



6 March 2025

Tēnā koe

Official Information Act request

Thank you for your email of 8 December 2024, requesting information about Māori Data Sovereignty and Māori Data Governance.

I have considered your request under the Official Information Act 1982 (the Act). Please find my decision on each part of your request set out separately below.

1. How does your organisation define Māori data as opposed to non-Māori data?

Te Manatū Whakahiato Ora does not currently define Māori data. Where relevant, external definitions (such as those proposed by Te Mana Raraunga) can be referenced, and an internal definition is under development by Te Manatū Whakahiato Ora.

2. Does your organisation have Māori Data Sovereignty and or a Māori Data Governance policy or strategy? If yes, I request a copy.

Te Manatū Whakahiato Ora does not have a current Māori Data Sovereignty or Māori Data Governance policy or strategy. Our Enterprise Information Governance framework does include a proposed Poutiaki operating model for incorporating Māori values, needs and expectations into Data (Information) Governance. Please see this document attached.

3. I also request a copy of your organisation Data Governance strategy/policy/policies?

Te Manatū Whakahiato Ora's information and data governance framework includes:

- MSD Information, Data and Analytics (IDA) Strategy
- Tiaki - Enterprise Information Governance Framework
- MSD Information Governance Policy
- Te Haoroa Interim Data Governance Framework

Please see these documents attached.

The Te Haoroa Data Governance Framework was approved at governance in 2023. The attached framework, from May 2024, was compiled to describe the interlink between governance practices and technology in support of delivery. Please note that this iteration of the framework has not been approved at any governance forum.

4. Has your organisation had with any success or no/limited success, implementation of any Māori Data Sovereignty Principles or Māori Data Governance? If yes, please provide details of the implementation and how you measured its success.

As part of developing its enterprise data capabilities, for example MSD's Enterprise Information Governance Framework, we are doing some work to understand how this may reference relevant principles. This work is in design phase, and measures of success are yet to be established.

5. How many. fte are allocated to Māori Data practices in your organisation?

Te Manatū Whakahiato Ora has two dedicated FTE focussed on Māori data practices:

- Senior Analyst, Māori Data & Insights
- Principal Māori Data Governance Advisor

Beyond these roles, other staff contribute to Māori data practices in meaningful ways as part of their broader responsibilities, but it is not possible to quantify their time as a nominal FTE allocation.

6. What country/countries are the majority of your organisation's data stored?

Our client data is stored primarily in New Zealand and Australia. Te Manatū Whakahiato Ora do use Cloud providers to store data with geographic locations in Sydney and Melbourne, Australia. We store a small set of data in these Cloud provider locations with a plan to increase over time.

7. Which Cloud Provider(s) do you use?

Te Manatū Whakahiato Ora use the following Cloud Providers based in the named geographic locations:

- Microsoft Azure
 - Primary geographic location is Sydney.
 - Secondary geographic location is Melbourne.
- Amazon Web Services (AWS)
 - Primary geographic location is Sydney.
 - Secondary geographic location is Melbourne.
- Google Cloud Platform (GCP)
 - We use a small set of SaaS products only.
- Oracle Cloud (OCI)
 - We use a small set of SaaS products only.
- IBM Cloud
 - We use a small set of SaaS products only and are actively decommissioning this Cloud provider.
- Te Heaoroa/SAS – (Hosted Managed Service)
 - Te Haoroa is Te Manatū Whakahiato Ora's cloud data and analytics platform, that is a histed service tenanted and managed by the SAS

Institute. SAS' cloud tenancy is in Microsoft's Azure Australia East (Sydney) geographic location.

MSD also use a large number of Cloud based products within our environment which sit on various providers cloud environments. Some examples of these products include:

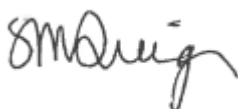
- Microsoft 365 suite which we use for communication and collaboration,
- Atlassian Jira and Confluence which we use for job planning, collaboration and knowledge sharing,
- Koha, hosted in Catalyst Cloud, which serves as a library of books and e-journals used by internal staff.

I will be publishing this decision letter, with your personal details deleted, on Te Manatū Whakahiato Ora's website in due course.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with my decision on your request regarding Māori Data Sovereignty and Māori Data Governance, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Ngā mihi nui

pp. 

Anna Graham
General Manager
Ministerial and Executive Services



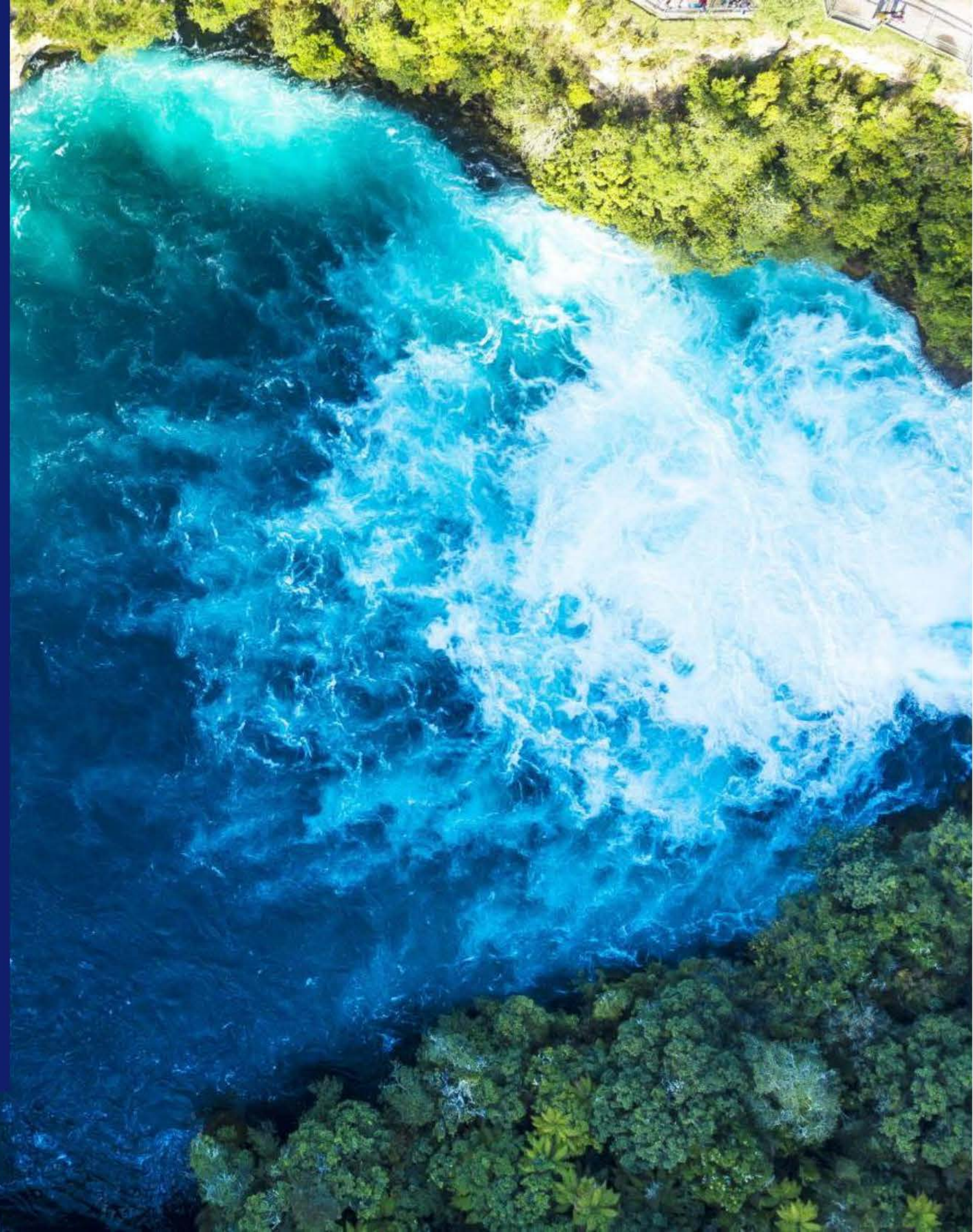
**MINISTRY OF SOCIAL
DEVELOPMENT**
TE MANATŪ WHAKAHIATO ORA

Information, data and analytics strategy

V 1.0 FINAL
May 2022

**Ko te pae tawhiti whāia kia tata,
ko te pae tata whakamaua kia tina**

Seek out the distant horizons,
while cherishing those achievements at hand



Contents

Strategic context	03
Driving forces	04
Our vision for the future	05
How we deliver value from data	06
ID&A strategy on a page	07
ID&A strategic shifts	08
ID&A transformation roadmaps	16



Our ability to deliver our future relies on our ability to manage, respect and use peoples’ information.

