KPMG

cutting through complexity

ADVISORY

Accident Compensation Corporation

Independent Privacy Follow-Up Review

17 December 2014

kpmg.co.nz

KPMG
10 Customhouse Quay
Wellington
New Zealand

PO Box 996
Wellington 6140
New Zealand

Telephone	+64 (4) 816 4500
Fax	+64 (4) 816 4600
Internet	www.kpmg.com/nz

Ms P Rebstock
Board Chair
Accident Compensation Corporation
PO Box 242
Wellington 6140

17 December 2014

Dear Paula

Independent Privacy Follow-Up Review

We have completed our work in relation to the follow-up audit of the Independent Review of the Accident Compensation Corporation's (ACC) Privacy and Security of Information. Our work was performed in accordance with our Engagement Letter dated 20 June 2014.

We would like to thank ACC's staff and management, external stakeholders and other organisations who contributed to this review.

We would be happy to answer questions relating to our report, or to provide more information about our review, at your convenience.

Yours sincerely

Souella Cumming
Partner

Contents

Disclaimers

Inherent Limitations

This report has been prepared in accordance with our Engagement Letter dated 20 June 2014. The services provided under our engagement letter ('Services') have not been undertaken in accordance with any auditing, review or assurance standards. The term 'Audit/Review' used in this report does not relate to an Audit/Review as defined under professional assurance standards.

The information presented in this report is based on that made available to us in the course of our work, publicly available information and information provided by the Accident Compensation Corporation. We have indicated within this report the sources of the information provided. Unless otherwise stated in this report, we have relied upon the truth, accuracy and completeness of any information provided or made available to us in connection with the Services without independently verifying it.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, Accident Compensation Corporation management and personnel consulted as part of the process.

The findings in this report are based on a survey and the reported results reflect the information provided by, and the perceptions of, the sample of respondents surveyed, as approved by the Accident Compensation Corporation, as at the date of the survey. Any projection to a wider group or to the future is subject to the level of bias in the method of sample selection and to changes in perceptions.

KPMG has not sought to verify independently the information contained in this report. No warranty of completeness, accuracy or reliability is given in relation to the information provided by the survey respondents.

KPMG is under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form.

Third-party Reliance

Other than our responsibility to the Accident Compensation Corporation, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility.

Our report was prepared solely in accordance with the specific terms of reference set out in the Engagement Letter, dated 20 June 2014, and agreed between Accident Compensation Corporation and ourselves, and for no other purpose.

KPMG expressly disclaims any and all liability for any loss or damage of whatever kind to any person acting on information contained in this report, other than the Accident Compensation Corporation. Additionally, we reserve the right but not the obligation to update our report or to revise the information contained therein because of events and transactions occurring subsequent to the date of this report.

1 Executive Summary

1.1 Context to the Independent Review

In August 2012, the Independent Review report into a Privacy breach by the Accident Compensation Corporation (ACC) – involving disclosure of the details of 6,748 clients – was released. *"The Independent Review Team concluded that the breach that occurred was a genuine error but that errors are able to happen because of systemic weaknesses within ACC's culture, systems and processes."* The Independent Review report included 44 recommendations designed to address these systemic weaknesses.

One of the recommendations was that a Privacy audit be undertaken every two years to consider ACC's adherence to its Privacy Strategy, including compliance and best practice elements. This review was requested by ACC in response to the 2012 recommendation. The Board requested this review in order to measure progress and identify further improvements that could be made.

Fieldwork was undertaken between June and October 2014 and included: a review of documentation; interviews with Board members, the Executive, management and staff; a survey of all ACC staff; site visits and walk-throughs of processes; a workshop with the Voice of the Customer (VOC) forum; and benchmarking with relevant organisations, both in New Zealand and internationally.

1.2 Objectives

The objectives of the review were to:

- Assess ACC's adherence to, and implementation of, its Privacy Strategy; the assessment was undertaken with consideration of the following:
  - Compliance with relevant legislation including the Privacy Act 1993.
  - Adherence to best practice, including the recently published Privacy Maturity Assessment Framework (published by the New Zealand Government).
  - Appropriateness in terms of the risk related to the nature of the client data/information maintained by ACC.
- Compare progress against that of external organisations that were consulted in the original review.
- Determine ACC's progress against the recommendations.

1.3 Overall assessment

Since the 2012 Independent Review, ACC has focused on making changes to the way in which personal data of clients is dealt with, and how such data are viewed by staff. ACC has invested significantly in Privacy-related resourcing, including:

- Setting the Privacy Vision and Strategy, and communicating this to staff.
- Setting up of a dedicated and relatively large Privacy Team.
- Developing and implementing a Privacy Strategy, as well as a range of new supporting policies and procedures.
- Reporting regularly to the Board and Executive on matters related to Privacy.
- Implementing Privacy training across the organisation.
- Ensuring that there is ongoing communication from the Privacy Team and management regarding Privacy.

- Deploying significant resourcing to address access requests, Privacy-related initiatives and other checks and balances.
- Establishing a Privacy breach reporting and analysis process, with a supporting breach reporting tool.
- Developing and publishing the Personal Information Management Index (PIMI).
- Holding risk workshops to identify potential Privacy risk areas.
- Implementing improvements and 'work-arounds'within the claims management processes, including reducing the use of spreadsheets for reporting and implementing mail marshal email control.
- Conducting quarterly assurance reporting over key Privacy controls in claims management to ensure ongoing visibility of effectiveness of manual controls.
- Establishing a Privacy impact assessment /Privacy threshold analysis process.

Together, these changes have had a positive effect on the overall maturity of Privacy management across the organisation. There has been a strong focus on resourcing, both to resolve the findings of the Independent Review and to reduce the likelihood of breaches occurring.

There has been a 53% reduction in the number of complaints about ACC made to the Privacy Commissioner between the 2012/13 and 2013/14 financial years.

ACC's key focus is on improving the public's trust and confidence in the accident insurance scheme. It is understood that the major breach has had a significant impact on trust and confidence, and has been the catalyst for the increased access requests over the period. The expectations that have been outlined are that services to clients and levy-payers need to be responsive, transparent and effective, and to provide value for money.

ACC has embarked on a significant transformation programme called Shaping Our Future to help make ACC fit for the future: transforming the organisation's ability to deliver great outcomes for New Zealanders through its value proposition, operating model and technology. Part of Shaping Our Future is about ACC 'looking through the eyes of its customers' to help rebuild the public's trust and confidence.

Public trust and confidence has increased to 54% in 2013/14, up from 47% in 2012/13, and ACC is targeting it to be 60% in 2014/15.

ACC's Privacy Strategy is the driving force behind most of its work on enhancing personal information management and, along with related policies, is considered to be a good basis on which to build into the future. The Strategy covers: what personal information is and why it is important; ACC's Privacy Vision, Principles and accountabilities; strategic intent; and performance indicators and how these will be monitored. The contents are consistent with the Independent Review recommendations. However, we have made some recommendations regarding the Strategy, which will guide ACC in continuing to enhance Privacy management within the context of the Shaping Our Future transformation programme.

The layered Privacy notice on ACC's external website is visible and detailed with information about ACC's Privacy practices including strategy and vision. External stakeholders acknowledge some improvement, although they do not have clear visibility over all of the changes, as consultation and engagement have been conducted on an 'as needed' basis.

The relentless focus of ACC's Board and Executive team is on Privacy and this is driving a culture where Privacy is both 'top of mind' and practised on a daily basis by management and staff. The cultural shift over the last couple of years is particularly evident within the ranks of front-line staff members, who are committed to continual improvement of Privacy processes. It is clear that ACC has managed to make Privacy an integral part of the staff work ethic and focus in a relatively short time frame. A dedicated Privacy Team has achieved significant results and has kept Privacy 'alive and well'. Investment and resourcing within the front line have ensured that historical information is cleansed or redacted prior to release.

Breach detail in the context of 'risk' or 'severity of harm' is not explicitly reported in ACC's external accountability documents. This has been incorporated recently into the reporting to the Board and Executive and includes a distinction based on risk, with any medium or high risks identified; included in this is the rationale for the risk rating. The current definition does not distinguish breaches based on materiality (for example, those based on sensitivity of information, the number of people involved, other indications of a systemic problem, etc.). While the definition is broad in this context and was appropriate for ACC at that point in time, it is narrow in the overall measurement of managing personal information (i.e. it does not consider measurement across the other Privacy Principles).

ACC should revisit the current definition of a breach in consultation with the Office of the Privacy Commissioner or the Government Chief Privacy Officer, to ensure it not only continues to meet ACC's needs for root-cause analysis, but also provides for more comprehensive reporting and assessment, both internally and externally.

Despite the level of resourcing and attention committed to improving Privacy management at ACC, the effectiveness of this is constrained by the fact that, fundamentally, the organisation remains the same. The same systems and business processes are in place as at the time of the Independent Review, although these are overlaid now by largely detective controls (i.e. processes designed to identify any issues). Many of the controls in place to mitigate Privacy risks are manual, and reliant on individuals to follow them, in the absence of re-engineered business processes with Privacy by Design Principles embedded. Therefore, human error remains an ongoing cause of Privacy risk.

