ACC Privacy Maturity Plan 2016/17

1 Purpose of the ACC Privacy Maturity Action Plan

Effective management of our customers' information is an essential element in creating a unique partnership with all New Zealanders. Our customers need to have confidence that their personal information managed by ACC is collected appropriately, stored securely and only disclosed with appropriate authority and that they can access it when they need it. Better management of personal information across the information lifecycle is fundamental to delivering on our Vision and Values, as well as, improving customer outcomes, and building public trust and confidence.

ACC collects and uses personal information from a large number of people and entities, including clients, providers and business customers. Our relationship with personal information is complex – some information is compelled by law (eg through the collection of levies or providing medical records for a claim) and some is volunteered (eg when a client submits a claim or a provider seeks payment for services). Some information comes directly from our customers and some comes to us through third parties. We then use that information to make decisions about a person's individual circumstances and in some cases we need to share it with others. Given this complex set of responsibilities, a wide range of customer expectations can arise.

But fundamental to all of our relationships is the need for our customers to have confidence that their personal information is collected appropriately, stored securely and accurately, only disclosed with appropriate authority and that they can access it when they need it. Building that confidence is an essential element in ACC creating a unique partnership with all New Zealanders.

Focus for next four years - embedding and maturing our approach to privacy

As part of putting the customer at the core of our services and building customer confidence, ACC needs to continue to mature from a culture of risk management to our developing culture as responsible information stewards. ACC's Statement of Intent 2015-2019 promises we will *'Improve the way we protect our customers' personal information'* to ensure:[1]

- Our people respect and protect customer information as if it were their own
- Processes and systems are designed to minimise the possibility of privacy breaches occurring.

This four year action plan formalises our approach to build on our progress and continue to improve our privacy maturity between now and 2020. It will embed a culture of information stewardship that aligns with the other changes we are making to improve our customers' experiences.

[1] ACC Statement of Intent 2015-2019

2 Building our Privacy Maturity as Part of Shaping our Future

ACC is in a period of significant change. A new organisational vision, values and customer experience approaches have been introduced. Our Target Operating Model puts the customer at the centre of our processes and will fundamentally transform the way ACC collects, uses, stores and discloses information. It also provides customers with better ways to access and correct their information. We will achieve this through the implementation of the Shaping our Future strategy and our Transformation Programme.

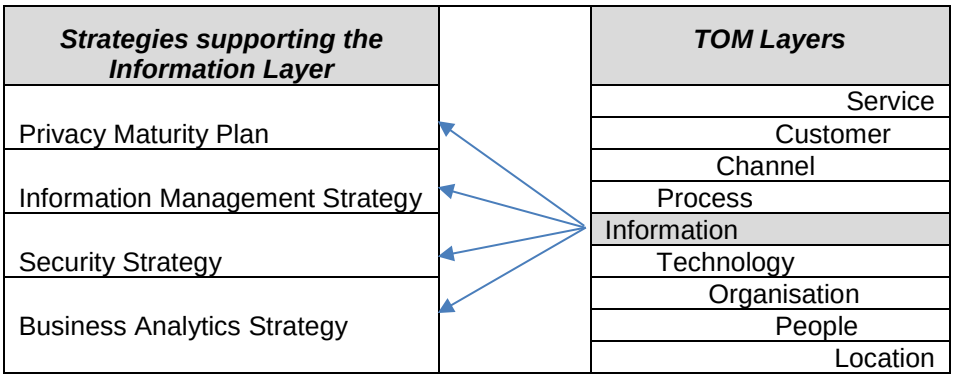
There are nine layers in the Target Operating Model – Service, Customer, Digital channels, Processes, Information, Technology, Organisation, People and Location. We will embed privacy in the design of all systems and processes that are developed under the layers of the Target Operating Model. Significant investment is planned in years 4 and 5 to establish an effective technology foundation that will reduce the number of privacy breaches associated with manual handling. It will put the customer at the centre of our processes and fundamentally transform the way ACC collects, uses, stores and discloses information, as well as providing customers with significantly improved access to and correction of their information.

The Information Layer describes how our data will be organised, distributed and shared, internally and with our customers. Our aim is to have accurate and timely data, which is specific, organised for a purpose, and is presented with context so that it has meaning and relevance.

The key features of the Information Layer include:

- A focus on continuous improvement, supported by the analysis of our customers' feedback and satisfaction, behavioural information, and data
- Sourcing information from trusted sources such as Inland Revenue, the Companies Office, and Ministry of Health to improve the quality of our data while ensuring we operate efficiently
- Identifying our principal data sources and avoiding replication of data between systems
- Only holding data that we need
- Ensuring our core systems are our single source of truth and provide a complete view of each customer.

