedures for secure destruction of personal data” as of July 22\(^ {nd} \), 2016 is 55% Implemented, 22% In-Progress, 18% Desired, and 5% Not Applicable.

\(^ {16} \) It is the primary worksheet in a no cost MS Excel spreadsheet called the Nymity Accountability Scorecard, available at [www.nymity.com/pmaf](http://www.nymity.com/pmaf).
Privacy context includes:

1. **Rules**\(^\text{17}\)  
   Organizations in many jurisdictions are required to comply with privacy laws and regulations. In addition, they must often comply with policies or other commitments such as privacy notices or codes of conduct. These sources of requirements are referred to as Rule Sources, and the requirements themselves are referred to as Rules. The privacy officer understands the Rules and therefore can provide context for how they apply to each type of data processing.

2. **Data Processing Practices**  
The privacy officer understands the organization’s practices that involve the processing of personal data, including business operations and back office functions such as human resources, marketing, and finance. Working with stakeholders throughout the organization\(^\text{18}\), the privacy officer can understand and provide context for how the Rules apply to organizational practices.

3. **Privacy Management**  
The privacy officer understands the privacy management activities that have been implemented throughout the organization and how they are maintained. Many decisions related to privacy management are influenced by the Rules and how they apply to data processing and explaining these decisions is a key element of providing context.

4. **Privacy Risk**  
The privacy officer understands the risk of harm to individuals and to the organization\(^\text{19}\). The privacy officer can explain how privacy risk influenced decisions around which privacy management activities to implement and why. Related to privacy risk, another element of context is the decision to prioritize one risk mitigation activity over another when resources are limited.

For some privacy management activities, it is obvious how the Evidence can be used to demonstrate compliance. For example, if a Rule requires that a privacy notice contains certain elements\(^\text{20}\), the privacy notice can be provided and it is easy to determine if the elements are present. The privacy officer would not need to contextualize the Evidence. In other cases, it is not obvious. For example, Rules often require that data is not processed for purposes beyond those for which it was collected. In this case, Evidence may include policies and guidance instructing employees of the requirement. These are easy to map to the Rule, and they are a good start, but they don’t go far enough. They demonstrate that the guidance was issued but not that it is being followed. To demonstrate that privacy is effectively embedded, the privacy office might show that Privacy Impact Assessments (PIAs) are required for all new collection and use of personal data\(^\text{21}\) and that part of the PIA includes identifying the original purpose for collection and determining if this use is consistent. This Evidence likely requires contextualization.

The following example provides a more in depth explanation of how Evidence can be contextualized to answer the question: How does the organization comply with the Rules?

The privacy officer may want to demonstrate how the outbound telemarketing team within a call centre complies with a requirement to obtain consent to collect and use data for the purpose of selling a product. The privacy officer can use existing privacy management documentation (i.e. Evidence) and provide context to demonstrate compliance as follows:

---

\(^{17}\) Rules: Requirements of a law, regulation, policy, or other commitment such as a privacy notice or code of conduct.  
\(^{18}\) Engage stakeholders throughout the organization on data privacy matters (e.g., information security, marketing, etc.) found in 1. Maintain Governance Structure in the Nymity Privacy Management Accountability Framework™.  
\(^{19}\) Conduct an Enterprise Privacy Risk Assessment found in 1. Maintain Governance Structure in the Nymity Privacy Management Accountability Framework™.  
\(^{20}\) "Maintain a data privacy notice that details the organization’s personal data handling practices" found in 8. Maintain Notices in the Nymity Privacy Management Accountability Framework™.  
\(^{21}\) "Maintain a data privacy policy" found in 3. Maintain a data privacy policy in the Nymity Privacy Management Accountability Framework™.
Evidence: Privacy Policy
The data privacy policy\textsuperscript{22} contains a provision which states that the organization must obtain consent for all types of data processing.

Context: Rules, Data Processing, Privacy Management
Having identified the call centre as a point of data collection and use [Data Processing], the privacy office determines that consent is required. The data privacy policy is a privacy management activity which sets the expectation for obtaining consent [Rules, Privacy Management].

Evidence: Data Privacy Training Materials
The general data privacy training curriculum for all employees with access to personal data\textsuperscript{23} contains general guidance for obtaining consent, and the role specific privacy training for call centre employees\textsuperscript{24} contains more specific guidance for when and how to obtain and record consent when collecting data.

Context: Privacy Management
The privacy office can show that through the use of general and role specific privacy training, the expectation to obtain consent is reinforced and communicated proactively [Privacy Management].