A perceived discrepancy was acknowledged by some staff spoken to during site visits (and from the free text field of the survey) between key performance indicators (KPIs) that consider quality (including the appropriate management of personal data) and those that assess quantity or volume (e.g. the number of claims processed per day). Staff advised that it is sometimes difficult to understand how to manage the apparent conflict between being assessed based on the speed of progressing a claim, and the need to undertake careful, and largely manual, Privacy checks. This, at times, results in frustration for the staff concerned.

ACC is aware that the longer-term solution is to embed Privacy by Design Principles into business processes through the impending 'Shaping Our Future' programme of work. Shaping Our Future is critical to enable ACC to address its interaction with clients, providers and levy-payers, and to design systems to address the various manual processes and current system limitations.

Developing a personal information inventory will be a critical input for the Shaping Our Future programme, as will further improvements and maturing of the three lines of defence framework: particularly embedding the aspects of mature risk management, compliance and quality assurance programmes.

ACC has implemented a dedicated Privacy programme of work as part of the strategic change portfolio. The programme has implemented and amended systems and processes, and resourced the Privacy agenda, to address the recommendations made by the 2012 Independent Review. This includes a dedicated Privacy Team represented on the Executive team, new or amended business processes, and training and education. Privacy by Design Principles have been used, where possible, to address complex business processes. This has resulted in tactical gains for ACC and some system enhancements, albeit within existing system constraints.

ACC acknowledges that risk of a future major, or more minor, Privacy breach is still relatively high, even though it has reduced over the past two years. Privacy remains the Board's highest-rated risk, due to the impact this would have on trust and confidence in ACC and its services. An overall organisational objective in relation to Privacy has been added to the Service and Purchase Agreement with the Minister to reflect the importance of this.

Good progress has been, and continues to be, made against the 2012 recommendations. Progress in enhancing the management of personal information, especially when compared with other organisations both nationally and internationally, has been rapid and focused. We are not aware of any other New Zealand agencies or organisations that have added a comparable level of dedicated resourcing and attention to Privacy protection, and issue detection, within such a short time frame. This is commendable.

Overall, ACC has made significant advances in Privacy management across the organisation since the prior review in 2012, including adherence to, and implementation of, its Privacy Strategy. The challenge for ACC into the future involves shifting from a focus on disclosure breach reduction to maturing information management in relation to each of the 12 Principles of the Privacy Act 1993. This requires the embedding of risk management best practice across all aspects of a well-understood personal information life cycle, including the collection, use, storage, access, disclosure and retention of personal data.

1.4 Summary of ongoing critical success factors

In order to reduce Privacy risk for ACC further, we have made the following recommendations:

1. Review and enhance the Privacy Strategy with a shift in focus to consider the wider personal information life cycle and reflect the requirements that will be evident two years on from the initial review. This should include the following:
    a. Integration with the Shaping Our Future programme, an enhanced Privacy Team work plan and integration with ACC's business planning processes (see section 3.2 of this report).
    b. Undertaking a formal, comprehensive Personal Information Inventory (section 3.5.1).
    c. Updating the Privacy Team's work plan to ensure it reflects priorities based on risk and the results of the Personal Information Inventory (section 3.5.3).
    d. Developing a Privacy performance measurement framework, including relevant KPIs, which should be based on specified requirements that cover all aspects of the 12 Privacy Principles and a reviewed definition of breaches and near misses (section 3.5.2).
    e. Proactive engagement and consultation with stakeholders in relation to the Privacy Strategy and other relevant matters (section 3.2.1).
2. Resolve the perceived discrepancy between quantity and quality KPIs for staff (section 3.3).
3. Enhance the enterprise-wide three lines of defence operating model to enable better integration with Privacy risks, and compliance and assurance frameworks (section 3.4.2). This should include:
    a. Embedding Privacy within defined, formal and structured organisation-wide operational risk management processes, including monitoring of the use of business unit-level operational risk registers and data recorded through these.
    b. Embedding Privacy within a strong three lines of defence model, including enhanced second line functions of risk management, compliance and first line quality assurance (section 3.4.2).
    c. Articulating Privacy risk within the overall organisational risk appetite and risk management processes (section 3.1.1).
    d. Reporting regularly to the Executive and Board with overviews of Privacy assurance (a combination of First-line quality assurance, Second-line compliance and Third-line assurance) results (section 3.4.2).
    e. Resourcing and deploying the Compliance programme agenda to ensure compliance with Privacy-related controls (section 3.1.1).
4. Enhance risk management, including assurance, in relation to third parties' information management processes (section 3.4.1). This should include:
    a. Ensuring that ACC's role in relation to Privacy within the wider sector – influencer versus enforcer – is included in the development and implementation of an approved Stakeholder Engagement Framework (section 3.4.1)
    b. Considering the approach to ensuring compliance and gaining assurance over providers' Privacy practices (section 3.4.1).

5. Confirm and agree on the approach for Shaping Our Future in addressing business process and system Privacy risks, issues and recommendations, and enhancement of Privacy maturity across all of the Information Privacy Principles, based on a Privacy by Design approach (section 3.6.1). This should include:

    a. The Privacy Team proactively engaging with the Shaping Our Future programme to ensure that its Privacy pillar is appropriately reflected in programme planning, design, implementation and resourcing (sections 3.2 and 3.6.1)

    b. An assurance that adequate Privacy Subject Matter Expert resource is embedded in the Shaping Our Future programme (i.e. developing processes, systems and controls to ensure that Privacy by Design is fully embedded), while maintaining the momentum of what is happening currently in the Privacy space.

1.5 Acknowledgements

We would like to thank ACC's staff, management, Board, external stakeholders and other organisations who have contributed to this review.

2 Background

2.1 ACC roles and responsibilities

ACC is the Crown Entity set up under the Accident Compensation Act 2001 that manages and delivers New Zealand's universal, no-fault, accident insurance scheme (the Scheme). The Scheme supports injured people to return to work, independence or everyday life, as quickly and safely as possible.

It is a large organisation in the New Zealand public sector, with a headcount of 3,308[1], 25 branches, 3 specialised units (for example, the sensitive claims unit) and numerous contact, service and processing centres. ACC deals with large amounts of information, much of which is personal information, in the course of its dealings with customers, customer representatives, medical professionals, other agencies and other external stakeholders. This includes[2]:

- 25,000 letters sent each day
- 7,000 claims processed each day
- 24,000 calls answered each day
- 1,000,000 emails dealt with each month
- 80,000,000 documents on file.

2.2 Privacy at ACC

In 2012, an Independent Review of ACC's practices in relation to Privacy and security of information was undertaken at the request of the Office of the Privacy Commissioner and the ACC Board. This was requested as a result of a significant Privacy breach that occurred on 5 August 2011 and became public in March 2012. ACC first became aware of the breach on 1 December 2011. The breach involved the unauthorised disclosure of the details of 6,748 clients and was the subject of intense media and government attention.

Following the breach becoming known to ACC, a response team was established to manage the breach and inform those affected. In addition, the Independent Review was commissioned.

The Independent Review found that ACC did not immediately appreciate the significance of the breach until it was made public, and that it could have done more to follow through on the information when it was initially informed of it.

As a result of the independent review, 44 recommendations were made. These recommended improvements are in the areas of:

- BOARD GOVERNANCE AND LEADERSHIP
- PRIVACY STRATEGY
- CULTURE
- ACCOUNTABILITY
- PRIVACY PROGRAMME
- BUSINESS PROCESSES AND SYSTEMS

A number of Privacy-related projects were initiated to address the recommendations of the independent review.

[1] *Source:* ACC's Annual Report 2014

[2] *Source:* ACC's Statement of Intent 2013–2016

ACC has since established a Privacy Team with responsibility for implementing the recommendations, dealing with Privacy issues and improving ACC's overall practices for personal information management across the organisation. The Privacy Team is managed by the newly created position of Chief Governance and Strategy Officer, who is the Executive Privacy Officer and holds formal responsibility for Privacy at the Executive level.

The team is led by a Strategic Privacy Manager and supported by the people managers throughout the organisation who are responsible for Privacy management within their teams. Performance criteria for all leadership (and staff) now incorporate Privacy.

Following the 2011 breach, there has been a marked increase in the number of requests from individuals for their files. This increases the risk of inappropriate data being released. As a result, ACC has introduced new teams whose specific task is to double-check outgoing files and correspondence. In addition, processes have been altered or developed to mitigate the risk of a Privacy breach, and training and education for all staff members, and a large number of third parties, is ongoing.

Privacy is a key component of ACC's planning and accountability documents and targets. Internally, targets for the number of Privacy breaches have been set that reduce over time. The Privacy Team reports on breaches notified to them and the number of breaches over the last two years is trending downwards, from a rolling three-month average of 68 per month in June 2012[3] to 19 in June 2014[4].