Effective use of information, data, and analytics is key to helping New Zealanders to be safe, strong and independent. We collect the information necessary to provide services and fulfil a range of reporting, accountability, data sharing, and integrity obligations.

Information and data is a fundamental enabler for MSD to deliver the vision of Te Pae Tawhiti. There are significant opportunities to inform better decision making, but we need to be careful to ensure we respect our clients’ privacy, human and ethical rights, and we keep people's information secure.

We must ensure that we consider the potential harm new uses may cause individuals and work to mitigate them to an acceptable level. The ability to leverage greater value from our data and information relies on people being aware of, and comfortable with, how we use it.

We hold a vast amount of information about our clients, the communities we support, and the effectiveness of our services, policies and processes. We need to understand the information we hold and effectively use it to design and personalise services. We need to understand what is effective and understand how and why we deliver services in the way we do. These things are critical to enabling our staff to do their jobs and to support an information- and insights-driven future services model.

Following an extended period of under-investment, MSD has aging technology, data infrastructure and immature information management and governance practices. This means we have gaps in our foundational capabilities that first need to be filled before we can maximise the value of the information we hold to support Te Pae Tawhiti.

Our practices need to evolve to appropriately respect the mana and dignity of people, whanau, communities and groups who share their data and information with us. Work also needs to be done to ensure that quality and reliable data can be accessed in a timely manner by those who need it.

- This Information, Data and Analytics (ID&A) Strategy addresses two critical components of data and information management for MSD:
1. Our ability to effectively collect, manage, use and share data and information to enable:
 - Valuable insights which inform policy, service design and organisational efficiencies, and
 - Enhanced and personalised experience for customers, staff and partners.
 - Staff to have easily available the information necessary to do their jobs, at the time and in the context they need it.
 2. Our commitment to use peoples’ data and information responsibly, building respect for Te ao Māori into how we work and ensuring that the information is always respected and protected.

The ID&A Strategy 2022 fits alongside the Technology Strategy 2022, communicating how we intend to shift our information, data and analytics practices to support the delivery of Te Pae Tawhiti. This Strategy sets out our vision for becoming a trusted steward of information that leverages the taonga we hold to improve the lives of New Zealanders.

Te Pae Tawhiti – Our Future presents our strategic direction and sets out three shifts we need to make as an organisation to achieve our outcomes

Mana manaaki

A positive experience every time



Kotahitanga

Partnering for greater impact

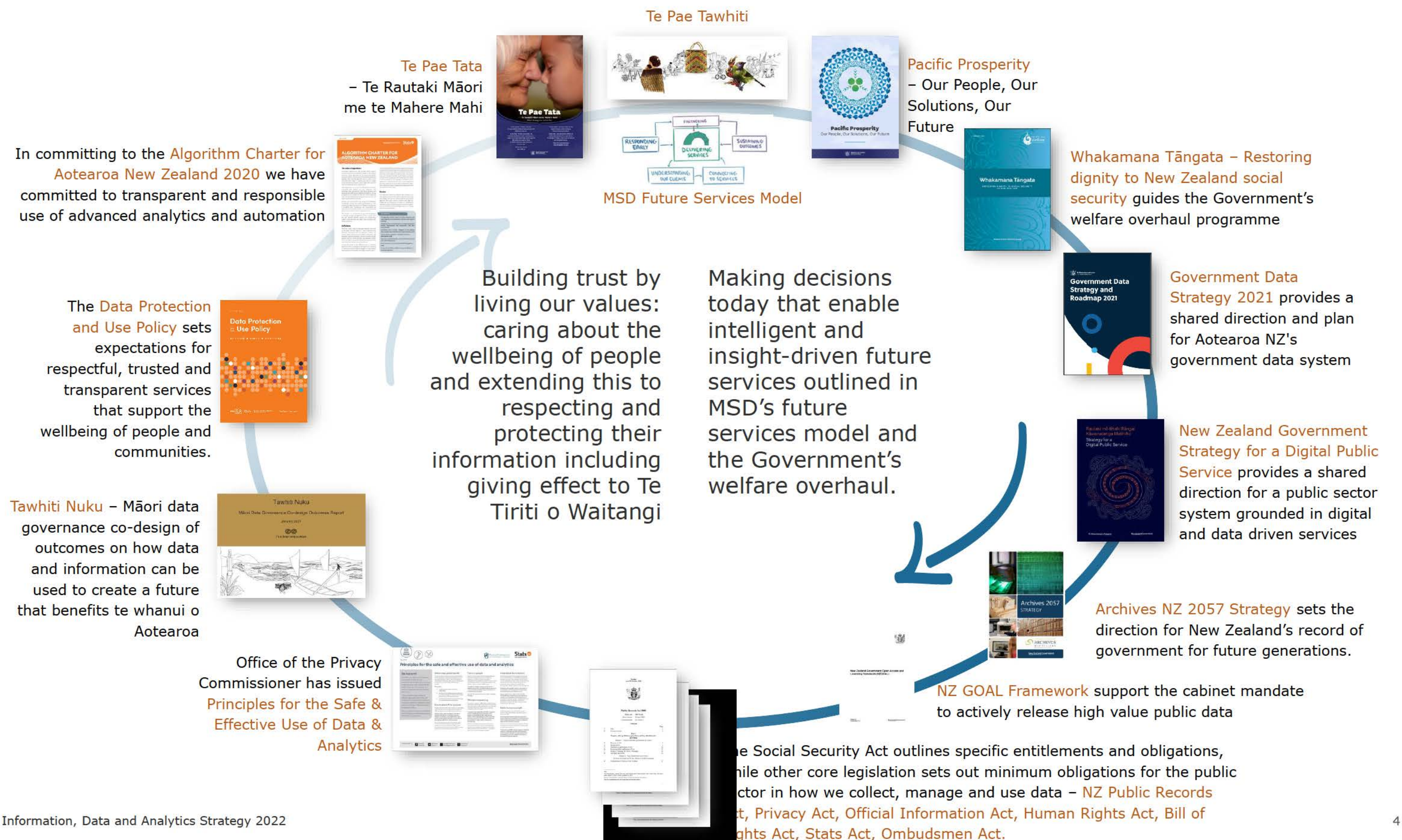


Kia takatū tātou

Supporting long-term social and economic development



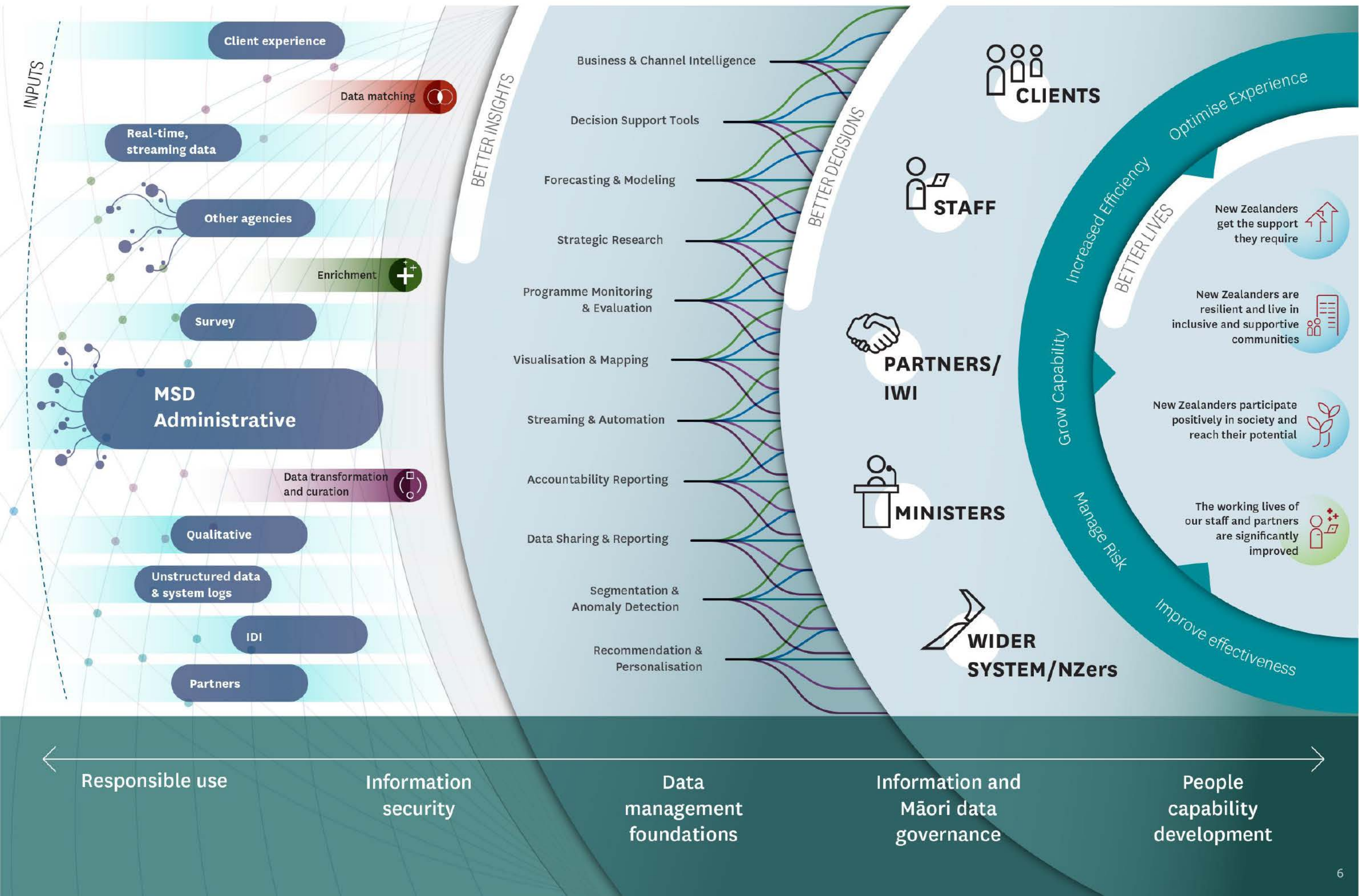
MSD have a responsibility to do the right thing while building a tailored, insight-driven and intelligent service model