Evidence: Call Centre Scripts
The call centre utilizes scripts for outbound telemarketing which guide the employees on how to obtain explicit consent for processing\textsuperscript{25}.

Context: Rules, Privacy Management
The privacy office can demonstrate that employees are provided with tools to help them comply with the policy [Rules] as the scripts include a statement for explaining the privacy notice and obtaining explicit consent [Privacy Management].

Evidence: CRM Screen Shots
The Customer Relationship Management (CRM) system contains a field where consent and opt-out requests are recorded. Validation mechanisms prevent the user from extracting a record for a purpose for which consent has not been obtained.

Context: Data Processing
Because the privacy officer understands how data is collected and flows throughout the organization [Data Processing], he or she can use the CRM to demonstrate that consent is being collected and managed.

Evidence: Privacy Office Consultation
The Call Centre director reached out to the privacy office via email to inquire about how the organization’s policy around obtaining explicit consent should be applied in a jurisdiction where implied consent is permitted by law. These emails and follow up discussions show how the privacy officer assisted the call centre to address consent requirements.

Context: Rules, Privacy Risk
The privacy office can explain that even though the law does not require explicit consent in all cases [Rules], they have made the decision to obtain it anyway. By simplifying the process and defaulting to the most restrictive requirement, the organization is less likely to be non-compliant [Privacy Risk].

\textsuperscript{22} "Maintain a data privacy policy found" in 3. Maintain Data Privacy Policy in the Nymity Privacy Management Accountability Framework™.
\textsuperscript{23} "Conduct privacy training" found in 5. Maintain Training and Awareness Program in the Nymity Privacy Management Accountability Framework™.
\textsuperscript{24} "Conduct privacy training reflecting job specific content" found in 5. Maintain Training and Awareness Program in the Nymity Privacy Management Accountability Framework™.
\textsuperscript{25} "Integrate data privacy into telemarketing practices" found in 4. Embed Data Privacy into Operational Practices Program in the Nymity Privacy Management Accountability Framework™.
Evidence: Audit Results
An internal audit of call centre operations included listening to a selection of recorded calls to determine if the process for obtaining consent was followed. No exceptions were reported.

Context: Privacy Management, Privacy Risk
Although the internal audit was not conducted by the privacy office, it becomes documentation that can be used as Evidence of privacy accountability and compliance. The report shows that the selected calls followed the requirements in the data privacy policy [Rules]. Because the policy exceeds the requirements of the law [Rules], the privacy office can explain why they determined there is a low risk of non-compliance with legal requirements for consent [Rules].

The privacy office was able to answer the question: how does the organization comply with the Rules around consent? Note that in the above example, the privacy office was able to demonstrate compliance using existing privacy management documentation, no extra documentation was produced. Also note that the documentation alone would not be sufficient to demonstrate compliance to someone who did not understand the Rules that apply to the organization, the way that data is processed, how privacy management is embedded in the organization, or the privacy risk profile. The documentation required the context provided by the privacy officer.
Section 2: Demonstrate Accountability and Compliance

Section 1 described the process for contextualizing Evidence to Rules in order to demonstrate compliance. This section will provide detailed guidance for how the privacy office can demonstrate accountability as a first step toward demonstrating compliance. Demonstrating accountability is showing how responsibility is exercised and making this verifiable.

Organizations across the globe and in all sectors use the Nymity Data Privacy Accountability Scorecard™, to gather Evidence of ongoing privacy management activities from Owners, creating an index of documentation (Evidence Worksheet) and automatically generating metrics on the status of privacy management (Scorecard).

The tool, available either as a free Microsoft Excel® workbook, or a software solution, generates reports which allow the privacy office to answer the following questions:

- “Has our privacy management been designed in compliance with one or more Rules?”
- “Is privacy management effectively implemented and maintained in a specific country or business unit?”
- “Where are the gaps between the current state and the desired state (compliance)?”
- “How does the organization go above and beyond the minimum for compliance, to process data responsibly?”

The tool provides the privacy office with the ability to demonstrate a compliance infrastructure.

While some cases require a dialogue with the privacy office where Evidence is contextualized to Rules, not all audiences desire that level of detail. For example, senior management and the board of directors want to know the status of privacy management. However, they are not likely to be experts in privacy and probably want a simple answer, supported by Evidence and analysis. Since 2009, Nymity has conducted ongoing research on practical approaches for demonstrating accountability. This research has resulted in:

- **Evidence Worksheet**
  A spreadsheet that provides a structured approach for recording privacy management activities, gathering Evidence from Owners, and indexing the location of documentation. In the call centre example above, the Evidence the privacy office used to contextualize privacy management was gathered using the Evidence Worksheet.