Awareness of personal information management practices and drivers is high throughout the organisation. Almost all staff members and management personnel spoken to during this review were highly supportive of Privacy as a concept, ACC's approach to Privacy, the Privacy Team and the ongoing work to support and enhance the management of personal information. The process for managing a Privacy breach is now well documented and understood, with clear escalation paths. Roadshows around the claims management network have helped to ensure staff members are highly aware of the process to follow if a breach occurs; this was confirmed throughout our site visits and survey.

[3] *Source:* ACC's Annual Report 2012

[4] *Source:* ACC's Annual Report 2014

3 Detailed Findings and Recommendations

In the two years since the major breach became a focus of media and government attention in 2012, ACC has committed a significant amount of time and substantial resources to minimising the risk of a similar event recurring. ACC has focused strongly on developing, embedding and enhancing the maturity of Privacy management across the organisation.

ACC’s Privacy Vision and supporting Strategy have been developed to ensure the work undertaken in this area continues, and that ACC becomes recognised as a leading practitioner in New Zealand Privacy management. ACC aims to achieve this through effectively and efficiently reducing Privacy risk for its customers by enhancing Privacy maturity throughout the organisation.

/53 % reduction in the number of complaints about ACC made to the Privacy Commissioner between the 2012/13 and 2013/14 financial years[5].

Significant advances, particularly in the acceptance of the importance of personal information management by all levels of governance, management and staff, show that Privacy continues to be a core focus for the organisation. This is reflected in Privacy being rated as the number one strategic risk. Additional processes, aimed at reducing the likelihood of personal data disclosure breaches, have been implemented.

ACC recognises that truly optimal Privacy maturity cannot be achieved in just a couple of years. The focus, to date, has been primarily on reducing the disclosure breach risk while making some progress in the other Privacy Principles. ACC’s next challenge is how to balance the focus between disclosure breach avoidance and the enhancement of Privacy maturity over all aspects of the management of personal data.

Particular areas of good practice are detailed below, along with identified gaps and areas for improvement.

3.1 Board governance and leadership

The Board and Executive’s continued focus on Privacy is driving a culture where Privacy is ‘top of mind’ for management and staff. The cultural shift is particularly marked, and it is clear that ACC has managed to integrate Privacy into the staff work ethic and focus in a relatively short time frame.

ACC’s Board and Executive proactively demonstrate the importance of, and their support for, best practice in the management of personal information. The Chief Privacy Officer (recently included in the role of the Chief Governance and Strategy Officer) is a member of the Executive team and, thus, is well placed to ensure that Privacy risks and issues are well known and considered within the context of all issues discussed by management.

/92 % of respondents to the survey[6] Agree or Strongly Agree that Leadership (Management / Board / the Executive) demonstrates that respecting Privacy is important and show its support for Privacy initiatives.

[5] *Source:* Office of the Privacy Commissioner

[6] A survey of all staff members was undertaken during August 2014 as part of this review, with a response rate of 56%.

Staff members agree that the Board and Executive lead by example and that behavioural expectations for staff are clear. This message is acknowledged, understood and valued by the wider organisation.

Following the negative public reaction to the 2011 breach, and the subsequent loss of trust and confidence in ACC, the Board has rated Privacy as the number one risk faced by ACC as it clearly understood that concerns over issues of Privacy had a significant impact on the public's trust and confidence in ACC.

The Board has made resourcing available for a relatively large Access Request and Privacy Team. There are ongoing Privacy projects and initiatives, including staff induction and training, which are having positive effects on the overall maturity of Privacy management across the organisation.

84%

of respondents to the survey believe the Board and senior management are Effective or Very Effective in communicating their expectations around Privacy and personal information management.

The Board has stated clearly its commitment to achieving ACC's Privacy Vision that: "*Personal information in our care will be managed as carefully and respectfully as if it were our own*". There is ongoing communication with staff and the Executive team, and Privacy is included in the Board Audit and Risk Committee's terms of reference and external accountability reporting. There is a cycle of continuous accountability to the Board by the Executive through regular reporting and updates. Privacy is a standing agenda item for Board, Executive and management meetings, and is discussed actively.

ACC's Board and Executive have participated in the development of, and endorsed, Privacy-specific strategy and policies, regular review of key measures, and the granting of formal accountability for Privacy within the Executive. The Strategy is covered in detail in section 3.2 of this report.

In addition, the Board requested this review to measure progress and identify further improvements that may be made.

The Board and Executive need to continue to drive a proactive and embedded Privacy vision and strategy to maintain the momentum. With the impending Shaping Our Future transformation programme, and the number of other strategic initiatives in train at ACC, there is a risk that momentum in this area could be lost. In essence, there is a need to keep the 'foot on the accelerator' to ensure personal information management at ACC continues to receive focus in order to mitigate Privacy risk to a sustainable and acceptable level.

3.1.1 Risk management

Practical risk-reducing tasks (such as locking away documents while a desk is unattended) are generally well implemented by the majority of staff. There is a good perceived understanding by staff and management of Privacy risks, ACC's tolerance for Privacy-related risk and expectations for personal information management. There is also a perception by staff that ACC is proactive in terms of initiating change rather than waiting to react to Privacy events.

56%

of Managers who responded to the survey think they are responsible for maintaining and regularly updating a Privacy risk register, even though90% think they are responsible for identifying, assessing and managing Privacy risk.

Privacy is included now, specifically, in the risk management framework at ACC and has been added to the risk matrix that is used to assess all risk. An Issues Management Team exists that is an escalation point for areas of high risk and potential media-related enquiries, including Privacy. In terms of formal risk management process, however, there are inconsistent practices noted across the different parts of the organisation, regarding how Privacy risks are identified, recorded and reported, and what mitigation strategies are put in place to manage these.

Privacy risk is not integrated with organisational operational risk management processes. Business unit managers are responsible for identifying, managing and reporting on Privacy risk within their areas of the business but the way in which these practices are carried out is inconsistent. Often, risk registers are not updated and, when they are, there is a focus on issues rather than on risk. While there is a good process in place for performing root-cause analysis on breaches reported (reactive), there is no process for collating Privacy risk data across the business (through the active monitoring of risk registers) in order to identify risk trends (proactive). Having this information, and the analysis of it, could enable organisation-wide assessment of operational and strategic Privacy risk, and implementation of mitigating actions. A more formal, structured approach is required in order to address these gaps.

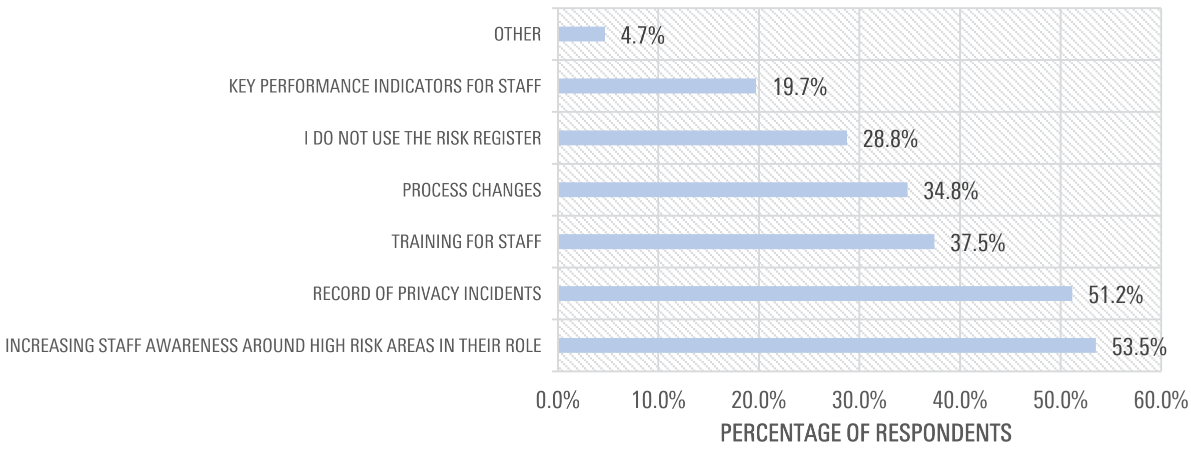
In order to be fully effective, there is additional work to be done in embedding a strong three lines of defence risk management model. Such a model intends to clarify responsibilities and to coordinate effectively and efficiently across these groups so that there are neither gaps in controls nor unnecessary duplication of coverage.

This relies on clearly articulating Privacy within the organisational risk appetite and risk management processes. This is particularly important because Privacy is rated as the Board's highest risk.