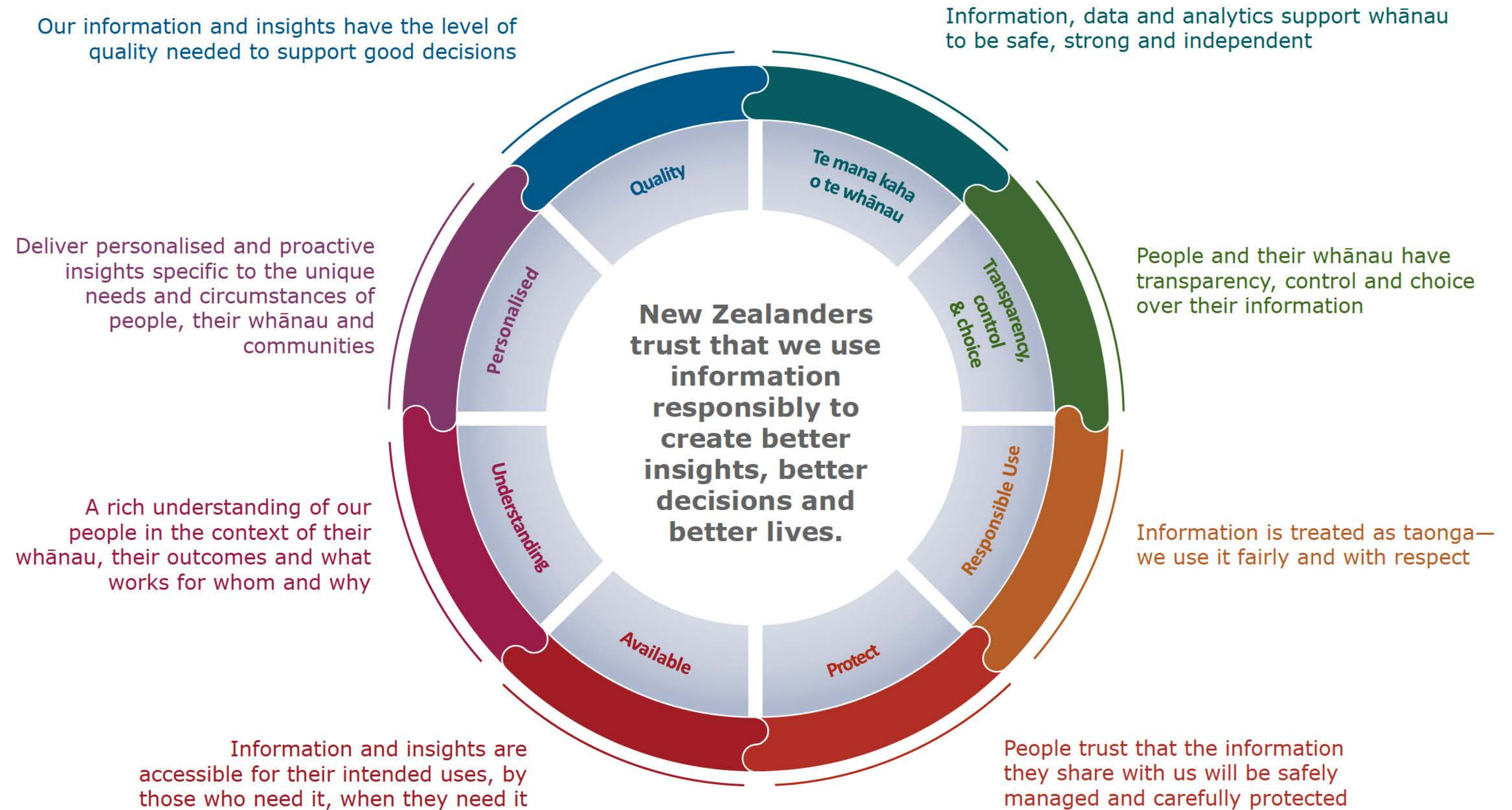


New Zealanders trust
that we use
information responsibly
for better insights,
better decisions and
better lives.

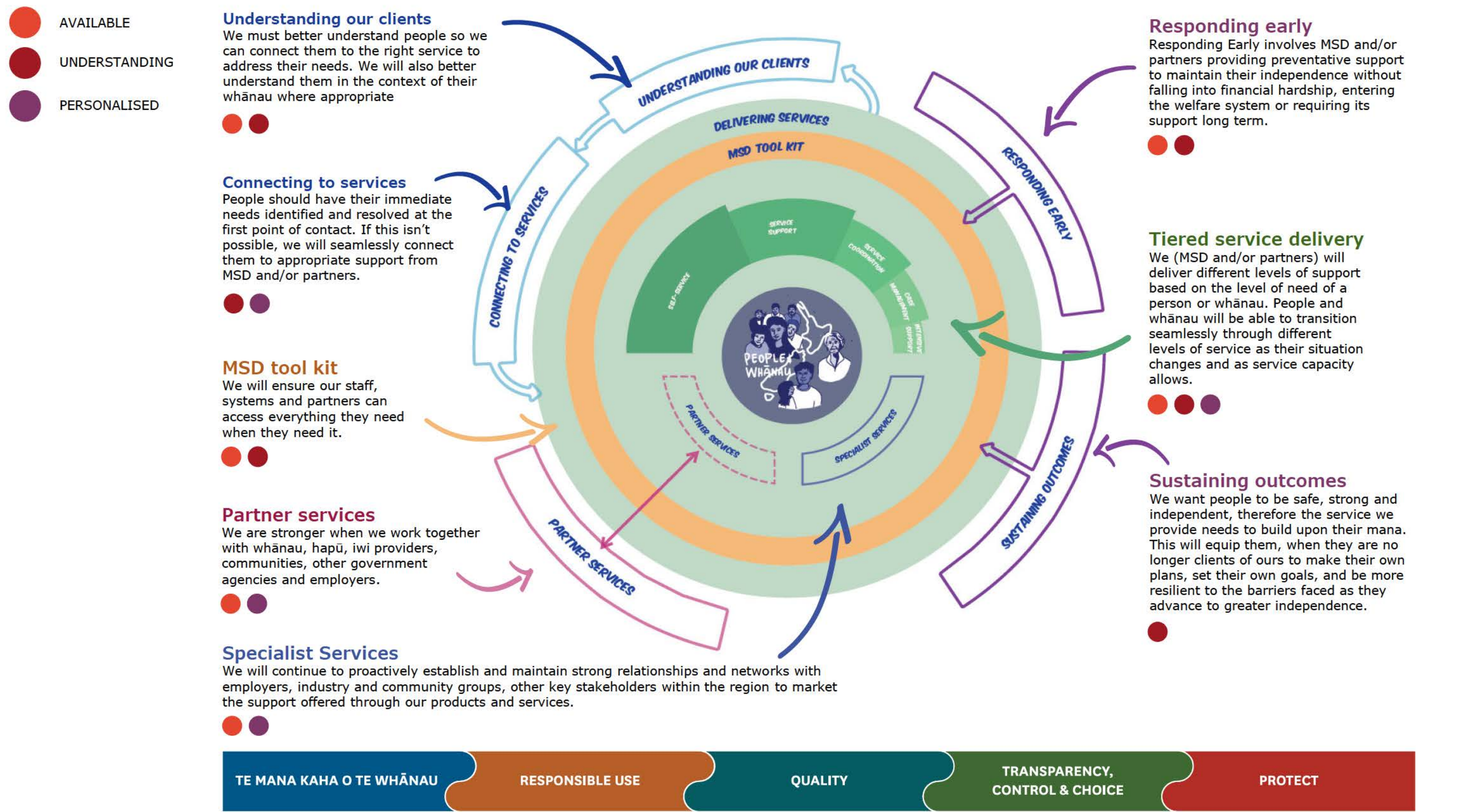
HOW WE DELIVER VALUE FROM DATA



Eight strategic shifts combine to ensure responsible information use and insights for better lives