- **Accountability Scorecard**
  A visual representation of the status of compliance, automatically generated from a completed Evidence Worksheet.

---

27 Rules: Requirements of a law, regulation, policy, or other commitment such as a privacy notice or code of conduct.

Nymity Demonstrating Compliance Manual:
A Structured Approach to Privacy Management
Copyright© 2016 Nymity Inc.
**Evidence Worksheet**

The Evidence Worksheet enables a streamlined approach for the privacy office to index the documentation that is produced by privacy management activities embedded throughout the organization. Maintaining records of this documentation in a single location enables the privacy office to demonstrate accountability on demand. If the Evidence Worksheet is kept up-to-date, the privacy officer can stand-ready to demonstrate compliance. He or she can maintain a current view of the status, and quickly respond to questions about how the organization complies with Rules.

**Automatic Visualization – Accountability Scorecard**

Completing the Evidence Worksheet automatically generates a chart that enables simple and high level demonstrations of accountability. As the privacy officer updates the Evidence Worksheet, the Accountability Scorecard is automatically generated featuring:

1. **Privacy Management Status Line (Blue Line)**
   The status of privacy management at any given time. The Scorecard shows the history of privacy management over time, enabling the privacy office to tell the story of the evolving privacy management.

2. **Compliance Line (Green Line)**
   The minimum level to demonstrate compliance, in other words, the point when all the Mandatory privacy management activities for compliance are evidenced with up-to-date documentation. This is explained in detail in Section 3, Accountability Scorecard Configuration Guide.

3. **% Managed**
   Located below the Compliance Line (Green line) is the percentage of Mandatory privacy management activities that are evidenced. If the status is 100% managed, the privacy officer can demonstrate compliance.

   A score below 100% Managed does not necessarily indicate that an organization is non compliant. It may mean that they have not yet obtained Evidence to demonstrate their compliance infrastructure.

4. **% Advanced**
   Located above the Compliance Line (Green Line) is the percentage of privacy management activities that go beyond compliance and thus, are Advanced. As detailed later, these are called Additional privacy management activities.

---

29 Mandatory privacy management activities are defined by the privacy office and are typically the required privacy management activities to achieve ongoing compliance to one or more Rule sources, for example, a privacy law.

30 Advanced privacy management activities are defined by the privacy office and are the activities that go beyond the strict letter of the law, in other words, are not mandatory by law.
activities that are implemented not because they are Mandatory, but because they’re part of the privacy office’s goal to go above and beyond.

Benefits of using the Evidence Worksheet and the resulting Accountability Scorecard
The privacy office can demonstrate accountability by simply providing Evidence of privacy management activities. However, by using the Evidence Worksheet and the resulting Accountability Scorecard, the following benefits are realized:

1. **Effective communication**
   The Accountability Scorecard allows the privacy officer to tell the story of privacy management including the past and present, supported by Evidence. The simple nature of the Accountability Scorecard enables the privacy officer to effectively communicate the status with context, even to audiences that don’t have a deep understanding of privacy. They can explain that the goal is to reach the Compliance Line – if the status is below that line (% Managed) there are gaps, and if it is above the line (% Advanced) then privacy management is above the minimum required to demonstrate compliance. The Scorecard provides the privacy officer the ability to demonstrate a compliance infrastructure and the organization’s capacity to comply.

2. **Supported by existing documentation**
   The Evidence Worksheet enables the privacy officer to keep a record of documentation that is produced by privacy management activities. Having a centralized index streamlines the process for contextualizing Evidence when demonstrating compliance and the privacy office can more quickly access the documentation if necessary when responding to questions. As noted in Appendix A: Fundamentals of Structured Privacy Management, documentation is not created merely for the sake of demonstrating compliance, it is produced as a by-product of ongoing privacy management activities that are embedded throughout the organization.

3. **Flexible and scalable**
   The Evidence Worksheet and Accountability Scorecard will work for organizations of any size, in any jurisdiction, and for all types of data processing. Some organizations use multiple Evidence Worksheets, creating Accountability Scorecards for different parts of the organization, for example, by country, or by business unit.
Section 3: Accountability Scorecard Configuration Guide

This section provides the instruction to configure and use the Evidence Worksheet that automatically generates the Accountability Scorecard.

Scorecard Structure

Effective privacy management requires that privacy management activities are embedded throughout the organization – not just at the privacy office level. For this reason, most organizations eventually choose to implement multiple Scorecards in order to streamline the process for collecting Evidence and generating more specific metrics to help pinpoint strengths and weaknesses.