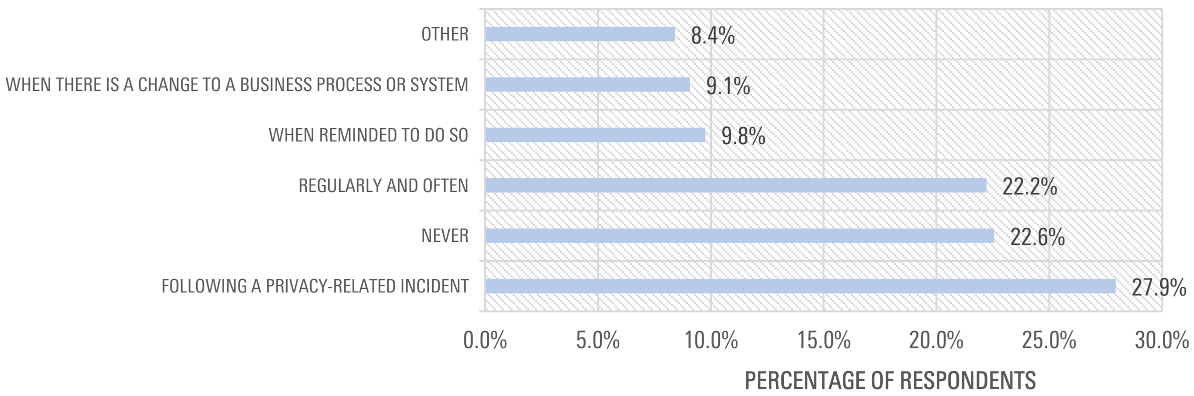
There could be improved coordination of the Compliance function, Quality Assurance Teams and Assurance Services to provide overall assurance to the Board and Executive, that Privacy-related risks and controls are being identified and managed in an effective manner. For detail, see section 3.4.2.

The graph below shows the ways in which managers currently use their teams' risk registers (note that all of these are mandatory).

"IN WHAT WAYS DO YOU USE YOUR BUSINESS UNIT'S PRIVACY RISK REGISTER?"



"HOW OFTEN DO YOU REVIEW AND/OR UPDATE THE PRIVACY RISK REGISTER?"



These survey answers demonstrate a lack of consistency in the process and approach to recording Privacy risk throughout the organisation. They also imply a lack of either guidance or understanding regarding the purpose of the risk registers.

In order for ACC to address Privacy risk, it must first identify and assess the likelihood and potential consequence of each risk. This requires:

a. A coordinated and consistent approach across the organisation

b. Consideration of Privacy risk within the agency's enterprise risk management function, which should include Privacy risk identification and assessment as integral parts of business-as-usual activity

c. Reporting on Privacy risks that includes key risk indicators. Risks should be linked to the Privacy Strategy so that risk information is integrated into reporting on Privacy management performance.

WE RECOMMEND that the issue of Privacy be embedded within defined, formal and structured organisation-wide operational risk processes. This process should include:

a. Articulating Privacy risk within the overall organisational risk appetite and risk management processes.

b. Resourcing and deploying the Compliance programme agenda to ensure compliance with Privacy-related controls.

c. Monitoring and reporting on the use of business unit-level operational risk registers, and the effectiveness of use of these.

d. Monitoring of mitigating actions taken as a result of identified risk.

3.2 Privacy Strategy

ACC has a Privacy Vision that is clearly understood and supported by staff. ACC's Privacy Strategy document is consistent with, and aligned to, the organisation's overall strategic intent.

A Strategic Privacy Manager position has been created in the Privacy Team; this role includes responsibility for leading the implementation of the Strategy.

The Strategy was developed in response to the 2012 Independent Review report. It was developed by the Privacy Team in consultation with the Board and Executive, and was approved by the Board.

The Independent Review report recommended that stakeholders be consulted also during the development of the Strategy. Consultation was primarily with the Advocate Representation Group, as part of the Voice of the Customer programme. ACC acknowledges that this consultation took place late in the development process, and we have been informed that it intends to request consultation earlier in the process when the Strategy is next reviewed (following the release of this report).

The Strategy is readily available for all members of staff to obtain and review. It is supported by a comprehensive suite of policy documents and front-line staff members are well aware of the Privacy policies and procedures that may impact on them in the course of their work. These policies and procedures are well regarded by staff.

The Strategy provides context and strategic intent for Privacy management and a high-level structure for allocating resourcing and monitoring effectiveness.

However, it does not contain much detail in terms of exactly how ACC's Privacy Vision is to be implemented. There are gaps between the high-level Strategy document, policies and procedures, integration with standard business planning processes, and the work plan of the Privacy Team.

/84%

of respondents to the survey rate the Privacy Strategy and related documents as Good or Very Good.

The move to truly effective Privacy management requires a detailed approach, supported by a comprehensive work plan for the Privacy Team, integrated with business planning processes within ACC. Enhancing the Privacy Strategy by drawing on other strategic intentions such as 'customer experience' could be the next stage.

The Privacy Strategy is focused strongly on avoiding disclosure breaches and was reflective of the organisational need at a point in time. Most of the short-term targets and risk mitigation strategies to address this risk have now been implemented. The challenge for ACC in the longer term lies in shifting focus from disclosure breach avoidance and associated risks to enhancing Privacy maturity over all aspects of the management of personal data. This will be required if ACC is to be recognised as an exemplar in the New Zealand public sector and to mitigate risks associated with the broader Privacy context.

ACC's Privacy policies specific to each of the 12 Information Privacy Principles (IPPs) are comprehensive, easy to understand and readily available to all staff. The IPPs are well known by staff and the Privacy Team provides additional advice when required.

However, Privacy-specific preventative and detective controls are strongly focused on IPP-11 (Disclosure). There is far less focus on the other IPPs. This is understandable given the context in which ACC was operating at the time in which the disclosure-specific controls were introduced. In order to keep enhancing the maturity of the overall programme of Privacy management, the focus will now need to widen to encompass each of the other IPPs. A life-cycle approach should be undertaken, whereby risks at all points in the flow of information are identified and appropriate controls put in place to mitigate these. This should be a key component of Shaping Our Future.

Since the initial review, managing personal information has received significant public interest and a considerable media profile, and New Zealand organisations in the public sector and the health and insurance sectors have continued to develop their programmes. In addition, the Government has established a Government Chief Privacy Officer, to build capability across the public sector. ACC had significant risk to manage, including rebuilding public trust and confidence and, therefore, it has invested significantly more in resourcing its Privacy programme and in the programme of work undertaken to address the findings of the 2012 Independent Review. The development of the Privacy Strategy, the focus on culture, the monitoring and reporting of Privacy breaches and the level of governance and oversight are all areas where ACC has developed leading practices from which other organisations can learn, and ACC is open in its approach to sharing its practices.

As with the previous review, ACC's business processes and systems have yet to be re-engineered based on Privacy by Design. Meanwhile, ACC has made a significant investment in preventative business processes and systems to address access requests and prevent disclosure of personal information. This investment is unique and significantly more than that of other organisations.

Global organisations are using business model transformation and technology to ensure personal information is managed more effectively. Also, they are focusing on customer engagement, and looking at consent management process and accessibility through online channels. As ACC embarks on its transformation programme, it will be able to 'design in' best practice.

WE RECOMMEND that the Privacy Strategy should be reviewed and enhanced, with a shift in focus to be integrated with, and reflective of the aims of, the Shaping Our Future programme.

3.2.1 Stakeholder engagement

At the time of the 2012 Independent Review, there was a discrepancy between the views of internal and external stakeholders regarding what was important when dealing with customer personal data:

"STAKEHOLDERS REPORTED, DURING THE CURRENT REVIEW, THAT THERE HAS BEEN AN INCREASE IN THE LEVEL OF TRUST IN ACC WHERE PREVIOUSLY IT WAS LOW."

There is a general consensus that ACC is now more willing to engage with external stakeholders. This has been evident through the consultation process with the new ACC 6300 consent form and the Executive team attending Voice of the Customer meetings. However, stakeholders were unaware of the changes ACC has made to its Privacy management practices as a result of the recommendations of the 2012 Independent Review, as they are consulted/engaged only on an 'as needed' basis.

Stakeholders continue to have varying experiences of how personal information is managed. This can differ between case managers in a branch, between branches and between regions. Stakeholders feel this is reflective of inconsistent Privacy management practices across ACC and question what assurance processes are in place to ensure processes are implemented effectively and consistently.

In our assessment, the issue with stakeholders is reflective of an opportunity to improve engagement and communication practices with them, rather than of the actual status of Privacy practices in ACC at the current time.

ACC acknowledges that lessons have been learned through the process of developing and promulgating the Privacy Strategy. One of these lessons is around the level of stakeholder engagement (both internal and external) that is required in order for the Strategy to reflect stakeholder needs fully. We understand that more in-depth stakeholder engagement is planned for inclusion in the next redevelopment of the Strategy.

There is opportunity for ACC to take a more proactive approach to engaging, communicating and consulting with external stakeholders to ensure these processes are meaningful and enable timely and appropriate communication of Privacy management changes. This should include not only consulting with stakeholders for input in a timely manner, but also communicating how that input is included and what the outcomes are. There is, currently, no feedback mechanism from ACC to provide stakeholders with visibility over the effectiveness of implemented changes (see section 3.4.1 regarding recommendations for improving stakeholder engagement).

ACC is involved proactively in ongoing discussions with the Office of the Privacy Commissioner and the Government Chief Privacy Officer, and works with the Privacy Leadership Forum and other All-of-Government forums. This reflects ACC's desire to be, and to be acknowledged as, a leader in Privacy management.

WE RECOMMEND that ACC proactively engages and consults with stakeholders in relation to the Privacy Strategy and other relevant matters.