The strategic shifts enable our Future Services Model: some underpin all parts of the model, while the available, understanding and personalised shifts align with different parts of the model



Information is treated as taonga—we use it fairly and with respect

Responsible use of information refers to the understanding that data and information should be treated as an extension of the person. As such, it is given the same respect that we give to the person.

Responsible use of information is important because...

People expect that we understand that we are stewards of the information we hold, and of information flowing through the system between clients, us and partners. They expect that we manage and use the information respectfully and in a manner that improves outcomes for the people and communities we support. This is in addition to the basic rights afforded to people under legalisation such as the Privacy Act, and are set out in various public sector expectations documents such as those on page 5. This will result in services that treat people with respect, enhancing their mana, demonstrating **mana manaaki**.

Better use of data and analytics can significantly improve outcomes for our clients, and is one of the cornerstones of enabling **MSD's future services model**. Leveraging greater value from data relies on us being able to demonstrate that we have prioritised people's rights and expectations when we use their information.

When this is working well...

Our staff behaviours and use of data demonstrate that information about people is not owned by the Ministry, that it is an extension of the person, that we are stewards and staff are expected to respect the information as such. Services are designed around people and are focused on benefits for those people, their whanāu and their communities. Our staff will have available good training and tools so that they know what responsible use is. *Further maturity in the application of our Service Design Principles and Privacy Human Rights and Ethics Framework will enable this. From our roadmap **Developing Te Ao Māori data capability (data as taonga), Capability Development, Design information policies and treatment, and Data & Information Governance** will deliver capabilities that further enable this.*

We understand where information has come from and what we are authorised to do with it, so that we can make respectful decisions about how to use it. We have

Moving from...

MSD has government-leading information and data management frameworks for new uses, but we have large legacy services that were designed before these frameworks were applied

Information about clients is often treated as something owned by MSD

We do not always handle the information in a manner that respects that the information is about a person.



...to...

People are at the centre of the information we collect, use, share and manage and the systems, services and approaches we design

We treat information about people as an extension of the person and use it fairly, with respect for the people it is about, and in a way that delivers clear benefits for the person and/or for New Zealanders

Diversity is respected by considering bias and discrimination in the development and design of systems, services and approaches.

a data model and technical products that enable us to capture where information came from and to manage what we can do with it accordingly. *From our roadmap **Data & Information Governance, Enterprise Data Model and Information Architecture, Metadata management and Master Data Management** will deliver these capabilities.*

Bias in our data sets is understood and efforts are made to compensate for this bias as appropriate when the data is used for future service design or delivery of services. Discrimination is actively considered in service design. *Continuing to apply our Model Development Lifecycle and Privacy, Human Rights and Ethics Framework will enable this. From our roadmap **Design information policies and treatment, Data & Information Governance, Enterprise Data Model and Information Architecture** will deliver this.*

People and their whānau have transparency, control and choice over their information

Transparency, control & choice relates to providing clients with options (where possible*) around what information we collect, how we collect it, who we share it with, and being transparent about how we use their information.

Transparency, control & choice is important because...

Public interest in, and expectations about, transparency of information and data use is high. There have been high profile examples of public dissatisfaction in the way that entities manage personal information—both public and non-government, domestic and internationally. This has coincided with changing regulatory environments and expectations internationally and from government (see public sector expectation documents on page 5).

Better use of data and analytics can significantly improve outcomes for our clients, and is one of the cornerstones of enabling **MSD's Future Services Model**. The public and Government expect that the use of algorithms and automation is balanced against individual rights. This includes the right to know how decisions affecting them are made and giving choices over how information is used, where this is possible. To deliver the **Future Services Model** we will need to give more control to people over what we do with their information if we want to operate in line with public expectations and legislation. Being open with people about what we do with their information enhances trust with our clients and demonstrates **mana manaaki**.

When this is working well...

We understand what information must be collected to enable us to provide services, and what information we collect for other reasons where we can give people more control over what we do with the information. Where possible, we enable people to choose whether to provide information or not and whether we share it with others and we respect those choices. We make clear what information will be used for and who it will be shared with. We make clear where clients have no choices about our use or sharing of their information, and why not. In order to do this, we need to know why information is collected or created and to be able to track that through our systems so that we can make informed decisions about use and reuse.

*Further maturity in the application of our Service Design Principles and Privacy Human Rights and Ethics Framework will enable this. From our roadmap **Data & Information Governance, Consent Management, Enterprise Data Model and***

Moving from...

MSD publishes what information and data that we hold, and how it used to make decisions at a high level. But clients do not have many choices or much visibility of what we do with their specific information, control over what we do with it, or who has access to it.



...to...

Where possible we give people choices about the information they provide, what it's used for and who it is shared with and respect the choices they make. Where there are no choices, we are transparent about our use of their information, who it is shared with and how we use it. We proactively publish information about how MSD makes decisions, including what information is used to make those decisions and where the information was collected from.

* "Where possible" means that while we aim to increasingly give people choices about what we do with their information, there remain many areas where people will not have choices. For example, we have Approved Information Sharing Agreements with other agencies where information is routinely shared and will continue to be. We also have to ensure that we have the information we need to determine eligibility for, and maintain integrity of, our services. In these areas we aim to be more transparent but will not provide choices around collection, use or sharing of information.

Information Architecture and Metadata Management will deliver these capabilities.

We make personalised information available, through self-service channels, about how information has been used, who we have shared it with and for what purposes. From our roadmap **Enterprise Data Model and Information Architecture, Metadata Management and Master Data Management** will deliver these capabilities.

We proactively publish information about how we use personal information to make decisions, where the information was collected from and who it was shared with. From our roadmap **Data & Information Governance, Enterprise Data Model and Information Architecture, and Metadata Management** will deliver these capabilities.

People trust that the information they share with us will be safely managed and carefully protected

Protecting data and information refers to keeping it safe from inappropriate access and misuse while still making it available to those who need it to deliver services.

Protecting information is important because...

If people are going to entrust their information with us, they need to know that we will keep it safe. Many of the ways we want to work in the future depend on clients consenting to new and different information uses. For them to do so they need to trust that we will protect it; in doing so we are demonstrating **mana manaaki**.

There have been a number of serious breaches of security across Government, including at MSD, that have resulted in ongoing high levels of expectation of the security environment for government agencies. This has led to centrally mandated obligations for agencies and regular assessment and reporting against those obligations. MSD has reported increasing compliance and maturity against these measures but further maturing of our security environment is desired. Our current levels of compliance and maturity are heavily reliant on manual or inefficient measures that are assessed retrospectively. These should be modernised with more automated methods that are proactive and forward looking.

When this is working well...

We know what information we hold and we protect it according to its value and risk through a range of proactive and flexible measures. Where information is highly sensitive we ensure it is highly protected (protection outweighs availability). But where information is lower sensitivity, or the value of opening up protections is high, we can scale our protections to ensure maximum value can be leveraged. From our roadmap **Identity and Access Management, Metadata Management, Master Data Management and Data & Information Governance** will deliver this.


Identity centric security controls the availability of data and information regardless if it is inside or outside of the organisation. Identity centric security also enables traceability of data and information where we know who owns, accesses, modifies, views and uses data. From our roadmap **Identity and Access Management** will deliver this. The Technology Strategy and Roadmap also sets out a range of

Moving from...

Controls to protect information do not always operate effectively and impact negatively on user experience. We do not take a risk / value-based approach to protecting information.

We have a dependency on our network perimeter as a hard boundary to protect our systems and information with few effective security controls inside our networks.