There are a few possibilities for structuring a multiple Scorecard approach. Based on Nymity’s experience with a number of successful Scorecard implementations, the best approach is often a hybrid of the following deployment approaches:

- **Functional/Use Based** (e.g. Marketing, Human Resources, Business Unit): deploying a Scorecard for each operational unit is recommended for organizations where the nature of personal data processing varies across the organization. For example, in financial services organizations, the same personal data (Customer information) may be used for delivering services as well as marketing. Setting up a Scorecard for both the business and the marketing department is a good way to get a whole picture.

- **Geography Based**: in organizations where personal data processing is relatively consistent across functions, it may be appropriate to create Scorecards for each jurisdiction or region. This is often the case when the primary use of personal data is for human resources. Deploying a Scorecard for each region makes it easy to customize based on local requirements, and to compare the status from one region to the next.

Most organizations deploy the Scorecard to measure, monitor, and report on the activities of the privacy office, as a ‘proof of concept’ before adding multiple Scorecards and rolling it out into the entire organization.

When using multiple Scorecards, conduct the following steps for each one. A Scorecard can have its own set of privacy management activities, Evidence Collection Questions, Responses, and Evidence.

Identify and Categorize Privacy Management Activities

The first step toward measuring privacy management is to identify the relevant privacy management activities. This can be done in a few different ways, either by focusing on one or more compliance rule sources, or by building on the privacy management baseline exercise outlined in “A Structured Approach to Privacy Management: Getting Started Manual” found at [https://www.nymity.com/data-privacy-resources/getting-started.aspx](https://www.nymity.com/data-privacy-resources/getting-started.aspx).

Identify Privacy Management Activities based on a Compliance Approach

To demonstrate data privacy compliance is to show that the organization complies with requirements of a Rule: a law, regulation, policy, or other commitments such as a privacy notice or code of conduct. A simple way to get started is to identify privacy management activities that are required by the Rules. To do this:

1. Read the Rule Source, for example, a privacy law, and identify the Rules that require Evidence to demonstrate compliance. Within a Rule Source, there are many Rules which do not require Evidence. For example, definitions, exceptions, commissioner’s powers, fines, etc. In the GDPR there are 99 Articles but only 39 of these Article require
2. For each Rule that requires Evidence, identify the privacy management activities that produce the Evidence. In other words, the privacy management activities that will help enable ongoing compliance with that Rule.

The Structured Approach to Privacy Management: Getting Started Manual provides a Compliance Strategy which is based on the same steps: identifying Rules which require Evidence and implementing privacy management activities that will produce the required Evidence. Appendix C: Getting Started with a Compliance Strategy contains examples of privacy management activities commonly implemented to satisfy the requirements for various Rule Sources such as the EU General Data Protection Regulation, Binding Corporate Rules, APEC Cross Border Privacy Rules, and others.

Identify Privacy Management Activities based on the Privacy Management Baseline

The Compliance Approach described above identifies privacy management activities based on the Rules. Another approach is to identify privacy management activities based on what is currently in place within the organization, known as a baseline.

Baselining privacy management is a second approach to identifying the privacy management activities for demonstrating compliance. Baselining privacy management is identifying the current status of privacy management activities, and can be done using the free MS Excel Workbook Privacy Management Workbook ("Workbook") provided by Nymity. The Workbook contains the privacy management activities found in the Nymity Privacy Management Accountability Framework™.

To baseline existing privacy management, identify which privacy management activities are Implemented, In Progress, Desired, and Not Applicable.

- **Implemented**: Privacy management activities that are already in place and have sufficient resources to be maintained are categorized as "Implemented".

- **In Progress**: If the privacy management activity is in progress of being implemented, or is scheduled to be implemented, it is categorized as "In Progress".

- **Desired**: Privacy management activities that are determined to be applicable or relevant for privacy management, but are not currently “Implemented” or resourced to be implemented are categorized as “In Progress”.

- **Not Applicable (N/A)**: Privacy management activities that are not applicable to the organization (or the part of the organization being assessed) are categorized as "N/A".

Many of the privacy management activities will apply to multiple Scorecards, and may have a different status in each one. Baselining privacy management is described in detail in Structured Approach to Privacy Management: Getting Started Manual.

Categorize Privacy Management Activities

The previous section described two approaches for identifying privacy management activities. If you select the baseline approach, the activities and current status will be recorded in the Nymity Privacy Management Workbook. If you select the compliance approach, you may wish to record them in a separate spreadsheet.

All privacy management activities must be categorized as Mandatory or Additional:

- **Mandatory**
  - Privacy management activities that must be implemented in order for the organization to comply with the
Rules. Typically, the privacy officer chooses one or more Rules to start with, and identifies the Mandatory privacy management activities necessary to achieve ongoing compliance.

