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 breaches	What can this tell you?	Look out for…
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 to privacy complaints, this could result in	• 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 accurately interpret the data.

	a higher number of individuals who feel that their complaint was not properly resolved.	
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, business unit, or product, this could indicate that there are issues with the	• There may be areas of your organisation that deal with more personal information daily than others. It's important to know

	way those areas handle personal information.	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.