The table on the following page shows the relationship between the Privacy Maturity Action Plan and other key elements that define the Information Layer of the Target Operating Model.



This action plan outlines how we will embed privacy through the Transformation Programme and our broader operations to build our privacy maturity. The actions we take under this plan will be integrated with the enterprise-wide work to improve our overall Information Management Maturity.

3 Assessment of Current State

An independent review in 2012 highlighted significant concerns with how (at that time) we were managing the personal information. We have made significant improvements and investment in our privacy performance since then including the establishment of a dedicated privacy team, and client information teams to manage information access requests. Privacy policies have been documented to support best practice, and system design processes include a preliminary investigation of privacy risk.

In December 2014, we commissioned a follow-up review on our progress since 2012.[2] The review noted that ACC had made substantial improvements. Frontline staff, in particular, now have a much better understanding of privacy, how to protect personal information and the processes required to mitigate against the risk of privacy breaches.

The review concluded:

> *We are not aware of any other New Zealand agencies or organisations that have put in a comparable level of dedicated resourcing and attention to Privacy protection, and issue detection, within such as short timeframe. This is commendable.*

However, privacy breaches are still occurring. Our processes are still manually intensive and rely on the attention of individual staff members to avoid mistakes being made. In the year to April 2016, the monthly average of privacy breaches using ACC's own definition ranged from 10-21. Ongoing focus at an enterprise level is required to maintain and improve this performance.

Privacy by Design[3] has been adopted as a core design principle within the Transformation Programme and all other change being implemented across ACC. Privacy by Design is an

[2] Both the 2012 *Independent Review of ACC's Privacy and Security of Information* and the 2014 *Independent Privacy Follow-Up Review* can be found at http://www.acc.co.nz/privacy.
[3] An overview of Privacy by Design is available at https://www.ipc.on.ca/english/privacy/introduction-to-pbd/

approach to protecting privacy by embedding it in the design of new technologies and business practices. It involves building in privacy into the design specifications and architecture of new systems and processes.

Privacy Maturity Assessment Framework

In August 2014, the Government Chief Privacy Officer (**GCPO**) issued core expectations of government agencies that represent good practice for privacy management and governance. The GCPO also issued the Privacy Maturity Assessment Framework (**PMAF**) to support agencies in meeting the core expectations.

The PMAF enables an organisation to determine its current level of maturity and assess whether this is appropriate, given the nature and risks associated with managing personal information. The Framework assesses privacy in nine focus areas and allows agencies to rate their performance against a five-point maturity scale. Details are contained in **Appendix 1**.

An independent assessment against the PMAF confirmed that ACC is measurably ahead of the rest of the Public Sector in overall privacy maturity and this has been confirmed in discussions with the GCPO.

The April 2015 independent assessment showed that our privacy culture and breach and incident management capability are already *Embedded*, which aligns to expectations for an agency of our size and complexity. This reflects the significant focus and investment we have placed in these areas since 2012.

The areas which were assessed as needing improvement in maturity were:

- Information Management
- Assurance
- Business Processes
- Implementation of the Information Privacy Principles (IPPs) from the Privacy Act 1993.

These areas were assessed as being weaker predominantly because we did not have privacy embedded into the design of our processes and systems. It should be noted that since the independent PMAF assessment of 2015, changes have been made to these improve these areas that will contribute to an increase in their privacy maturity. For example, establishing the Information Governance Group and formalising the information strategy will uplift the level of maturity from Ad Hoc to Defined.

Our key areas of focus for the next four years will therefore be:

- agreeing an enterprise-wide approach to information management. Specifically appreciating information as a business asset rather than a by-product of business processes

- implementing an enterprise-wide approach to privacy assurance, and enhancing its effectiveness through building on the basics of the three lines of defence model
- improving business processes through consideration of the value of the information that we manage
- enhancing our maturity across all the IPPs through effective and detailed policies, and using customer feedback to identify improvement opportunities.

Our assessed current state against each of the maturity focus areas is reflected in the diagram at the end of section five of this document.

4 Actions

The systemic changes that will be delivered by our Transformation Programme are key to sustainably improving our privacy performance. They will fundamentally transform the way ACC collects, uses, stores and discloses information, as well as provide our customers with significantly improved abilities to access and correct their information. This will be complemented by the delivery of our Strategic Change Portfolio[4] and our ongoing programme of other continuous improvement activities.

This will enable us to achieve our strategic objectives relating to privacy, including increased privacy maturity and improved breach performance across our operations.

The deliverables below reflect the key areas of change that will improve our privacy maturity and performance across the next four years. Initiatives have been mapped against the element of the PMAF that they will have the greatest improvement impact against.