- **Additional**
  Most organizations go above and beyond the minimum for compliance, implementing privacy management activities that are not Mandatory but do contribute to the responsible processing of personal data. These privacy management activities are categorized as Additional. Examples include:
  - Maintain privacy awareness materials\(^{31}\)
  - Monitor and report metrics for data privacy complaints (e.g. number, root cause) \(^{32}\)
  - Obtain data privacy breach insurance coverage\(^{33}\)

Configure the Evidence Worksheet

Once the Scorecard structure has been determined and the privacy management activities identified, the Evidence Worksheet is ready to be set up.

Create Evidence Collection Questions

For each privacy management activity, the privacy officer 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. The question has to have a yes or no answer as it is necessary for the automatic generation of the Accountability Scorecard.

**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 the privacy office, privacy network and others responsible/accountable for data privacy” it is better to be specific. For example, “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.

Record the Evidence Collection Questions in column B of the Evidence Worksheet. Questions corresponding to Mandatory privacy management activities go in the top section (starting with cell B8) and Additional privacy management activities go in the bottom section (starting with cell B60).

---

\(^{31}\) “Maintain privacy awareness materials (e.g. posters and videos)” found in 5. Maintain Training and Awareness Program in the Nymity Privacy Management Accountability Framework™.

\(^{32}\) “Monitor and report metrics for data privacy complaints (e.g. number, root cause) found in 9. Respond to Requests and Complaints from Individuals in the Nymity Privacy Management Accountability Framework™.

\(^{33}\) “Obtain data privacy breach insurance coverage” found in 11. Maintain Data Privacy Breach Management Program in the Nymity Privacy Management Accountability Framework™.
Assign Owners
As discussed in detail in Appendix A: Fundamentals Structured Privacy Management, the Owner may be the privacy office or an individual or individuals in the operational or business unit. Note that the Owner does not necessarily complete the privacy management activity, but is ultimately responsible or answerable for it.

Record the Owner for each activity in column C.

Determine Frequency
For each Privacy Management Activity, a Frequency must be defined. As discussed in detail in Appendix A: Structured Privacy Management, all privacy management activities must be performed on an ongoing basis – either periodically or continuously.

For each privacy 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 may be sufficient to provide summary evidence on a monthly or quarterly basis.

Record the Frequency for each activity in Column D.

Collect Evidence from Owners
After the Scorecard is configured 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.

Enter the date of the initial update in cell F3. As you complete the following sections for each Question, the Score will automatically update.

The Response contains two parts: (1) – a ‘yes’ or ‘no’ response to the Evidence Collection Question (column F), and (2) a comment to provide additional context (column G).

Evidence: All ‘yes’ responses require Evidence. The privacy office may log the Evidence in column H via a link to a URL or a description as to where that document can be found.
Automatically Calculated Data Privacy Accountability Score

This section is for information purposes to understand how the graph created the Accountability Scorecard.

The Data Privacy Accountability Score represents the status of privacy management as a percentage of the Mandatory and Additional privacy management activities 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.

\[
\text{% Managed} = \frac{\text{# of Mandatory Activities Evidenced}}{\text{# of Mandatory Activities Identified}}
\]

When all Mandatory activities are evidenced, the privacy management score is considered 100% Managed, and the status has reached the Compliance Line. When Additional Privacy management activities have been implemented and evidenced, privacy management has gone above and beyond the minimum requirements and achieved an Advanced score.

\[
\text{% Advanced} = \frac{\text{# of Additional Activities Evidenced}}{\text{# of Additional Activities Identified}}
\]

<table>
<thead>
<tr>
<th>ID</th>
<th>Question</th>
<th>Owner</th>
<th>Response</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>Is the Data Privacy Policy reviewed based on legislative and operational changes?</td>
<td>Privacy Office</td>
<td>No</td>
<td>The Data Privacy Policy has not been reviewed in the last two years, we plan to do so within the next two months.</td>
</tr>
<tr>
<td>M2</td>
<td>Do the individuals in the privacy office maintain their privacy knowledge?</td>
<td>Privacy Office</td>
<td>Yes</td>
<td>All members of the Privacy Office maintain privacy certifications. Email confirmation from all members of the Privacy Office that their certifications are in good standing.</td>
</tr>
<tr>
<td>M3</td>
<td>Does the Privacy Office track and analyze the impact of new laws, changes in laws, relevant enforcement actions and new regulator expectations?</td>
<td>Privacy Office</td>
<td>Yes</td>
<td>The Privacy Office subscribes to Nymity’s Privacy to track legislative developments. No applicable changes to laws or regulations. Memo between Privacy and Legal regarding legislative developments (none noted).</td>
</tr>
<tr>
<td>M4</td>
<td>Do all third-party contracts contain</td>
<td></td>
<td></td>
<td>Contracts are likely being reviewed as</td>
</tr>
</tbody>
</table>

IMPLEMENTATION NOTE

Configuring the Scorecard (identifying activities, formulating questions, assigning ownership, etc.) requires the expertise of the privacy office familiar with the organization’s privacy management 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% compliance score in one area can be compared “apples to apples” to an 80% compliance score in a completely different jurisdiction or business area.

