Measure and Monitor

Overview

The purpose of this pou is to ensure that your organisation can build a self-sustaining privacy culture that isn't just 'once and done' but is embedded and ongoing.

OPC often see that organisations' privacy programmes are reactive, responding to a specific event or inquiry or not having the time or resources to implement a proper strategy. Organisations often improve practice by responding to the event but may then lose momentum. Building an effective privacy management system requires continuous improvement to lift capability, maintain good practice once this is achieved, and establish a privacy culture that reflects the values of your organisation.

Who is this for?

Your privacy function, as well as those with oversight of, and accountability for, your organisation's privacy work programme.

Key objectives of the Measure and Monitor pou

What would we expect to see?

- Systems and processes are in place for monitoring privacy practice, including performance indicators that are monitored for completion and reviewed when necessary. Measurement outcomes are regularly reviewed by the organisation's governance function to ensure they remain fit for purpose.
- The organisation can demonstrate where performance has improved, and where monitoring has led to changes in practice/process/structure that have improved privacy outcomes.
- Processes are in place to hear from staff about privacy issues.

Monitoring your privacy programme

Monitoring your privacy programme is a key part of ensuring continuous improvement in your organisation's privacy practices. Monitoring can provide you with a holistic picture of your programme and identify areas where training, culture, and processes may need to be improved.

Monitoring activities will look different in different organisations. However, we consider there are some 'must-dos' for all organisations. These are:

- Keeping an incident log that records breaches and near misses and is used to inform reporting.
- Keeping a privacy complaints register that records complaints resolved internally, and complaints made to OPC.
- Keeping a privacy requests register that records the timeliness of responses.

Other monitoring activities may include:

- Seeking staff feedback on the privacy training they receive, and awareness raising activities.
- Conducting a staff survey with privacy-based questions to assess understanding.
- Keeping a record of the number of Privacy Impact Assessments completed.
- Keeping a record of the number of privacy training sessions provided to the organisation.
- Seeking stakeholder feedback on engagements with the privacy function.

Your monitoring activities should give you the data you need to be able to measure the effectiveness of your privacy programme over time. For example, keeping an incident log of breaches and near misses enables you to report on the number and types of incidents, and identify and analyse trends.

Measuring your privacy programme

Collecting data is a useful way to communicate the current state of your organisation's privacy practices and the effectiveness of your privacy programme over time. It's also a useful tool to monitor compliance with certain privacy obligations, including the management of privacy requests.

The table below provides you with examples of useful ways to measure different aspects of your privacy programme, including what they might tell you, and things to look out for.

You will need to consider which measures will help you achieve your organisation's privacy goals and outcomes. These should be based on the key objectives and actions you have committed to in your privacy management plan.

Note: If you're a public sector organisation then you will be required to complete the Privacy Maturity Assessment Framework (PMAF) to measure, and report on, your privacy programme.

Training & Awareness	What can this tell you?	Look out for…
Number and type of privacy trainings offered to staff.	• Who you have managed to reach with training so far, and where any gaps might be.	• This is a quantitative measure, so won't give you information on the quality or effectiveness of your training.
Percentage of staff trained and how often.	• How well your privacy training programme has been operationalised over time.	• Understanding the percentage of staff who have received training is a good starting point, but you may need to test staff understanding as well to ensure the training was effective. • You also need to consider what kind of roles trained staff have, and if there are gaps – such as high-risk teams/roles with no one who has received training.
Survey feedback on privacy training, for example, feedback on an internal e-learning module.	• How useful and/or engaging the organisation found the module.	• The training might have been popular but not necessarily effective.
Engagement of stakeholders with the privacy programme.	• If engagement is low or high and in which areas. • If your awareness campaigns or initiatives are effective.	• Repeated engagement from the same area of your organisation may indicate they aren't getting the information they need.
Number of unique clicks on internal privacy policies and procedures.	• Whether staff know how and where to access privacy policies and procedures.	• Reporting on the number of clicks without analysis of who is visiting the site, for example, it could just be the privacy team.
Time spent by staff on web pages containing internal policies, procedures and privacy information.	• Whether the material is easy to access. • Whether staff are interested in, or using, material available to them.	• Time spent could indicate staff found the page helpful, or that it was hard to understand. Consider seeking qualitative feedback from staff.
Number of initiatives or campaigns to promote privacy e.g. privacy week, newsletters, intranet stories, and messages from leadership.	• Whether communications are only at specific times of the year or because of an event.	• As well as privacy-specific campaigns, use other campaigns to promote relevant privacy messages where possible, such as cyber security awareness, to show how privacy links in with the organisation's work as a whole.
Requests, enquiries, complaints, and	**What can this tell you?**	**Look out for…**