[4] The Strategic Change Portfolio is overseen by the Enterprise Portfolio Management Office and consists of all major strategic investment programmes and projects delivered outside the Transformation Programme.

Deliverable Area:

Transformation Programme
Strategic Change Portfolio
Business Plan / Service Agreement Deliverables

Maturity Element	FY16/17	FY17/18	FY18/19	FY19/20
Governance, Leadership & Accountability	Strengthen Information Governance	Information Strategy Implementation		
	Privacy Policy Update			
	Information Management Policy Update			
Culture	Culture and Change Delivery			
	Ongoing Privacy Communications and Engagement			
Assurance	Implement Privacy Audits	Develop Information Assurance Framework		
	Supplier Management Framework			
	Transformation Programme Independent Quality Assurance			
	Assurance Services Annual Assurance Plan Delivery			
Information Management	Enterprise Content Management as a Service (ECMaaS)			
	Data Classification and Assessment	Information Classification Framework		
	Business Analytics and Reporting		Mobile Business Analytics Capability	
	Current State Information Assessment	Enterprise Information Register		
	Information Management Strategy approved			
	New Zealand Business Number			
	Business Support Modernisation			

Maturity Element	FY16/17	FY17/18	FY18/19	FY19/20
Privacy Risk Assessment	Privacy Risk Assessments for Strategic Change Portfolio			
	Privacy Risk Assessments for Transformation Programme			
	Implement Privacy Risk Assessments for Continuous Improvement	Privacy Risk Assessments for Continuous Improvement		
Privacy Programme	Secure File Transfer			
Business Processes	Levy Invoice Simplification			Business Customer CCRP Integration
	Business Customer Self Service			
		Client Self Service		
	Provider Self Service			
		Evidence Based Approach to Client and Provider Management		
	Core Claims Management Modernisation			
	Customer Feedback			Field Enabled Case Management
	Practice Management System Integration			
	Continuous Improvement Enhancements			
Implementation of Information Privacy Principles	Enterprise Business Rules			
	Ongoing Privacy Education and Training			
	IPP Compliance Review (Collection, Storage and Security, Retention, Unique Identifiers)	IPP Compliance Review (Access, Correction, Accuracy)	IPP Compliance Review (Use and Disclosure)	
Breach & Incident Management	Implement GCPO Breach Definition			
	Breach and Incident Management and Analysis			

5 Measuring our Success

Privacy Breaches

Privacy breaches are a key indicator of the success of our privacy investment. We will continue to track and report on privacy breaches through our published external accountability reporting and internal performance reporting. This will ensure that we remain accountable at an enterprise level to continually improve our privacy performance and provide us with a benchmark for measuring the success of our initiatives.

From 1 July 2016, ACC will be implementing the Privacy Breach Reporting Framework (Framework) that was released by the GCPO in December 2015. The Framework gives public sector agencies a tool to identify and report on the scale and severity of privacy breaches, and assist in providing context when reporting incidents internally, or to the public through official documents. Details of the Framework are included in **Appendix 2**.

Our Service Agreement Targets are:

Proposed Measure [and owner]	Suggested Targets						Commentary
	14/15	15/16 [to 31 Jan 16]	16/17	17/18	18/19	19/20	
Privacy breaches	4	2	<5	<5	<5	<5	Updated measure to reflect GCPO privacy breach reporting framework. A breach is defined as an incident rated at Level 3, 4 or 5 and recommended as being reported externally under the GCPO reporting framework
			with zero category 5 breaches				

Under the Framework, a privacy breach is when an agency does not comply with one or more of the IPPs. Compared to our current breach definition, the Framework will capture a broader range of privacy incidents (including what ACC currently defines as 'non-compliance events').

Privacy Maturity Improvements

We will measure improvements in our privacy maturity through annual re-assessments against the PMAF. Our objective is to be assessed as *Embedded* against all nine elements of the PMAF by 2020. Through delivery of actions outlined above, the expected annual improvements in maturity levels against the Framework are illustrated in the following table:

	Ad Hoc	Developing	Defined	Embedded	Optimised
1. Governance, Leadership & Accountability			***Current State***		
2. Culture				***Current State***	
3. Assurance		***Current State***			
4. Information Management	***Current State***				
5. Privacy Risk Assessment			***Current State***		
6. Privacy Programme			***Current State***		
7. Business Processes		***Current State***			
8. Implementation of IPPs		***Current State***			
9. Breach & Incident Management				***Current State***	

6 Outcomes

By implementing the actions in this Maturity Plan, the following outcomes will be realised against the elements of the PMAF by 2020.