3.3 Culture

Privacy management across ACC has been enhanced with dedicated staff committed to continually improving and enhancing Privacy processes.

There is a high level of Privacy awareness across ACC, especially in the front-line network and offices. The cultural shift is particularly marked, and it is clear that ACC has managed to make Privacy an integral part of the staff work ethic and focus in a relatively short time frame.

This has been achieved through a combination of: acknowledging the impact on staff of the 2011 breach and implementing approaches to ensure something similar does not happen again; developing and maintaining Privacy training; communicating with staff in a way that includes a focus on why changes are being introduced; and introducing mandatory processes that require acknowledgement of the importance of Privacy.

There has been strong support and communication from the Board, Executive and Privacy Team to keep ACC's Privacy Vision 'top of mind' for staff. The Vision is well known by staff.

ACC'S PRIVACY VISION: "PERSONAL INFORMATION IN OUR CARE WILL BE MANAGED AS CAREFULLY AND RESPECTFULLY AS IF IT WERE OUR OWN".

The acknowledgement of the importance of Privacy across all levels of staff and management represents a significant improvement when compared with the findings of the 2012 Independent Review. The cultural shift supports the effectiveness of the business process changes that have been undertaken at the same time. This is important as Privacy risk is managed currently by people, manual processes and some system enhancements, rather than by a systematic re-engineered approach.

The next phase is to embed Privacy by Design within ACC's Shaping Our Future transformational programme:

95% of respondents to the survey Agree or Strongly Agree that, overall, ACC demonstrates a culture of respect for the personal information it holds and treats it appropriately.

> “THE CORPORATION’S TOP PRIORITY IS TO PROVIDE HIGH-QUALITY SERVICES TO CLIENTS AND LEVY-PAYERS. THE AIM IS TO SHIFT THE CULTURE OF THE CORPORATION FROM A PREOCCUPATION WITH PROCESS COMPLIANCE TO ONE OF LOOKING AT THINGS THROUGH THE EYES OF THE CUSTOMER[7].”

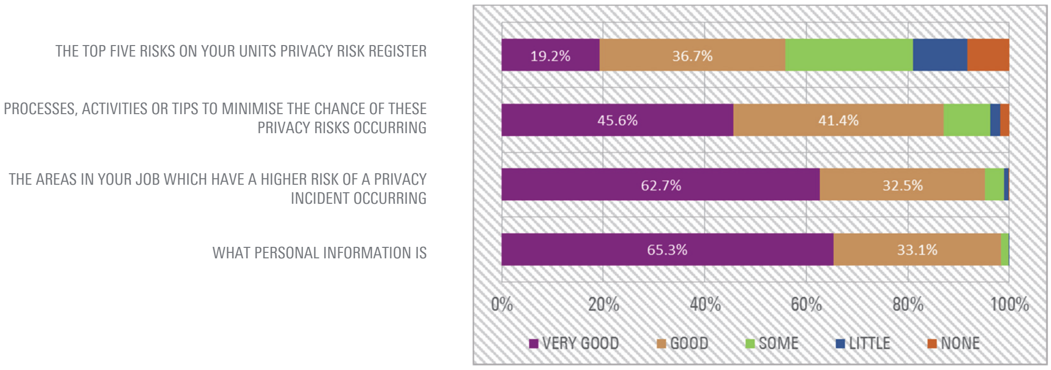
ACC conducts a Gallup survey of staff[8], which asks participants to rate their agreement with the statement *“Privacy and confidentiality are built into everything we do at ACC”* on a scale from one to five. There is generally strong agreement with this statement from staff:

GALLUP SURVEY	2013 result	4.44/5
	2014 result	4.54/5

Staff members who were part of ACC at the time of the 2011 breach are highly aware of Privacy risk and the impact the breach had on them personally. ACC has implemented Privacy and on-the-job training that has had a similar desired effect for newer staff. The overwhelming consensus from all staff, regardless of their length of service with ACC, is that personal information management is key to the organisation and to them doing their jobs well.

Members of staff have good, perceived understanding and awareness of Privacy, as illustrated by their answers to the following question, set out in the graph below:

> “HOW WOULD YOU RATE YOUR UNDERSTANDING/ AWARENESS OF EACH OF THE FOLLOWING?”



A future challenge for ACC will be maintaining cultural awareness and understanding of the importance of Privacy among new and existing staff.

Behavioural competencies for staff now include Privacy performance measures. As a result, Privacy-related issues now have consequences for individual roles and accountability is clearly articulated. However, there is a fine balance to be maintained between encouraging open and proactive reporting of breaches and related issues, and managing individual staff performance through the performance management process when Privacy concerns arise. In order to encourage open reporting, it is important to emphasise that performance implications will depend specifically on whether or not Privacy-related processes were being followed at the time of the issue, rather than on problems arising purely as a result of ‘human error’.

[7] *Source:* ACC’s Statement of Intent 2013–2016

[8] 2,844 staff members participated in the Gallup survey in 2014

A tool to boost staff engagement could be to place a focus on rewarding positive Privacy-related practices in order to ensure the focus on Privacy is a balanced approach. Some sites visited had started implementing rewards for identifying near misses, and the feedback from staff in these instances was positive. Consistency across the claims network in this area could help to enhance a positive Privacy culture.

Additionally, some staff spoken to during site visits (and some comments made in the free text field of the survey) acknowledged a perceived discrepancy between key performance indicators (KPIs) that consider quality (including the appropriate management of personal data), and those that assess quantity or volume (for example, the number of claims processed per day). Staff advised that it is sometimes difficult to understand how to manage the apparent conflict between being assessed on the speed of processing a claim, and conducting careful and largely manual, Privacy checks. This, at times, results in frustration for the staff concerned.

WE RECOMMEND that ACC investigate the relationship between quantity and quality KPIs for staff, and how this influences Privacy performance.

The survey also reflected other opinions of individual staff, which will continue to provide a challenge for ACC in embedding a consistent culture across a large and diverse organisation. While staff members generally hold a positive view of Privacy management at ACC, some comments were received in the survey results that reflect mixed views. Some of the commentary included the following themes:

- Difficulty in applying a quality focus to already-high workloads (i.e. a perception that proper management of personal information requires additional time and processes)
- A perceived 'overload' of Privacy information and processes
- The notion that the focus on Privacy is 'over the top'.

It is apparent from the survey, and from people spoken to during this review, that the positive view of the Privacy culture at ACC far exceeds the negative. A culture that respects Privacy, and is acknowledged as such, is particularly important in the absence of fully mature and Privacy-focused systems and processes.

3.4 Accountability

At the time of the 2012 Independent Review, ACC leadership did not have specific responsibility for Privacy and, as a result, there was no clear and consistent focus, and insufficient requirements for reporting to Board level. Staff roles and responsibilities for Privacy were not clearly defined, and expectations were neither apparent nor measurable. Additionally, there were no processes in place to evaluate third parties against ACC's expectations in terms of Privacy management. The report recommended that ACC clearly identify and document roles and responsibilities, and implement a set of key criteria for driving and assessing ACC's Privacy management performance for all staff.

Since the review, Privacy-related competencies have been incorporated into KPIs and objectives. The Executive has consistently communicated the Privacy message through the Privacy Team to people managers, and breaches must be reported formally to the Board and Executive.

The Chief Privacy Officer (recently included in the role of the Chief Governance and Strategy Officer) is a member of the Executive. Within individual teams throughout ACC, people managers are responsible for management of personal information and Privacy risk. A responsibility guide for managers has been developed and roadshows regarding their responsibilities are undertaken by the Privacy Team.

Projects are required to undertake a high-level Privacy Threshold Analysis, followed by a full Privacy Impact Assessment if results indicate the need. The Information Technology Team also performs an accreditation process to ensure Privacy risks have been adequately considered within the systems development life cycle. To date, few have been completed, although the numbers are increasing.

Survey results show that the Executive and staff generally acknowledge that Privacy is everybody's responsibility.

3.4.1 Third-party providers

ACC frequently receives personal information about clients from, and makes it available to, a large number of third-party providers in order to assist with rehabilitation of the client. These providers include DHBs, GPs, mental health specialists, FairWay Resolution (formerly Dispute Resolution Services Ltd), Child Youth and Family, vocational providers, accredited employers and many other medical professionals.

ACC's focus over the last two years has been on the aspects of personal information management that are of a higher immediate risk and are within ACC's ability to control (i.e. internal staffing and business processes). This has provided for short-term solutions (manual and some system development) and an improvement in overall mitigation of the risk of disclosure breaches. However, less focus has been placed on external or third-party providers who have access to ACC data, or provide, personal data to ACC. This is due to the perceived difficulties of exerting control over a large number of non-contracted parties, though these parties are covered by their own professional codes of practice.

A Privacy clause has been added to all new contracts. However, the majority of providers come under the Cost of Treatment Regulations and, therefore, are not contractually bound by ACC. There remains a risk to ACC's reputation due to disclosure breaches that occur as a result of incorrect data being provided to ACC by third-party providers.