breaches		
Number of access and correction requests.	• Many correction requests in a particular area may indicate issues with the accuracy of personal information you hold. • No requests may indicate that individuals don't know they can make these requests, or the information to do so is hard to find.	• Whether requests are going to the right part of the organisation and are being logged. • Request volumes could be subject to external factors, for example, a significant privacy breach might result in a spike in access or correction requests. Consider using trend analysis to more accurately interpret the data.
Response time for access and correction requests.	• Whether you're meeting your legal obligation. • Whether too much time is being spent on simple requests.	• Requests can come into the organisation in many ways. Measuring response times without looking at reasons for delay can mean process improvement opportunities across the organisation may be missed. For example, if requests to general enquiry inboxes or mail rooms are not promptly sent to the privacy function this could show a lack of process.
Number of privacy complaints received and upheld, and the themes of the complaints e.g. collection, disclosure, or access.	• A high number of privacy complaints could indicate that your organisation is not handling personal information in accordance with the Privacy Act. • The types of privacy complaints. • Whether the complaints are bundled e.g. a general customer complaint with a privacy angle. • Whether the complaint was upheld or note and if so, what was done to fix things.	• Even if a complaint is not upheld, it can tell you a lot about how you're communicating with people. • Complaints take time to deal with and can place pressure on staff. Knowing what that workload looks like could help you to develop more efficient processes.
Number of privacy complaints made to the Office of the Privacy Commissioner and the outcome of those complaints.	• A high number of complaints made to OPC might indicate that you need to change the way you manage complaints internally. For example, if your organisation is taking a combative or overly defensive stance when responding	• If your organisation generally has a low number of complaints, a percentage increase that appears significant may only mean one or two more complaints than usual. It's useful to have a baseline of average complaint numbers to help

	to privacy complaints, this could result in a higher number of individuals who feel that their complaint was not properly resolved.	accurately interpret the data.
Number and type of privacy breaches and near misses, and the root cause.	• Privacy breaches and near misses are an important measure of compliance. • Breaches and near misses provide valuable insights into areas for improvement.	• An increase in breaches or near misses may be due to an increase in staff reporting them once they've been trained. If you see a trend of incidents increasing after a training session, that may be an indication the training was successful. • Similarly, a strong decline or no breaches being reported in particular areas of the business may raise questions. • However, repeated breaches of a similar nature that could be resolved with more awareness or training may indicate that existing training is insufficient. • Don't ignore near misses. They can be a great indication of a problem waiting to happen.
Where privacy breaches or near misses are occurring, for example, working offsite, in the office, or in transit.	• Whether particular attention needs to be given to certain areas or types of workplaces.	• The number of incidents may reflect the culture of reporting within each of these areas. For example, if a business unit that works predominantly offsite has a strong culture of reporting privacy incidents, it could appear they are having more incidents than other areas.
Number and types of external enquiries to the privacy function.	• A high number of enquiries to the privacy function might indicate that your privacy information (such as statements and notices) is not sufficient. • The types of enquiries your privacy function receives can provide useful insights into the privacy issues that really matter to the people you deal with.	• If your organisation generally has a high number of privacy enquiries, then this may not be significant. It's useful to have a baseline of average enquiry numbers to help accurately interpret the data.
Sources of enquiries, complaints, and breaches.	• If enquiries, complaints, or breaches tend to be prompted by a particular process,	• There may be areas of your organisation that deal with more personal information

	business unit, or product, this could indicate that there are issues with the way those areas handle personal information.	daily than others. It's important to know your data and map your information flows.
Number of Privacy Impact Assessments being completed.	• Number of initiatives that passed under a threshold assessment. • Amount of time to complete a PIA can indicate complexity of projects or resourcing issues. • If some areas of the organisation aren't completing PIAs, despite doing work that requires a PIA, this could be an indication that a greater focus on privacy by design is needed in those area.	• PIAs alone don't tell the whole story, and numbers alone don't provide much insight into the kinds of risks described in the PIAs.