Identity is inconsistently verified across our applications and systems. Access to our network implies authorisation and assumes identity has been verified.



PROTECT

...to...

We protect information according to its value and risk; security and privacy controls are right sized, easily scalable and embedded in the design of a system or process.

We protect our information wherever it is, relying on identity defined boundaries that enable the right information to be presented at the right time to the right people.

Information is classified and tagged across all our systems with automated management of access, retention and disposal based on this.

initiatives to move away from a traditional on-premise network-based environment to a zero-trust cloud-based environment

Classification of information and the automated management of its retention and disposal will be enabled by **Information and Data Lifecycle Management** and **Metadata Management**, which captures the contextual data required during the consent process to manage data appropriately. From our roadmap **Information Maturity (Enterprise Content Management)** will deliver this for corporate information.

Protection will be built into the design of our systems, through patterns and automation where possible, and ongoing monitoring will provide assurance that protections remain fit for purpose. Further maturity in the application of our Service Design Principles, move to cloud-based systems as outlined in the Technology Strategy and Roadmap and delivery of the foundational capabilities outlined in the security roadmap will enable this.

Information, data and analytics support whānau to be safe, strong and independent

Te mana kaha o te whānau is the vision of Te Pae Tata, which seeks to empower Māori to be self-determining – active within their community, living with a clear sense of identity and cultural integrity and with control over their destiny.

Information, data and analytics is important to support te mana kaha o te whānau because...

Making the information MSD holds available to iwi-Māori and communities will enable to them to make decisions that achieve their aspirations: **kia takatū tātou**. The data, analytics and research we deliver need to be grounded in te ao Māori concepts, so that they're relevant for tangata whenua. We also need to show **mana manaaki** in providing support and capability building so Māori are empowered to build their own information and data products.

Giving tangata whenua control over their destiny also means protecting their data as a taonga. We will need to work with **kotahitanga** to govern Māori data, so that it's protected, stored, maintained and used appropriately. We'll also need to continue to build our cultural competency and develop mutually beneficial relationships with iwi to succeed.

When this is working well...

We have mutually beneficial, enduring partnerships across the different ways information, data and analytics are used responsibly. This includes working together with tangata whenua on kaitiakitanga for **Data & Information Governance (including Māori Data Governance)**, as well as building **Better Outcomes frameworks** so data can be collected and analysed in te ao Māori frameworks.

We understand kaupapa Māori approaches and can work within them or apply them when they're needed. We're using tools like our *Privacy, Human Rights and Ethics Framework* and *Model Development Lifecycle* to assess and prevent bias and discrimination, and have an organisational culture that supports this.

Moving from...

MSD is committed to Te Pae Tawhiti and the Mana Ōrite agreement, but we need to do more and build on pockets of good practice.

MSD doesn't have a position on Māori data governance. We go to the Māori Reference Group for advice and guidance.

Little data is provided to tangata whenua and is generally one-off.



...to...

Information, data and analytics support whānau to be strong, safe and prosperous – active within their community, living with a clear sense of identity and cultural integrity and with control over their destiny

We partner with tangata whenua to ensure that kaitiakitanga (stewardship) is at the heart of how we take care of data.

Our partnerships extend to supporting whānau Māori and iwi with **Capability Development**, or Māori research organisations, to grow the capacity of the research sector. **Developing Te Ao Māori data capability**, we have built and have an ongoing focus on the capability of our staff and leaders to engage competently on Māori data issues and are aligned with cross-government approaches, like Mana Ōrite.

We are sharing relevant data with iwi through **Secure & Efficient Data Sharing**, while those who want to can also access information through **Self-service BI** tools, or work with us on joint projects through the **Collaborative Analytics & Data Science Platform**.

Our information and insights have the level of quality needed to support good decisions

Quality refers to the accuracy, timeliness and completeness of the information we hold and the insights we create from it.

Effectively managing quality is important because...

Information and insights are used to make decisions when they're trustworthy and a key driver of trust is quality. They need to be accurate and complete enough, and ready to be used when the decision is being made.

The quality of our data and information determines the services we can deliver and the experience of clients, staff and partners. Quality means a 'single source of truth' for important data and information, so we show **mana manaaki**: people don't have re-tell their story and we get it right the first time.

Some decisions need 'gold standard' quality, like verifying identity or public reporting on the number of people on benefit. But for others we can deliver for 'fit for purpose' quality, so we can support more decisions, with more impact.

Quality needs to be measured over the full lifecycle of information: from when it's collected, used, updated and destroyed. The same applies to insights, which have a use-by date if they're not maintained. Quality can also be about holding information in the right format so it can be reused easily, or not holding the information ourselves, but having a record that we've verified it.

When this is working well...

We have effective **Data & information governance**, which sets the ways we measure and maintain the quality of the data we hold. We are continuing to grow our **Data & information governance** by partnering with tangata whenua, so that we look after and use Māori data appropriately.

We maintain a single source of truth for our key information assets through **Master data management**, so it's used consistently across the organisation and with partners. **Metadata management** helps us find the right data and information, understand what it means, know where it came from, and what we have consent to use it for, like working across a whānau.

Moving from...

MSD does not know, understand, or govern its information assets appropriately, and therefore cannot unlock the value of its information.

Our insights sometimes have a 'one size fits all' approach to quality, or the quality is unknown



...to...

Information is collected and maintained in a format and quality that is appropriate for its use.

One source of truth is maintained, clients and partners do not have to repeat their story.

Decision makers have confidence that our insights are fit-for-purpose, high quality, and timely

We have ongoing processes for **Data quality management** and **Information and data lifecycle management** to monitor and maintain accuracy of information / data collecting, and insights we're generating, so services continue to be delivered effectively even as our systems or processes change. We can understand quality across our system by using **Enterprise Data Model and Information Architecture**.

We can describe the quality of our insights and what decisions they're suitable for: from rigorous evaluations to inform major investment decisions by ministers, to quick analysis for urgent operational changes. We have invested in Data **Capability Development** so that we have the skills and culture to maintain quality information and insights.

Information and insights are accessible for their intended uses, by those who need it, when they need it

Availability ensures that information required to support decisions is accessible for those who need it, when they need it. We have the tools, services and capability to create the insights required.

Effectively managing availability is important because...

Information and insights can only improve lives if they're available to the right people at the time decisions are being made.

We must deliver on **Mana manaaki**, a positive experience every time, as clients need to be able to easily find information on the supports they're eligible for, and services that may help them, as well as information we hold about them. Staff need real-time information at their fingertips too, so they understand a client's context and what may work for them to achieve their aspirations. They also need to be able to quickly find guidance and processes that help them do their jobs effectively.

We need to make information available to tangata whenua and partners to deliver on **kotahitanga**, using insights and information sharing for mutual benefit.

People outside MSD need access to information about the benefit system to understand how it works and how it's performing. This includes ministers, media, researchers and the general public. Information and insights need to be provided in ways that work for everyone and their different circumstances: open and in line with accessibility standards.

When this is working well, we will have...

An up-to-date **Enterprise Data Model and Information Architecture** shows how our data and information is created, organised, and used, so we know how it links together and understand the impact of system or process changes.

Metadata management helps us find the right data, understand what it means, know where data came from, what we can use it for, where it is being used, and the rules for access and sharing the data. **Master Data management** gives us a source of truth for our key data, so we can make the correct information available and it's easier to share with others when appropriate. These capabilities also mean we know who we can share data with without additional authorisation using **Self-service BI** and **Secure & efficient data sharing** and whether we can automatically release data to clients through **automated client data self service**.

Moving from...

Clients and employees cannot access information they need easily and in a timely manner

Data and insights are partial and difficult to find

MSD does not always have the tools, technology, or capacity to collaborate or share information effectively with our partners to best meet New Zealander's needs or outcomes



...to...

Staff can access the information they need to do their jobs, where and when they need it and can see the impact of their work.

Relevant data and insights are available, understood, and easily found or created for both internal and external users.

Clients can easily access information about themselves and their interactions with us

We have mutually beneficial partnerships founded in Whanaungatanga (relationships) and Mana Ōrite (equality), collaborating on insights and sharing information safely.

Access to only what people need is enabled by **Identity and access management**, while **Information and data lifecycle management** ensures we know what data can be used for, and what should be retained or disposed.

We have developed a sustainable data platform through **Te Haoroa** so our information is consistently available and resilient. A clear **Information, data and analytics operating model** and **Development of data assets** support us to make the right information and data products available.