Until the Compliance line of 100% Managed is reached, the percentage Advanced is depicted as a Potential Score. In other words, Additional Privacy management activities do not affect the Privacy Management Score until all Mandatory Privacy management activities are completed. Even though the Additional Privacy management activities do not affect the overall score, the privacy officer can still account for them and collect Evidence. This allows the privacy officer to gain a holistic view of privacy management.
**Implementation Note**

The Scorecard allows the privacy officer 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 management 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 as they used multiple Scorecards.

**Ongoing Scorecard Management**

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 (e.g., a new activity is evidenced).

After the initial update, the Response (yes/no), Comment, and Evidence will be automatically populated, referring the reader to the previous status.

To update the status – either a scheduled or an interim update – enter a new date in cell K2. Identify any Responses which need to be updated. Responses need to be updated when:

- The answer has changed; for example, the Response was ‘no’ and the activity has now been complete and Evidence is provided
- Frequency has elapsed; for example, the last update was three months ago and the activity has a frequency of Quarterly.

For the questions that require an Update, select “Yes” in the “Update” column to reset the answers and provide new ones. The cell will automatically highlight yellow so it is easy to scan for changes from one update to the next.

The Evidence Worksheet provides for 20 Updates by default. If the Evidence Worksheet is updated quarterly, the Accountability Scorecard will demonstrate compliance for five years.

**Implementation Note**

Automatic

The Accountability Scorecard visualization is updated each time an Update is placed in the Evidence Worksheet.
Appendix A: Fundamentals of Structured Privacy Management

In 2002, Nymity began its research on accountability. In 2012, Nymity enhanced the research with on-the-ground workshops around the world, including privacy and data protection regulators, examining what it takes for organizations to “demonstrate” accountability through effective privacy management. One component of this research resulted in an understanding of structured privacy management that has three key elements: 1. Responsibility, 2. Ownership, and 3. Evidence.

1. Responsibility

**Responsible organizations maintain the right set of privacy management activities.**

Nymity’s research has resulted in the Nymity Privacy Management Accountability Framework™ ("Framework"). It is this Framework that forms the foundation for the “responsibility” element in a structured approach to privacy management.

The Framework is not a checklist of activities that must be completed; rather it is a menu for privacy management that can be adapted to any organization. No two organizations’ privacy management are the same, and thus this Framework provides the flexibility necessary for planning, scaling, and communicating privacy management. The Framework is not based on principles or controls, but on privacy management activities that can be monitored and tracked. It is a comprehensive, jurisdiction- and industry-neutral listing of 130+ privacy management activities within 13 Privacy Management Categories.

In a structured approach to privacy management, responsibility means that appropriate Privacy Management Activities (Activities) have been implemented and are maintained on an ongoing basis. *Privacy Management Activities are ongoing procedures, policies, measures, mechanisms, and other initiatives that impact the processing of personal data or that relate to compliance with privacy and data protection laws.* The appropriate Activities are determined based on the organization’s compliance requirements, risk profile, business objectives, and the context of data processing (type of data processed, nature of processing, purpose for collection, use and disclosure, etc.).

2. Ownership

**An individual is answerable for the management and monitoring of each of the privacy management activities.**

Ownership is the second element of structured privacy management and builds upon the element of responsibility. Even if the privacy office is accountable for data privacy or compliance, the privacy office itself usually processes very little personal data, if any. As such, the effectiveness of privacy management 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 and business units, for example, human resources, marketing, product development, IT, customer service, etc., as that is where the data is being collected and processed.

Privacy management activities may be:

- Maintained by the privacy office, for example:
  - Maintain a data privacy policy
  - Conduct privacy training
  - Maintain a data privacy notice that details the organization’s personal data handling practices
  - Identify ongoing privacy compliance requirements, e.g., law, case law, codes, etc.
- Influenced or Observed by the privacy office, for example:
  - Integrate data privacy into direct marketing practices
  - Integrate data privacy into an information security policy
  - Conduct due diligence around the data privacy and security posture of potential vendors/processors
Table 0.1 provides examples of privacy management activities within each of the 13 Privacy Management Categories which are performed by various stakeholders within the organization.