Elements	Outcomes
Governance, Leadership & Accountability	• There is ongoing, visible commitment from senior leadership • Governance oversight of privacy is effectively operating across the organisation • A formal privacy management structure is in place, including a Privacy Officer, and clear accountability for privacy at all levels
Culture	• Leadership work collectively and visibly to improve privacy • There is clear evidence of respect for privacy embedded as part of a customer centred culture
Assurance	• Three lines of assurance are in place, providing ongoing feedback on privacy performance and maturity • Assurance reporting and monitoring effectively informs of any changes in performance
Information Management	• There is a defined and effectively operating structure to manage data and information • There is an effective information management strategy supporting delivery of the information layer within the Target Operating Model • Information management is integrated into business processes and continually monitored for improvement.
Privacy Risk Assessment	• Privacy risk management is fully integrated with our wider enterprise risk management framework • Identifying and managing privacy risk is a business-as-usual activity
Privacy Programme	• Privacy is a core competency across all areas of our operations • Privacy policies and procedures are understood and adhered to by all our people • Privacy training empowers staff to manage personal information with confidence
Business Processes	• Privacy analysis is fully integrated into business processes designed with privacy as the default setting • Privacy impact assessments are a standard part of all change and continuous improvement activities, • Systems and business processes are automated and digital where possible to minimise the risk of privacy incidents • Continuous monitoring of systems containing personal information
Implementation of Information Privacy Principles	• We are able to demonstrate ongoing, effective compliance with IPPs 1-12 • Supporting policies and processes are documented and continually monitored for improvement opportunities
Breach & Incident Management	• The incident handling and escalation process is effective and monitored, minimising the risk of privacy incidents escalating into events that cause harm to individuals • Breach incident reporting is in place and all incidents are analysed to inform changes

7 Risks and Mitigations

The following are identified risks, and possible mitigations:

- **Uncertainty about technology**: ACC's privacy performance is heavily reliant on people because processes to prevent privacy incidents are predominantly manual. If the technologies are challenging for people to adopt, this could impact on the delivery of solutions and risks of manual work-arounds as a solution to preventing privacy incidents. While ideally technology solutions will employ optimal privacy protections, they will require testing before implementation to ensure their fitness for purpose; assessment to ensure compliance with government computing standards (particularly if cloud-based); and thorough training to ensure users adopt them with minimal disruption to operations.

- **Failing to incorporate Privacy by Design**: All changes across ACC are required to incorporate Privacy by Design into system and process design. It would be difficult to retroactively apply adequate protections if they are not incorporated at the design stage. Implementation of any initiative needs to have a privacy lens applied early in the design process.

- **Staff will lose their privacy mind-set**: If technology solutions are not delivered with adequate training, are not intuitive or do not assist staff to meet privacy considerations, staff may ignore or misuse them. Conversely, if staff rely on technology solutions that are not designed with full privacy protections, they will not take personal responsibility for ensuring information is protected. Mitigating this risk will require maintaining our engagement with staff about privacy and continued education about and promotion of best practice behaviour.

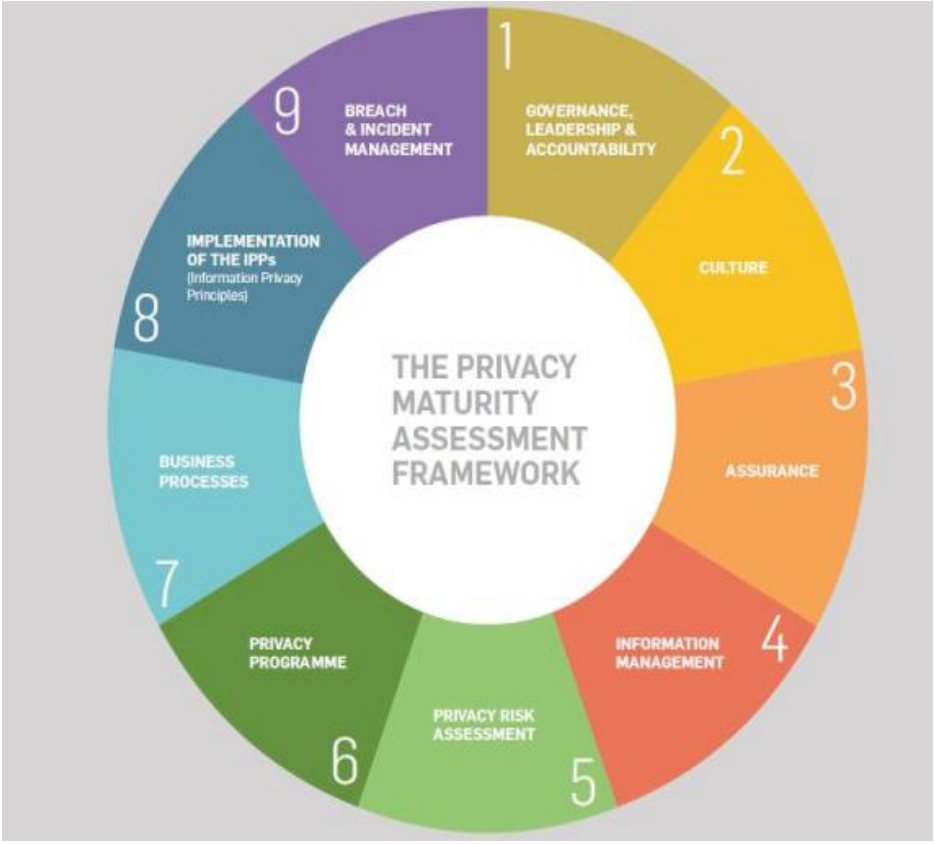
- **Reduced resources**: As ACC's privacy performance improves and the number of breaches reduces, there may be an inclination to decrease the privacy resources available. This could impact on the type of training for our staff to ensure a high awareness of privacy is maintained. It could impact on the analysis of privacy incidents undertaken, and the resulting initiatives to target high risk areas. Reduced resources may also impact on the assistance available to Shaping Our Future and other parts of the business to ensure Privacy by Design is considered. To mitigate this risk, it is important that these initiatives are appropriately resourced.