Appropriate, relevant information and insights can be accessed safely through core systems, for staff, client and whanau, and external partners and agencies. This is enabled through **Self-service BI (business intelligence)**, **Secure & Efficient Data Sharing**, and **Collaborative Analytics & Data Science Platform**.

A rich understanding of our people in the context of their whānau, their outcomes and what works for whom and why

Understanding what matters for each person and their whanau's unique circumstances, how well our services are meeting their needs and how their outcomes contribute to the performance across the sector.

Understanding is important because...

For our services to improve outcomes they need to be effective: delivered to the right people, in the right way, at the right time. We need to understand what matters for individuals and their whanau (**mana manaaki**) that will in turn help understand how our services and those of our partners are working, and measure these in ways that are relevant to tangata whenua and communities.

Understanding is key to making good decisions about where we invest our resources, so we can enable **kia takatū tātou**: long term economic and social development. These decisions range from frontline staff choosing the right type of support, to partner services we purchase and how we provide robust options for ministers. It also includes answering enduring research questions about how the welfare system is functioning and what we can do to improve.

Moving from...

In some areas MSD knows the impact of services and initiatives, but we don't measure everything that matters.

Data needs can be an after-thoughts during change processes, so we don't understand what is happening and how data works together.

...to...

We respect views of tangata whenua and partner with them to implement the right frameworks to design services and understand outcomes for tangata whenua and hāpori

We have a rich understanding of what is happening, what works for whom and why across meaningful outcomes.

We have a deep understanding of our performance and the effectiveness of the system, including the strength of communities.

We think ahead, designing for the insights we will need to support good decisions.

Different perspectives are considered, and groups consulted with in the collection, use, sharing and management of information.

When this is working well:

We are measuring outcomes that matter to people and their whānau, so we have a holistic understanding of their specific needs, circumstances and communities. This is represented in the **Better Outcomes Framework** and **Development of Data Assets** in our roadmap.

Our insights enrich our understanding of how well welfare supports meets the needs and preferences of people, their whānau and communities. We measure and can explain the performance of the welfare system, providing a suite of **Investment Tools** so national and regional decision makers can ensure we're making the best use of our resources. We use information and insights to **Enable early intervention** where it can have the biggest impact.

We publish our data and insights via **Secure & Efficient Data Sharing** and

Self-service BI for client, iwi and partners to leverage, ensuring they are easily accessible and understood. We take into account the different perspectives and skills of those we are sharing information with.

We use our **Collaborative Analytics & Data Science Platform** to develop mutually beneficial insights with partners and other agencies. We also provide a **Self-Service BI** to empower people to use the data we hold to make better decisions for their communities.

We have effective **Capability Development** processes and a culture that builds the data literacy of staff and partners so they can use data products to make good decisions. We work with 'analytics by design', assessing the data needs when we make system or service changes, so we can create insights to make good decisions. We understand how our different channels and systems interact through **Omnichannel analytics**, so they're as effective as possible.

Deliver personalised and proactive insights specific to the unique needs and circumstances of people, their whānau and communities

Our ability to deliver **personalised** services is dependent on effectively combining quality, available data and information with an understanding of needs and what works for different people.

Personalisation is important because...

The support New Zealanders need is not one size fits all: **mana manaaki** means delivering support that's right for people in their current situation and what they want to achieve.

This includes making relevant information about suitable services nearby available to case managers as they're working with clients, to job matching suggestions for clients and employers, or real-time, intelligent recommendations to help people find out what they're eligible for, regardless of the channel they choose.

Personalisation helps us scale our support and knowledge beyond one to one interactions, through effective self-service options and decision support tools, so we can help more New Zealanders.

We will use personalisation and automation safely: with appropriate human oversight, and by assessing trade-offs in accuracy, transparency, bias and discrimination.

When this is working well:

We are delivering relevant information and insights when they're needed for decisions. This includes **Enabling automated decision making** and **Enabling recommendations** where appropriate, to make processes more efficient and provide a great user experience. We also provide a range of **Embedded analytics**: customised decision support tools within our applications.

Specific examples include **Supporting employment platform data & analytics** to deliver effective job matching for jobseekers and employers and **Omnichannel analytics**, which provide consistent recommendations to people regardless of the system or channel they're working in.

Moving from...

MSD uses very little personalisation to help with individual decisions. We rarely use information and data to provide tailored services, so systems and processes can be poorly targeted and confusing which causes inconsistent service delivery and outcomes.



...to...

We apply ethical analytics to personalise interactions, provide relevant content, insights and recommendations and deliver a safe and efficient user experience.

Analytics are delivered at the right time, to the right person, in the right way to support decisions.

Tangata whenua (hapū/iwi) have relevant and timely data and information, so they are empowered to make informed decisions for their whānau.

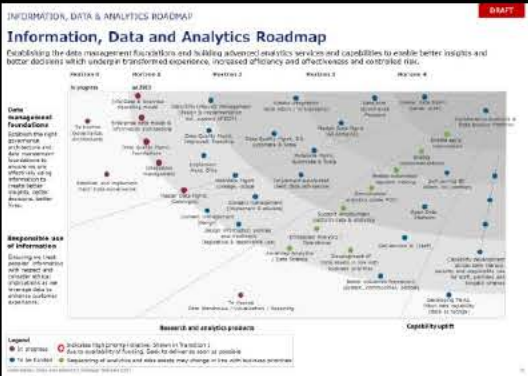
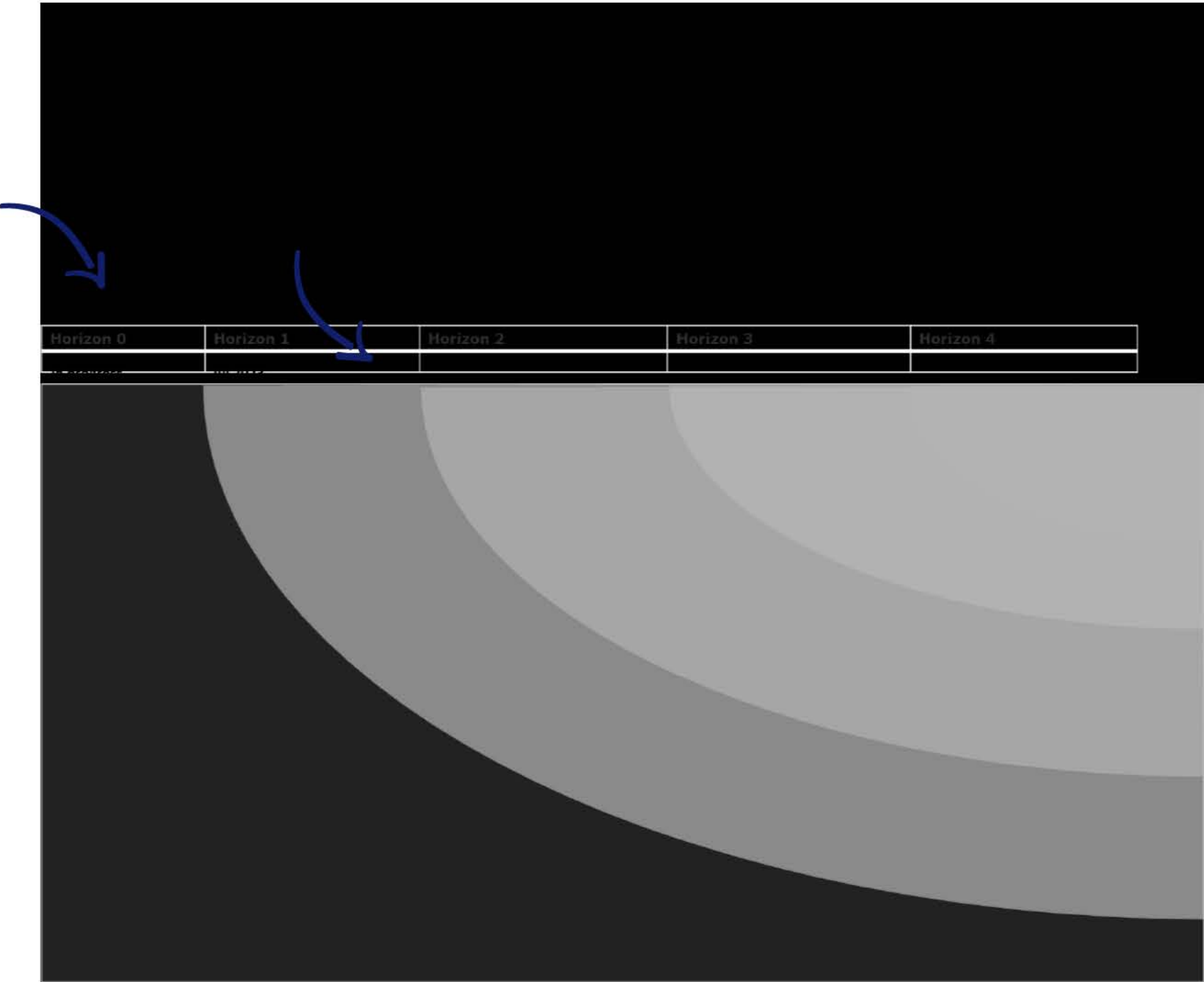
The personalisation we deliver is sustainable by working within a clear **Information, data and analytics operating model** and strong **Advanced Analytics/Data Science** capability to deliver or support the right solutions.