<table>
<thead>
<tr>
<th>Privacy Management Categories</th>
<th>Activities Owned by the Privacy Office – Examples</th>
<th>Activities Owned by Operational Units – Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Maintain Governance Structure</td>
<td>Maintain a Privacy Strategy</td>
<td>Owner: Human Resources</td>
</tr>
<tr>
<td></td>
<td>Require employees to acknowledge and agree to adhere to the data privacy policies</td>
<td></td>
</tr>
<tr>
<td>2. Maintain Personal Data Inventory</td>
<td>Maintain an inventory of key personal data holdings (what personal data is held and where)</td>
<td>Owner: Corporate Records Management</td>
</tr>
<tr>
<td></td>
<td>Classify personal data holdings by type (e.g. sensitive, confidential, public)</td>
<td></td>
</tr>
<tr>
<td>3. Maintain Data Privacy Policy</td>
<td>Maintain a data privacy policy</td>
<td>Owner: Human Resources</td>
</tr>
<tr>
<td></td>
<td>Maintain an employee data privacy policy</td>
<td></td>
</tr>
<tr>
<td>4. Embed Data Privacy Into Operations</td>
<td>Maintain policies/procedures for collection and use of children and minors’ personal data</td>
<td>Owner: Marketing</td>
</tr>
<tr>
<td></td>
<td>Integrate data privacy into direct marketing practices</td>
<td></td>
</tr>
<tr>
<td>5. Maintain Training and Awareness Program</td>
<td>Conduct privacy training</td>
<td>Owner: Customer Service</td>
</tr>
<tr>
<td></td>
<td>Incorporate data privacy into operational training, such as HR, security, call centre</td>
<td></td>
</tr>
<tr>
<td>6. Manage Information Security Risk</td>
<td>Maintain an acceptable use of information resources policy</td>
<td>Owner: Information Security</td>
</tr>
<tr>
<td></td>
<td>Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)</td>
<td></td>
</tr>
<tr>
<td>7. Manage Third Party Risk</td>
<td>Maintain data privacy requirements for third parties (e.g., clients, vendors, processors, affiliates)</td>
<td>Owner: Legal</td>
</tr>
<tr>
<td></td>
<td>Maintain procedures to execute contracts or agreements with all processors</td>
<td></td>
</tr>
<tr>
<td>8. Maintain Notices</td>
<td>Maintain a data privacy notice that details the organization’s personal data handling practices</td>
<td>Owner: Facilities/Corporate Security</td>
</tr>
<tr>
<td></td>
<td>Provide notice by means of on-location signage, posters</td>
<td></td>
</tr>
<tr>
<td>9. Respond to Requests and Complaints from Individuals</td>
<td>Investigate root causes of data protection complaints</td>
<td>Owner: Call Centre</td>
</tr>
<tr>
<td></td>
<td>Maintain procedures to address complaints</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conduct PIAs/DPIAs for new programs, systems, processes</td>
<td></td>
</tr>
<tr>
<td>11. Maintain Data Privacy Breach Management Program</td>
<td>Maintain a data privacy incident/breach response plan</td>
<td>Owner: Legal:</td>
</tr>
</tbody>
</table>
3. Evidence

**Documentation that is a by-product of privacy management activities is made available by the Owner.**

The third element of structured privacy management is Evidence. In responsible organizations, the Owner of a privacy management activity provides supporting evidence that the activity is being maintained.

When privacy management activities are performed on an ongoing basis, Evidence is produced as a by-product. Evidence is documentation which may be formal (e.g., policies, procedures, reports) or informal (e.g., communication, agendas, system logs) and can be used with context by the privacy officer to show that a privacy management activity is being performed. For example, the privacy management activity “Maintain PIA/DPIA guidelines and templates” produces several forms of Evidence, including: policies requiring PIAs, procedures and workflows documenting the approval process, PIA guidelines and templates, training documents on how to conduct PIAs, logs of PIAs, etc. This documentation serves as Evidence of accountability.