The transfer of highly sensitive personal health information from ACC to providers is also an area of risk. Many business units have a range of transfer mechanisms in place such as courier, email, other electronic transfer and delivering in person; these imply a residual risk of information being in possession of an unintended recipient. As part of Shaping Our Future, opportunities exist to implement secure document-transfer systems to reduce this risk.

Alternative operating models that seek to minimise the risk of inaccurate data within the wider third-party provider community, and ACC's role in the sector, need to be considered and clarified.

There is a perception within ACC that it is not able to compel these third parties to meet ACC's information management requirements but, rather, can only influence them. In an attempt to influence these providers, and ensure they have appropriate personal information management practices in place, ACC is increasingly communicating its expectations through training sessions and an Information Privacy Pack available on the website. ACC has engaged with two key stakeholder groups, Advocate Representation Group and Consumer Outlook Group, on privacy-related matters. While these groups represent important stakeholders they are a subset of the wider stakeholders with which ACC engages, and there is potential for the feedback to be limited to the views of these representative groups. Ensuring the best approach to obtaining the wider stakeholder perspective should be considered as ACC develops its stakeholder engagement framework.

Privacy issues result from this information transfer when incorrect information provided by another party is used by ACC, or Privacy breaches arise from other parties dealing with clients on ACC's behalf, due to a lack of robust Privacy processes. The reputational and related risk of Privacy breaches by third parties often still rests with ACC.

Related to this issue is the lack of a centralised Privacy contact within ACC for providers. Currently, various groups of providers have different channels for raising a Privacy issue/ potential Privacy breach, which may lead to inconsistencies in how these are reported. This problem would be vastly reduced if a relationship model existed that detailed a central contact point for providers within ACC concerning Privacy matters.

Currently, the responsibility for provider auditing sits with the clinical review team. Reviews are carried out on an ad hoc basis, are issue based and reactive, often after a problem has arisen. ACC needs to consider how compliance and assurance are obtained over third-party provider Privacy systems and processes.

We recommend that ACC develop a programme of work around management of third-party providers and stakeholders going forward, with visibility at the Executive level. Specifically, the recently developed Stakeholder Engagement Framework should be signed off by the Board and Executive, and the scope of this framework should include coordinated interaction with Advocate Representation Group and Consumer Outlook Group. The role of ACC in the health sector needs to be clarified, and a roadmap detailing how to achieve this clarification should be developed. In order to improve the personal information management practices of regulated providers, communication with health providers needs to be consistent and focused on Privacy. The conferences of health sector professional bodies could be useful fora at which to communicate ACC's Privacy message to a large number of providers.

WE RECOMMEND that risk management, including assurance, in relation to third parties' information management processes be enhanced, including:

a. Ensuring privacy engagement is considered during the development of ACC's wider stakeholder engagement framework, including confirming ACC's role under respective relationships as influencer or enforcer of privacy practices.

b. Reviewing the framework through which ACC engages stakeholders in development of projects or policies that will directly impact on them to ensure that input is balanced and representative.

c. Consideration of a secure document transfer system for third parties or alternative operating models.

d. Assurance over third parties' personal information practices.

3.4.2 Three lines of defence

ACC has adopted an organisation-wide risk and control framework (three lines of defence) based on international best practice. The objective is to strengthen risk management with each line providing ongoing feedback on the effectiveness of Privacy management and the system of internal control over Privacy:

First line: The front-line business functions should continually identify risk and business improvement actions and implement effective controls.

Second line: Privacy and risk activities should be integrated with the wider system of internal control as part of an efficient, effective assurance framework.

Third line: Internal audit should have a systemic and disciplined approach to evaluate and improve the agency's Privacy risk management, control and governance processes.

ACC has focused on enhancing the three lines of defence. This has been achieved through the introduction of new detective controls in the form of new and altered business processes and teams (First line). Identified breaches and near misses are reported to the Privacy Team, which undertakes root-cause analysis (Second line) that enables initiatives to fix the issue. Independent Privacy-related assurance reviews and other reviews that incorporate Privacy components within scope (Third line) provide Privacy-related assurance.

Gaps still exist in the First line:

- Risk identification, monitoring and reporting processes are not applied consistently across ACC.
- Business improvement actions are not applied consistently across the organisation, with some teams implementing additional processing checks and processes.

In the Second line:

- The risk management function in respect of Privacy requires improvement (as detailed in section 3.1.1 of this report).
- The compliance function in respect of Privacy needs to be strengthened. A compliance framework is being developed and is to be deployed within the organisation. A formal programme of compliance and relevant reporting to ensure that Privacy processes are being followed would enhance assurance and confidence in the reduction of risk. Currently, reliance is placed on monitoring by team leaders and managers, rather than on dedicated Second line of defence monitoring. An approved, evidence-based compliance programme and plan should be in place, linked to the annual attestation process. This should be a rolling process based on risk and linked to the other Second line of defence functions/activities.

One of the elements that may inform an effective Privacy compliance framework is the existing annual attestation as to compliance with legislation completed by each part of ACC. This includes compliance attestations regarding the Privacy Act 1993 and the Health Information Privacy Code 1994.

For the Third line of defence:

- While, more recently, Privacy considerations have been included within the scope of relevant assurance reviews, the coordination and communication between the Privacy Team and the Assurance Team with regard to targeted/risk-based testing and reporting back could be improved.
- Given that Privacy is deemed to be the number-one risk for ACC by the Board and Executive, coordinated assurance across all the lines of defence and reporting to the Board Audit and Risk Committee could be enhanced.

WE RECOMMEND that the three lines of defence model be embedded in respect of Privacy, including enhanced Second line of defence functions of risk management, compliance and quality assurance.

Explicit assurance over Privacy-specific business processes and design, coordinated and integrated across all three lines of defence, and provided as a result of comprehensive risk management processes, could be used to provide an overall Privacy assurance summary to the Board.

WE RECOMMEND that a consolidated overview of Privacy assurance results should be reported to the Executive and Board, at appropriate intervals.

3.5 Privacy programme

ACC has a Privacy Team that, in the New Zealand context, is large. The team is focused specifically on improving Privacy management practices and Privacy maturity across ACC. This dedicated Privacy Team has achieved significant results and has kept Privacy 'alive and well' within the organisation.

The team drives regular messaging and communication on Privacy-related topics including monitoring, reporting and root-cause analyses of breaches.

The team provides Privacy advice to front-line staff with regular site visits, the development of Privacy-related policies and a training material. It provides Privacy reporting to the Board and Executive of statistics obtained via the Privacy Breach Reporting tool. The tool also assists with root-cause analysis, which drives process and system enhancements.

An externally reported Personal Information Management Index (PIMI) has been utilised as a yardstick to assess Privacy maturity. ACC intends to move to assessment against the public sector Privacy Maturity Assessment Framework to ensure that there is appropriate focus on the other Privacy Principles in addition to disclosure.

A model of Privacy champions was implemented initially, although the appointment and application of these champions was not consistent. This model has been formally disestablished, and the responsibility has been transferred to people managers. This is a positive shift that ensures the appropriate skill set, training and authority for the position exist and is consistent across the claims management network. Additionally, people managers are responsibility for updating the Privacy Risk Registers and communicating all Privacy process changes to their staff.

3.5.1 Personal Information Inventory

ACC has not undertaken a comprehensive process to identify all personal data it holds or to which it has access, where this data is held, the information flows and who has access to them, and for what the information is used. A Personal Information Inventory is considered essential for properly identifying all risks associated with that information and those processes, and is recommended as a critical input into the development of Shaping Our Future.

A Personal Information Inventory is an integral step in fully understanding an organisation's Privacy risks and, therefore, informing the Privacy Team's work plan. Documented data flows of personal information collected, used, stored and disclosed for all purposes will provide sufficient detail to inform decisions and actions.

In order to properly address Privacy risks, ACC must first identify:

- The types (sensitivities) and quantities of personal information held.
- How personal information is accessed and used.
- Where and how the information is held.
- The associated information flows.

Risks associated with particular types or quantities of information, users or clients may then be identified and properly assessed.

WE RECOMMEND that a full (organisation-wide) Personal Information Inventory be undertaken. This should inform ACC's strategic and operational Privacy risk assessments and reporting, the Privacy Strategy and the Privacy Team's work plan, and would be a critical input to the Shaping Our Future programme.

3.5.2 Privacy performance measurement and KPIs

Breach detail in the context of 'risk' or 'severity of harm' is not reported explicitly in ACC's external accountability documents. This has been incorporated recently into the reporting to the Board and Executive, and includes a distinction based on risk, with any medium or high risks identified, including the rationale for the risk rating. The current definition does not distinguish breaches based on materiality (for example, those based on sensitivity of information, the number of people involved, other indications of a systemic problem, etc.). Potentially, this does not allow for prioritisation of resources for investigation or resolution, or for reporting to the Board and Executive based on risk. Without assessment of the potential severity of harm, breaches reported cannot be differentiated to allow comprehensive assessment of the actions taken.

While the definition is broad in the context of breach definition, and was appropriate for ACC for the point in time, it is narrow in the overall measurement of managing personal information (i.e. it does not consider measurement across all aspects of the information management life cycle).