We invest in **Data capability development** so that our staff have data literacy to effectively carry out their roles, and collaborate with partners on our **Collaborative Analytics & Data Science Platform**, to further improve personalisation where appropriate. We also invest in **Development of data assets** that are necessary for effective personalisation.

The Information, Data & Analytics and Security roadmaps are presented across five horizons to align with Te Pae Tawhiti Transformation Programme horizons.

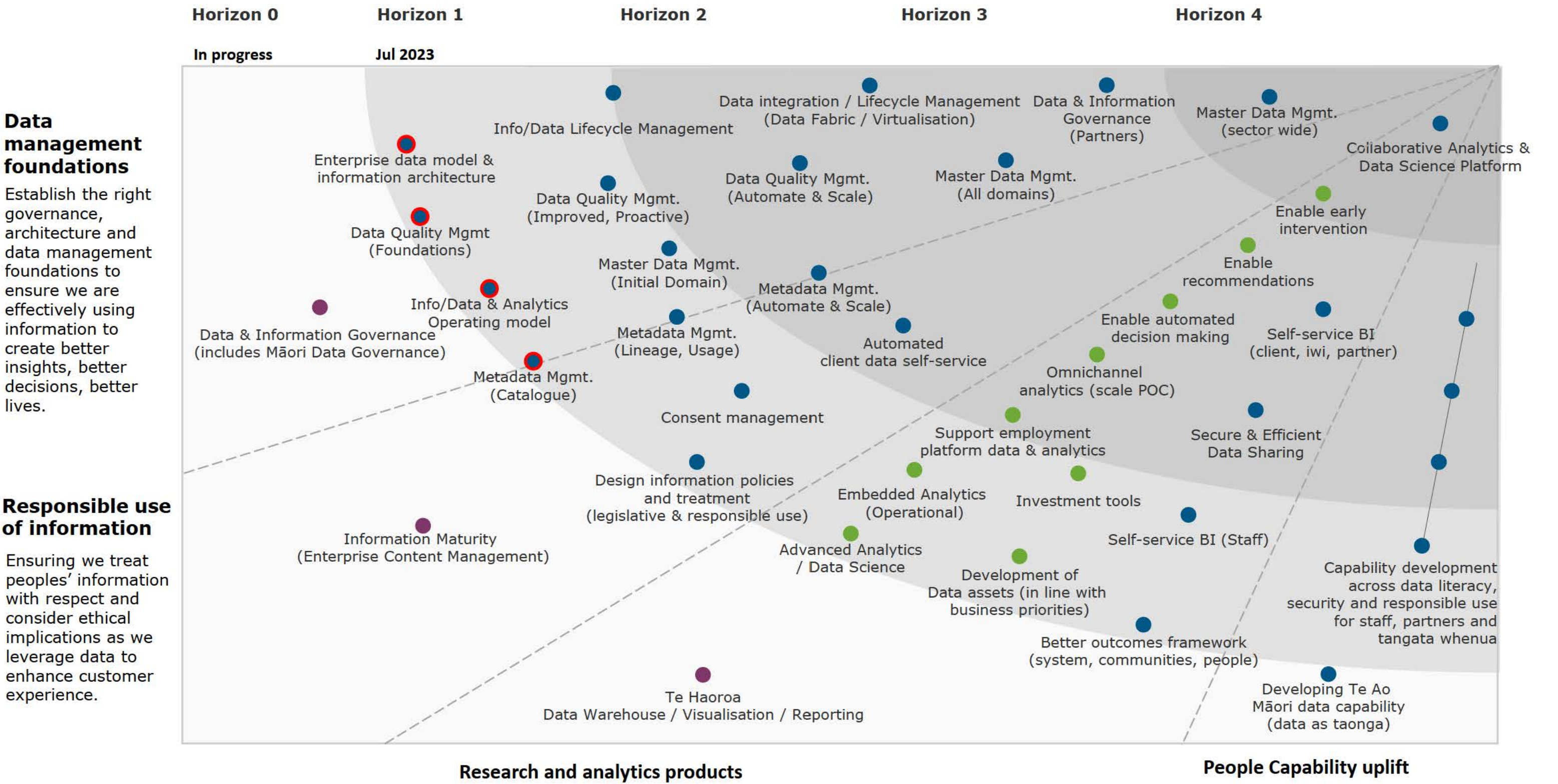
Activities depicted in Horizon 0 are already funded and on the committed delivery plan.

Where Te Pae Tawhiti Programme identifies the need to accelerate any other activities into Horizon 0, funding will need to be sourced accordingly.



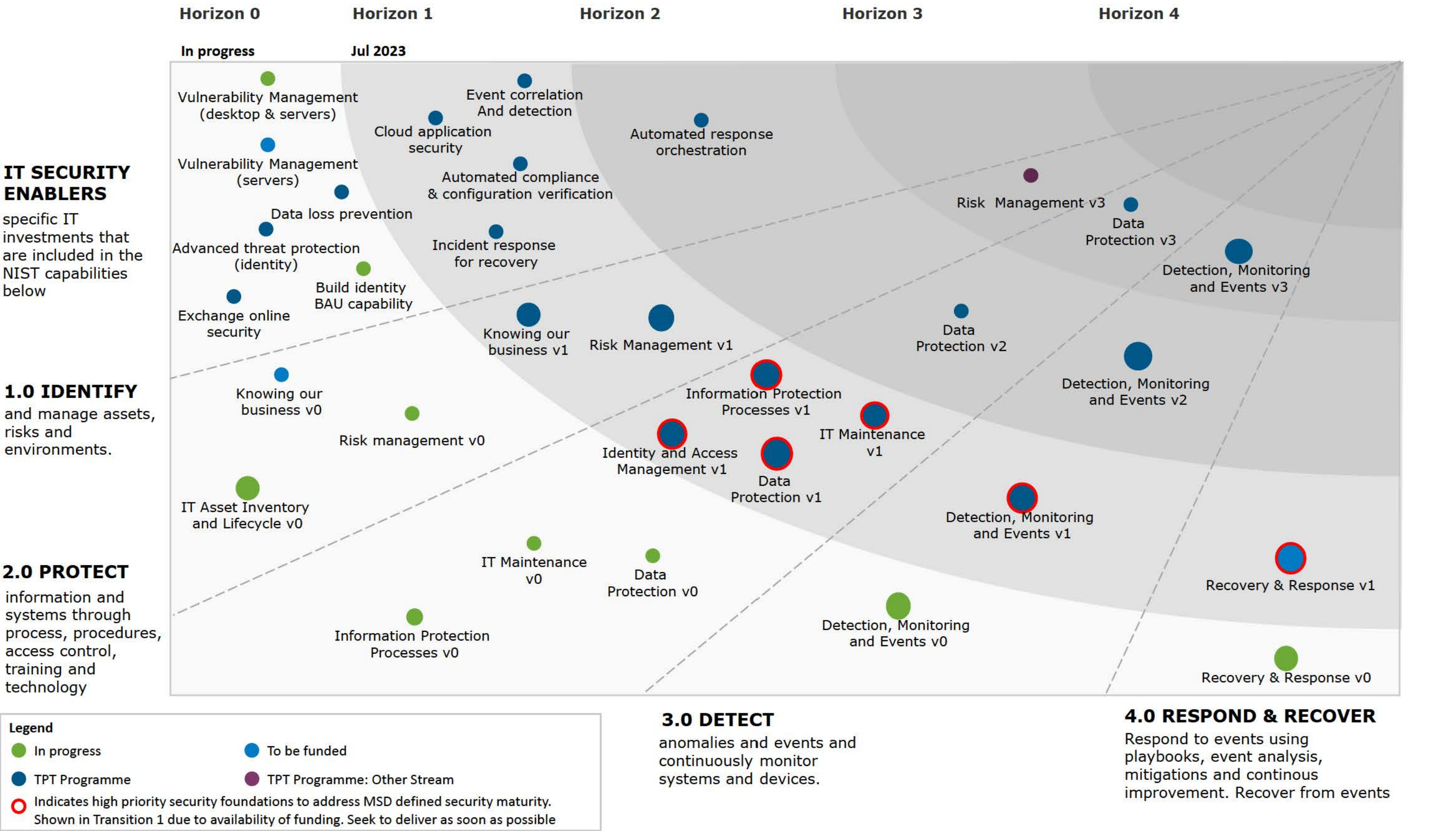
Information, Data and Analytics Roadmap

This shows how we will establish the data management foundations and advanced analytics services and capabilities. This will deliver better insights and better decisions which underpin transformed experience, increased efficiency and effectiveness and controlled risk.