Refer to Table 0.2 for the characteristics of formal and informal documentation and corresponding examples:

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

Table 0.2 – Characteristics of Formal and Informal Documentation

Table 0.3 describes the role that the privacy office plays depending on the source of the documentation, as well as corresponding examples of the document types:

<table>
<thead>
<tr>
<th>Source</th>
<th>Privacy Office Role</th>
<th>Example Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Produced</strong></td>
<td>The privacy office performs the activity</td>
<td>Data Privacy Policy, Privacy Notice, Data Privacy Training Curriculum, Privacy Impact Assessment Guidelines</td>
</tr>
<tr>
<td>Generated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>by the privacy office with input from other key stakeholders</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 0.3 – Role of the Privacy Office depending on the source of the documentation
Table 0.3 – The Privacy Office’s Role in Production of Documentation

<table>
<thead>
<tr>
<th>Source</th>
<th>Privacy Office Role</th>
<th>Example Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Influenced</td>
<td>Input or opinions are provided by the privacy office</td>
<td>Direct Marketing Procedures, Privacy Impact Assessments, Employment Policies, Records retention schedules</td>
</tr>
<tr>
<td>Collected</td>
<td>The privacy office is kept up-to-date on progress, often only upon completion</td>
<td>Internal Audit Results, IT Security Assessment Results, Business Continuity Plans</td>
</tr>
</tbody>
</table>

Table 0.4 outlines how formal and informal documentation can be produced, influenced, or collected by the privacy office as evidence of the Privacy Management Activities.

<table>
<thead>
<tr>
<th>Privacy Management Activities</th>
<th>Evidence/ Documentation</th>
<th>Source/ Role</th>
<th>Formal/ Informal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain a data privacy policy</td>
<td>Data Privacy Policy</td>
<td>Produced by privacy office</td>
<td>Formal</td>
</tr>
<tr>
<td>Integrate data privacy into policies/procedures regarding access to employees’ company e-mail accounts</td>
<td>E-mail monitoring policy and procedure</td>
<td>Influenced by privacy office, Produced by Information Technology</td>
<td>Formal</td>
</tr>
<tr>
<td>Measure participation in data privacy training activities (e.g. numbers of participants, scoring)</td>
<td>System generated report of data privacy exam scores</td>
<td>Collected by privacy office, Produced by Human Resources</td>
<td>Informal</td>
</tr>
<tr>
<td>Provide notice in marketing communications (e.g. emails, flyers, offers)</td>
<td>Examples of e-mail marketing communications</td>
<td>Influenced by privacy office, Produced by Marketing</td>
<td>Informal</td>
</tr>
</tbody>
</table>

Table 0.4 – Samples of Evidence, Role of the Privacy Office, and Formal/ Informal Evidence

Frequency: Privacy Management Activities are Ongoing

Responsible organizations do not treat privacy as a project, although in many cases privacy management may have started as a project. On the contrary, a responsible organization sufficiently allocates resources to privacy management and continually reevaluates its privacy management 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

Privacy management is a set of ongoing privacy management activities that 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 0.5 reviews privacy management activities to show how the two approaches for the frequency of activities might differ:

<table>
<thead>
<tr>
<th>Privacy Management Activity</th>
<th>Periodic</th>
<th>Continuous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain flow charts for data flows (e.g. between systems,</td>
<td>On an annual basis, require that key stakeholders review the flow charts</td>
<td>Implement as part of the project management requirements that proposed</td>
</tr>
<tr>
<td>between processes, between countries)</td>
<td>for accuracy and update the diagrams as necessary</td>
<td>changes to data flows are identified and the flow charts are updated</td>
</tr>
<tr>
<td>Measure participation in data privacy training activities (e.g.</td>
<td>Each quarter, review reports generated by the e-Learning system to</td>
<td>as a condition of project sign-off</td>
</tr>
<tr>
<td>numbers of participants, scoring)</td>
<td>determine whether all employees have completed the requirements</td>
<td></td>
</tr>
<tr>
<td>Engage stakeholders throughout the organization on data privacy</td>
<td>Establish a cross-functional committee of privacy stakeholders (e.g. IT,</td>
<td>Create an email alias or group discussion for data privacy stakeholders,</td>
</tr>
<tr>
<td>matters (e.g., information security, marketing, etc.)</td>
<td>Marketing, Legal, HR, etc.) who meet on a quarterly basis to discuss data</td>
<td>to facilitate communication on data privacy matters</td>
</tr>
<tr>
<td>Maintain procedures to restrict access to personal data (e.g.</td>
<td>On a monthly basis, review reports of active system users to ensure their</td>
<td>Configure the HR system to send alerts to Information Security when the</td>
</tr>
<tr>
<td>role-based access, segregation of duties)</td>
<td>access is still appropriate and sign-off to indicate approval</td>
<td>employees are terminated or when there are changes to the job title,</td>
</tr>
</tbody>
</table>

Table 0.5 - 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.

An organization that has embedded Responsibility, Ownership, and Evidence into the privacy program has implemented accountability and is now equipped to demonstrate accountability.