The Privacy Act is being reviewed and the proposed changes include assessment of whether a breach is 'material'. This requires assessment of the sensitivity of information, the number of people involved and any indications of a systemic problem. A second tier of mandatory reporting is proposed for more serious breaches where there is a real risk of harm.

It appears likely that the current review of the Privacy Act will result in a broader focus on breaches of the other Principles of the Act and, therefore, requires consideration by agencies of a corresponding broader range of risks and issues encountered.

With the probable upcoming changes to the Privacy Act regarding mandatory reporting, and the Board's ambitious goal of zero breaches, it is a good time to reconsider the internal and external breach reporting processes. The Privacy Team should revisit the definitions of breach and near miss, including 'other party data loss', breaches of each of the Principles of the Privacy Act, and the level of risk based on quantity and sensitivity of the information. We recommend that the Privacy Team, in conjunction with the Board, develop the Privacy performance measurement framework, including relevant KPIs, to assess Privacy performance.

The Privacy Breach Reporting tool is available to all staff and managers, and is well known throughout ACC. It has the capability for staff members to run reports relevant to their business units or locations, in order to analyse trends and communicate common areas of concern to their colleagues.

This tool is used by people throughout the organisation to report Privacy breaches and near misses to the Privacy Team. The items reported via the Privacy Breach reporting tool channel are the key inputs to the Privacy Team's breach reporting statistics and root-cause analyses. Statistics, root causes and any breaches of particular interest are reported to the Board and Executive.

The Privacy Team actively encourages use of the tool.

The majority of the items reported using the tool are breaches rather than near misses and the majority of these are disclosure breaches. This is beginning to change and some breaches of the other Information Privacy Principles are reported now as well.

When staff members report breaches using the Privacy Breach Reporting tool, they rate the potential impact and likelihood of the issue recurring and categorise the cause (e.g. "attached wrong document to email"). The number of breaches rated as high risk is included in summary reporting to the relevant management teams. Breach categorisation and risk rating inform the root-cause analysis process undertaken by the Privacy Team.

ACC should revisit the current definition of a breach, in consultation with the Office of the Privacy Commissioner or the Government Chief Privacy Officer, to ensure it not only continues to meet ACC's needs for root-cause analysis, but also provides for more comprehensive reporting and assessment, both internally and externally.

The Privacy Team also reports on relevant (upheld) complaints to the Privacy Commissioner. There now exists a strong link between the Privacy Team and the Office of the Complaints Investigator, with all complaints made under Right 7 of the Health Information Privacy Code automatically flagged to the Privacy Team.

Currently, reporting to the Board and Executive does not include 'other-party data loss' breaches unless these are of a high profile or otherwise of particular interest. 'Other-party data loss' breaches are those where either the breach originated at a third party, or a third party has provided incorrect personal data that has resulted in a breach (e.g. an incorrect address).

WE RECOMMEND that ACC develop a Privacy performance measurement framework, including relevant KPIs, to assess Privacy performance. The framework and KPIs should reflect the developing maturity of Privacy management practices and, in particular, the changes from a disclosure breach focus, to include:

a. Consideration of all of the Principles of the Privacy Act

b. Categorisation based on risk

c. Assurance that 'other-party data loss' is part of the Board/Executive reporting processes.

3.5.3 Privacy Team's work plan

The Privacy Team's work plan is an internal team document that is used to record workload and responsibility for certain projects and tasks and, to a limited extent, to plan future work. The team deals with issues as they arise and, in conjunction with appropriate areas of the business, undertakes root-cause analysis of known Privacy breaches and near misses, and assist in identifying and implementing solutions to reduce the risk of such issues recurring.

There is no formal link between risk and a systematic, comprehensive future-focused Privacy work plan.

In an ideal world, any organisation would have unlimited resources to apply to mitigating Privacy risk to a level at which it is impossible or highly unlikely for a breach to occur. In the absence of unlimited resources, a Privacy Team work plan based on risk is recommended. In addition, it would inform any assessment of resourcing required to support the Shaping Our Future programme.

There is an opportunity to enhance and improve the Privacy work plan that considers:

- Areas of risk identified through a comprehensive Personal Information Inventory
- Potential non-compliance with the other 11 Privacy Act Principles (currently, it is focused on disclosure)
- Integrated Privacy risk management throughout the organisation.

The Privacy Team should develop a proactive Privacy work plan that is linked to the Privacy Strategy experience in sync with Shaping Our Future.

WE RECOMMEND that the Privacy Team's work plan be redeveloped to reflect prioritisation of Privacy Team activities based on risk (as identified by the comprehensive Personal Information Inventory).

3.5.4 Training

The Privacy Team has implemented a Privacy training regime that is refreshed regularly, and a process for monitoring completion. Privacy training is mandatory for all staff and the online modules are well regarded by users. The issue of Privacy is included in staff and manager induction, and all staff members complete an annual e-learning refresher module, which ensures Privacy is kept 'top of mind'. On top of the generic training for all staff, branch and service centre managers conduct their own training to ensure Privacy process changes are understood and any additional training required for specific roles is completed. The Privacy Team is perceived as a valuable resource, and the Privacy advisors for each region are visible and well regarded by staff. Additionally, the Privacy home page on the intranet has a substantial collection of resources that all staff can access.

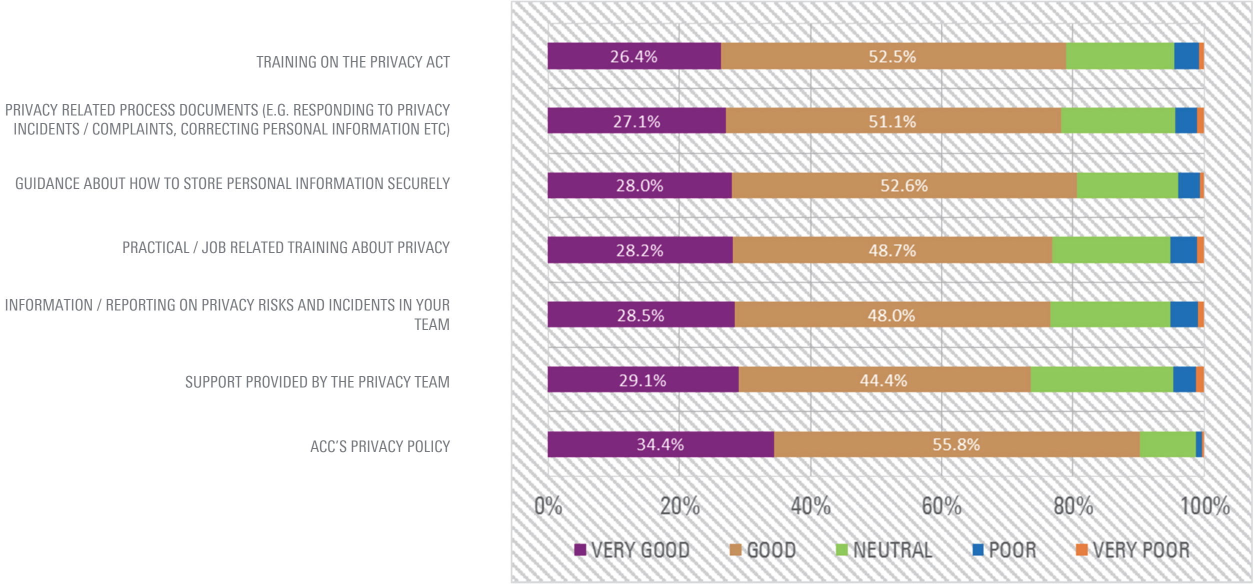
95%

of respondents to the survey have completed Privacy training.

The training has been effective in raising the profile of Privacy and giving staff an understanding of 'the basics' of Privacy. Also, it has also allowed the Privacy Team be more visible throughout ACC, and the majority of staff are aware of whom to contact with queries.

The Privacy Team is well respected by staff and management in terms of the advice, communication and training it provided.

PLEASE INDICATE HOW ADEQUATE YOU BELIEVE THE FOLLOWING ACC PRIVACY RESOURCES ARE:



Individual front-line teams throughout the organisation also undertake on-the-job training for new staff, which emphasises the appropriate management of personal information.

3.6 Business processes and systems

Across the organisation, business processes and systems have been reviewed and updated in response to Privacy risk. In particular, disclosure breaches are mitigated by additional checking processes and access risks are mitigated by increased education.

The technology that ACC uses is essentially the same as that which was in place at the time of the 2011 breach. This includes client data systems, email, faxes and the use of spreadsheets.

ACC has implemented a dedicated Privacy programme of work as part of the strategic change portfolio. The programme has led to implementation of a range of checking processes (tactical and some system enhancements) for most outgoing data and communications in order to mitigate the risk of disclosure breaches. Many of these checking processes are manual and can be intensive and time-consuming.

When sending attachments externally by email, staff are required to confirm that the entire email contents are appropriate before the system will send. Anecdotal evidence suggests, however, that this has become a 'tick box' exercise and is not continuing to add value.