- **Privacy is not integrated into business planning**: Privacy processes, risks and considerations impact many areas of the business. In particular, the Information Management and Information Security areas (and accompanying strategies) are natural companions to privacy, and the Customer Feedback Strategy includes privacy feedback components. It is important that privacy is linked into all business planning processes across the organisation, so that the protection of our customers' personal information is embedded into every aspect of our operations.

- **Governance processes lessen their focus on privacy**: The significant focus and investment in privacy at ACC has contributed to our success in improving privacy culture and reducing privacy incidents. Given the number of initiatives underway over the next several years, these competing priorities may distract or reduce our attention on privacy. ACC management needs to ensure that privacy remains a priority as one of our strategic intentions.

Appendix 1 – Privacy Maturity Assessment Framework

The PMAF assesses privacy in nine focus areas, rating current performance against a five-point maturity scale. The diagram on the left below shows the nine focus areas, and the table on the right show the maturity scale and descriptions from Ad Hoc to Optimised.



Ad Hoc	Developing	Defined	Embedded	Optimised
Unstructured approach where privacy policies, processes and practices are not sufficiently defined or documented. Privacy management is mostly dependent on initiatives by individuals rather than processes.	Privacy management is viewed as a compliance exercise and the overall approach is largely reactive with some documented guidelines. There is limited central oversight of the privacy policies, processes and practices with siloed approaches within business units.	Privacy policies, processes and practices are defined and comprehensive to meet the operating needs of the agency and are consistently implemented throughout. The business has a holistic and proactive approach with widespread awareness of privacy management	Privacy management is embedded into the design and functionality of business processes and systems and is consistent across the agency. Well-defined governance and oversight structures exist.	Privacy management is viewed as a strategic initiative with a clear agency culture of continual improvement. The agency is viewed by stakeholders and the public as a leader in privacy management, introducing innovative initiatives to meet their needs.

Appendix 2 – Privacy Breach Reporting Framework

Government Chief Privacy Officer (**GCPO**) has developed guidance for breach reporting, which was officially launched in December 2015. The purpose of this Privacy Breach Reporting Framework (**Framework**) is to give agencies a tool to identify and report on the scale and severity of privacy breaches and near misses (where this information is requested). It may also assist agencies in providing context around privacy breaches and near misses reported internally, or to the public through official documents such as annual reports. ACC is seen by the GCPO as a leader in privacy breach reporting and was involved in the development of this Framework including using our privacy incident data to support testing and calibration of the Framework.

A privacy breach is when an agency does not comply with one or more of the IPPs set out in section 6 of the Privacy Act 1993. The matrix has seven key areas to be assessed:

- number of individuals affected
- sensitivity of the information at issue
- harm to the individual
- harm to the agency
- potential for media attention
- source of the privacy breach
- whether the information has been recovered, accessed, or able to be accessed

Each assessment response is assigned a value, the total of which determines the rating of the privacy breach. The purpose of the ratings is to provide an indication of the severity and scale of the privacy breaches occurring. Once ratings are totalled, they are allocated a Level from 1 to 5, with 5 being the most serious.