Assurance and Reporting

Assurance is about providing your leadership, governance function, and other key stakeholders with a clear message about your organisation's privacy practices, to give them confidence that the expected privacy outcomes and benefits are being achieved. It helps to measure the effectiveness of your privacy procedures, demonstrate compliance, increase privacy awareness, highlight any gaps, and provide a basis to support improvements to your privacy programme.

Providing assurance by using reports, assessments, and communication (at all levels of your organisation) are all good ways to ensure privacy assurance is a key component of your privacy programme.

You may also consider seeking independent assurance of your privacy practices and culture overall. For example, using an external audit provider every five years to provide your organisation with an independent assessment.

Reports to senior leadership or relevant governance groups should include the data from the measures you have selected above, as well as an accompanying comment about your organisation's privacy practices and programme. Data is most useful when used to tell a story about what is happening. Numbers alone won't usually paint an accurate picture. The trends or patterns you are seeing over time, plus the reason for them, is what is important. You can use the 'What can this tell you?' section of the table above as a starting point to help inform your reporting.

Organisation examples

We've included some use cases based on fictional organisations to demonstrate each of the pou in practice. Read more about them in Introducing the Organisation Examples.

Large business – Fern Leaf

As a large business, Fern Leaf adopts a three line of defence model. This is a risk governance framework that splits responsibility for operational risk management across three areas. People in the first 'line' own and manage risk directly. The second line oversees the first line, setting policies, defining risk tolerances, and making sure they're met. The third line, consisting of internal audit, provides independent assurance of the first two lines. Privacy risks are part of Fern Leaf's overall risk strategy. This greatly assists the workload of the privacy team as they can collaboratively work with the risk function to document what they decide to measure and how they will do so. Results of assurance reporting are regularly reported to Fern Leaf's Board and incorporated into their risk strategy conversations.

Small business (charity) – Reach High

Reach High has developed a Privacy Risk Register to capture all its privacy risks and events. The register is an excel spreadsheet with tabs for the following privacy-related activities or events:

- Privacy programme actions (capturing progress).
- Privacy training delivered.
- PIAs completed.

- Privacy requests received and managed.
- Privacy Complaints received (including escalated complaints).
- Privacy breaches.

The Director of Support Services manages the register and reports on this to the CEO and other senior leaders monthly. As a small business, this approach is appropriate, and ensures that the CEO has oversight of key privacy metrics.

Start-up – Swiftstart NZ

Given their size and limited resources, Swiftstart NZ decides to adopt a streamlined approach to privacy measurements. The Operations Manager produces quarterly documentation of key measurements to ensure Swiftstart NZ's founders maintain visibility of its privacy practices without overwhelming their capacity.

Measurements include the number of reported incidents or breaches, response time to incidents, and effectiveness of remediation measures. Additionally, the Operations Manager confirms completion rates of staff privacy training. These minimal yet essential measurements not only demonstrate accountability but also enable Swiftstart NZ to efficiently report to clients if necessary, fostering trust and transparency in its operations.

Small business (non-tech) – Green Gardens

Green Gardens has developed a Privacy Register which is an excel spreadsheet that captures the following privacy-related activities and incidents:

- Privacy training completed.
- Privacy requests received and managed.
- Privacy complaints received.
- Privacy breaches and near misses.
- Privacy analysis documents.

The Administrator manages the register and uses it to report to the Owner/Manager as part of their 6-monthly business meetings, where they have a standing agenda item for privacy.

Independent contractor – Jo Jones

Jo Jones maintains a Privacy Register which is an excel spreadsheet that captures the following privacy-related activities and incidents:

- Privacy requests received and managed.
- Privacy complaints received.
- Privacy breaches and near misses.

Government agency – The Ministry

The Ministry has a well-established risk and audit function and an audit and risk committee made up of external and Tier 3 level members, who receive regular reporting on all identified risk, including privacy. Reporting on completion of Privacy Threshold Assessments, PIAs, complaints, breaches, near misses, and other privacy events are provided to the committee regularly. The Committee can make recommendations to SLT to remediate risk. The Ministry

also plans to get an independent assurance review of its privacy risk management approach every 5 years or more frequently if themes are identified through reporting.