The use of spreadsheets for collating and reporting data is an ongoing area of risk for ACC. Spreadsheet use is considered inherently risky due to: the potential for unknown data to be accessible (e.g. through pivot tables); the potential for identifying individuals through review or analysis of the data; and the ease with which these can be sent to inappropriate recipients. We were informed that the use of spreadsheets has been reduced; however, many are still used as bases for reporting.

Checks are usually in the form of additional required steps within processes. Although these may have reduced the risk of disclosure breaches, they also increase the time required for processing, and 'work-arounds' have been introduced by some individuals or teams in order to meet quantity KPIs.

In addition to the newly introduced checking systems being primarily manual, the majority of ACC's systems of evaluation and management of claims also rely on human intervention (with the exception of low-risk, low-value claims). This reflects the environment in which ACC operates, but provides the opportunity for human error when staff members are dealing with the personal data of clients.

Manual processes also increase the time required for processing.

The majority of these checking processes involve staff checking files, letters and, at times, emails prior to these being dispatched:

- Significant investment and resourcing at the front line (e.g. the Client Information Team (CIT)) is focused on cleansing historical documentation in order to prevent potential breaches.
- All outgoing emails with attachments require confirmation from the sender before they are released.
- Spreadsheets are still used for reporting but staff members are aware that only one spreadsheet or one claim file should be open at a time.

While it is understood that these processes may have resulted in many potential breaches being prevented or identified before they occur, these are considered to be neither efficient nor sustainable over the long term.

Shaping Our Future is critical to enable ACC to address its interaction with clients, providers and levy-payers, and to design systems to address the various manual processes and current system limitations. A core part of understanding the requirements will be to ensure that all touch points with clients, providers and levy-payers are identified. The Shaping Our Future programme provides an ideal opportunity to optimise Privacy management and for ACC to become an exemplar in New Zealand Privacy management.

3.6.1 Privacy by Design

Shaping Our Future is the organisation's overarching transformation programme that aims to improve the public's trust and confidence in ACC, and empower and engage staff to deliver great service. The programme aligns with ACC's five strategic intentions for the next four years, which are: Privacy; injury prevention; customer experience; financial sustainability and governance; and trust and confidence.

Privacy by Design is one of the Principles of Shaping Our Future. Privacy by Design is an approach to protecting Privacy by embedding it into the design specifications of technologies, business practices and physical infrastructures. Privacy by Design is considered to be good practice and to be effective in reducing Privacy risk. Information technology is a foundation pillar of Shaping Our Future and will be a key enabler when ensuring the personal information in ACC's care is secure.

Privacy by Design involves designing technology, processes, training, documentation and all aspects of a system with effective Privacy management as a core component. Privacy is embedded into system/process design and, thus, the risk of Privacy problems is reduced.

Shaping Our Future provides an ideal opportunity for ACC to embed Privacy by Design or Privacy by Redesign throughout the organisation. It is crucial that Shaping Our Future, as a transformation programme, develops a formal plan to ensure the Privacy by Design principle is embedded throughout the organisation in order to achieve optimal Privacy maturity.

> "SHAPING OUR FUTURE IS A PROGRAMME INITIATED TO HELP TO MAKE ACC FIT FOR THE FUTURE – TRANSFORMING THE ORGANISATION'S ABILITY TO DELIVER GREAT OUTCOMES FOR NEW ZEALANDERS THROUGH ITS VALUE PROPOSITION, OPERATING MODEL AND TECHNOLOGY. THIS WORK WILL PROPOSE HOW BEST TO ORGANISE WHAT ACC DOES, AND HOW IT DOES IT, TO BETTER MEET THE NEEDS OF CLIENTS, LEVY PAYERS AND PROVIDERS. THIS MEANS MAKING ACC MORE RESPONSIVE, MORE TRANSPARENT, EASIER TO DEAL WITH, DIGITALLY ENABLED AND FIT FOR PURPOSE WITH EMBEDDED PRIVACY FOCUS FOR THE COMING DECADES." [9]

ACC intends that the recommendations made in the 2012 Independent Review relating to Business Processes and Systems will be implemented by the Shaping Our Future programme. These have not been actioned fully, to date; they include the following:

- Undertake an end-to-end review of the claims management process, including Electronic Claims Management System (EOS) functionality and other information management systems.
- Re-engineer processes as needed, adopting Privacy by Design and/or Privacy by Redesign.
- Review processes by which clients and others about whom ACC holds personal information are able to access, review and challenge, or even update, that information… with a view to implementing an online portal for clients.
- Review information-exchange practices with employers and ACC health service providers, supported by appropriate ICT services and processes.
- Undertake a systematic review of all business processes and create compilations of personal information about clients other than the actual EOS records
- Develop and implement a strategy to reduce reliance on the use of email as a business tool.

WE RECOMMEND that the approach for Shaping Our Future in addressing business process and system Privacy risks, issues and recommendations, and enhancement of Privacy maturity across all of the Information Privacy Principles be confirmed. This should be based on a Privacy by Design approach. The Privacy Team should engage proactively with the Shaping Our Future programme to ensure the Privacy pillar of the programme is reflected appropriately in programme planning, design, implementation and resourcing.

[9] *Source:* ACC 2013/14 third quarterly report, 31 March 2014

Appendix 1: Review Terms of Reference

The objectives of this review were to:

- Assess ACC's adherence to, and implementation of, its Privacy strategy. The assessment was undertaken with consideration of the following:
  - Compliance with relevant legislation, including the Privacy Act 1993.
  - Adherence to best practice, including the recently published Privacy Maturity Assessment Framework (published by the New Zealand Government).
  - Appropriateness in terms of the risk related to the nature of the client data/information maintained by ACC.
- Compare progress against that of external organisations that were consulted in the original review.
- Determine ACC's progress against the recommendations.

Our work was undertaken in accordance with the scope and approach outlined in the proposal and included documentation review, interviews, surveys, workshops and validation of the information provided. It included coverage across ACC teams, including the Privacy team, and geographical locations including the corporate office and network.

Appendix 2: Detailed Approach to the Independent Review

2.1 Review of documentation

The Independent Review Team familiarised itself with ACC's role and functions, its regulatory obligations, organisational structures, and policies and procedures for handling personal information. Documentation detailing changes to people, process and policy since 2012 was reviewed also. Information obtained during this process informed the targeting of further work, including the interviews conducted.

2.2 Interviews

The Independent Review Team conducted over 150 interviews with ACC staff members, covering a comprehensive range of business units at all levels of the organisation. This included areas considered to have greater access to personal information due to the nature of their functions or the volumes of claimant information handled. Interviews were conducted in the Corporate Office, Hamilton Service Centre, Dunedin Service Centre, Counties Manukau Branch, Palmerston North Branch, Christchurch Branch, Sensitive Claims Unit and Treatment Injury Centre.

Interviews at the Corporate Office included those with members of the Executive and with members of staff from various levels of the Privacy Team, and the Procurement, Finance, Clinical Services, Risk and Actuarial, Legal, Injury Prevention, Research, Assurance Services, Enterprise Planning and IT, People and Communications departments, and from the Office of the Complaints Investigator.

2.3 Survey

A survey was sent to all ACC staff members, in order to obtain information on employee knowledge and understanding of:

1. Privacy in general (i.e. what it means to respondents)
2. How Privacy is managed within their roles
3. How ACC approaches Privacy management in general.

Questions were designed to obtain input from throughout the organisation on the key themes of: Culture; Leadership; Resources; Implementation of the Information Privacy Principles; Incident Management; and Risk.

Responses to the survey questions were received from 2,020 staff, giving a response rate of 56%. These responses informed the Independent Review Team's interview schedules and overall analysis.

2.4 Consultation with external stakeholders

A consultation session was held with representative members from the Voice of the Customer programme, including the Advocates Representation Group and the Consumer Outlook Group. The objective of this session was to obtain:

1. Their views on:
   a. The changes ACC has made over the last two years in its approach to personal information
   b. The impact that changes to culture, policy or practice have had on external stakeholders, if any
   c. The current status of Privacy management within ACC
   d. Any particular areas of good practice or concern with regard to the management of personal information
2. Information on any involvement/consultation those groups or individuals have had with the development of key policy or practice/approaches, including the Privacy Strategy
3. Accounts of any current or recent interactions with ACC regarding personal information management.

2.5 Comparison with other organisations

A comparison of ACC's Privacy management practices against a selection of other agencies was undertaken, including those exhibiting national and international best practice. This included assessing how ACC's culture compared to the risk management and compliance cultures of similar Privacy and public-sector organisations.

Appendix 3: Glossary of Terms

GLOSSARY TERM	DEFINITION
ACC	Accident Compensation Corporation
BREACH	Throughout ACC, this is defined commonly as the unintentional disclosure of personal information to a third party
CIT	Client Information Team
DHB	District Health Board
EOS	Electronic Claims Management System
IPPS	Information Privacy Principles of the Privacy Act 1993
KPI	Key Performance Indicator
KPMG	A New Zealand partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative
NEAR MISS	Throughout ACC, this is defined commonly as the discovery of a Privacy breach before it is disclosed externally
PIMI	ACC's Personal Information Management Index
SOF	Shaping Our Future

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.