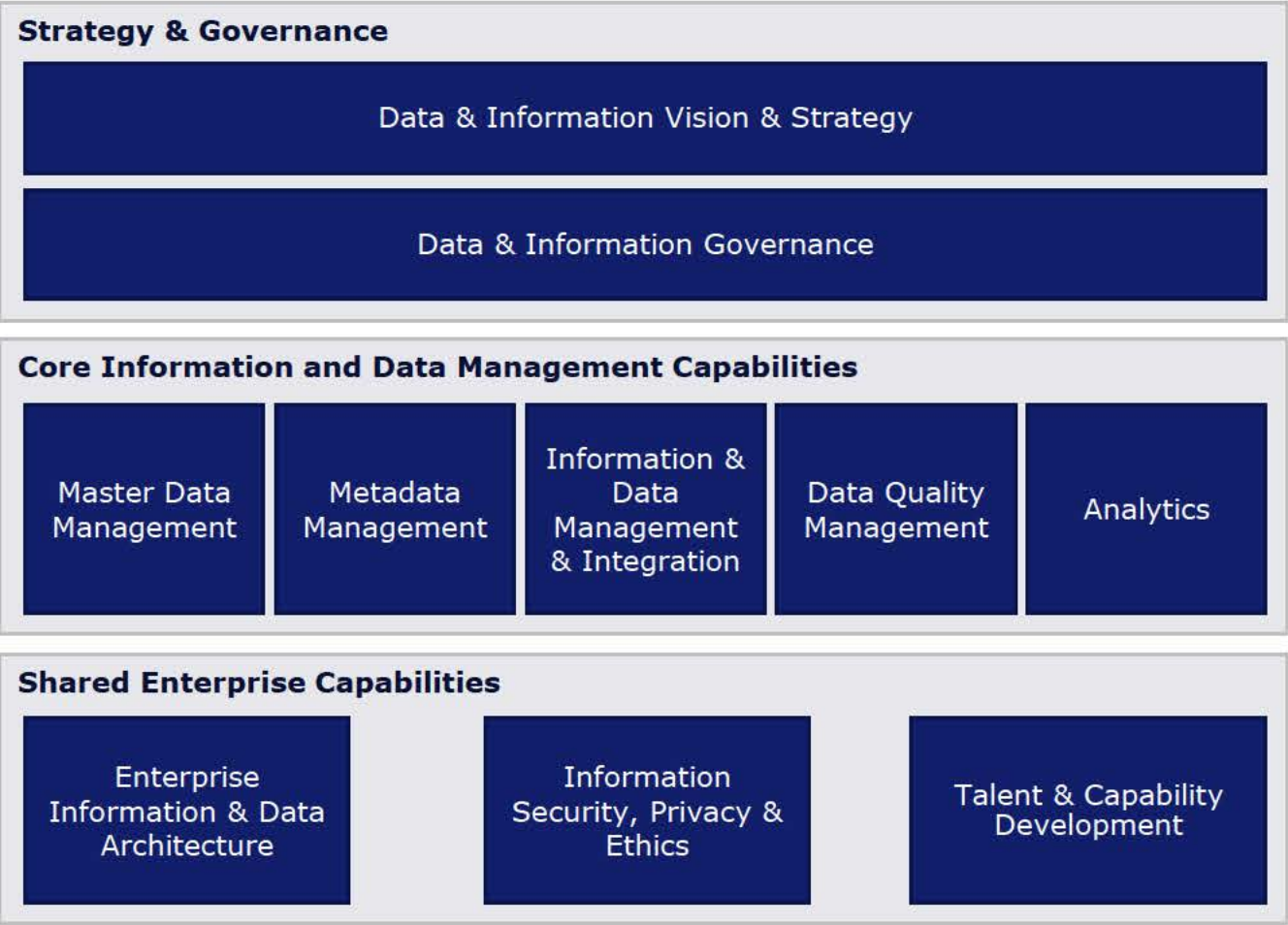


Information Security Roadmap

Information security foundations address current gaps in MSD’s defined maturity objectives to support identification, detection, response and recovery from incidents and unauthorised activity.



Information, Data and Analytics Capabilities



The Information Data & Analytics Roadmap identifies series of initiatives that will continue to evolve the maturity of each of these Information and Data Management business capabilities.

Capability	Definition
Data & Information Governance	Data governance is a steering function that sets standards for data, and monitors the performance of data management functions, so we can prioritise work on our most important data and we have confidence in using data for decisions. It also includes ownership and accountability, incorporating Maori Data Governance.
Master Data Management	Master data management is about ensuring that we use consistent up-to-date information across our business, so that we are delivering services accurately and people do not need to re-tell their story.
Metadata Management	Metadata helps us find the right data, understand what it means, know where data came from, where it is being used, and the rules for access and sharing the data. We know what we can do with the data and what is useful for.
Data Quality Management	Data quality management is an operational function that maintains high-quality data, so we have confidence in the decisions. This involves measuring and monitoring quality, and fixing data errors, and matching data.
Information & Data Management & Integration	Data integration, pipeline management and lifecycle management ensures we can access the relevant data when we need it, get it to the right systems in the appropriate format, and that it is kept safe until it is disposed of. This capability includes the shared storage of information so that it can be accessed for many current and future use cases.
Data Analytics	Data analytics allows us to personalise interactions, provide relevant recommendations and deliver a safe and efficient user experience. We use data analytics to understand what has happened, why, and what can be improved in our services to deliver better outcomes.
Enterprise Information & Data Architecture	Enterprise Information (Data) Architecture designs and maps all of the information and data across all of our systems, so we can understand how things connect and who we can make changes to improve our use of data.
Information Security, Privacy, Human Rights and & Ethics	Information Security, Privacy, Human Rights and & Ethics ensures we use data and information responsibly, protects and keep it safe, respect privacy, and use it ethically. This covers the frameworks, and policies, and operational assurance.
Talent & Capability Development	Ensure people have the right skills to use data, information, and data products, effectively and responsibly to do their job. They understand the value of data and information and manage it appropriately to ensure quality for decisions.



**MINISTRY OF SOCIAL
DEVELOPMENT**

TE MANATŪ WHAKAHIATO ORA

Appendix - Roadmap Initiatives



Establish the right governance, architecture and data management foundations to ensure we are effectively using information to create better insights, better decisions, better lives.



Info & Data Governance (includes Māori Data Governance)

Implement an information governance framework with supporting capabilities, processes and policies. Broaden role of data stewardship from information access control to information quality management.

Develop a co-designed model to approach data governance in a way that embeds iwi-Māori needs and interests in data. We partner with tangata whenua to ensure that kaitiakitanga (stewardship) is at the heart of how we take care of data.

Data stewardship practice drives ongoing maturity and practice improvement across organisation, where data governance is a formalised MSD business function.

Info/Data & Analytics Operating model

The organisation structure for data and analytics operating model is fully embedded and supports data governance, support each level of strategy, management and operations.

Enterprise data model & information architecture

The enterprise data model will provide a holistic view of the data across the organisation and can identify where information is in common, ensuring our data architecture is structured and is intentional.

We have an Enterprise Information view on both our structured and our unstructured information to demonstrate people are at the centre of the information. We map the enterprise information model to MSD business processes and systems that create, read, update, or dispose of information.

Our data architecture captures outcomes valued by iwi-Māori and pacific communities, building tight alignment with the all-of-government data model to support ease of reporting social outcomes across the ecosystem.

Metadata Management

Create a common metadata foundation to deliver insights and intelligence across all data management processes. Data, information, and insights can be found quickly and easily by anyone who needs it, using an Enterprise Data Catalogue. All domains are identified and described, and metadata reflects Te ao Maori needs.

We capture data movement information to support the data lineage and provenance, ensuring we have an understanding of, and confidence in, the data assets maintained.

Establish the right governance, architecture and data management foundations to ensure we are effectively using information to create better insights, better decisions, better lives.



Data Quality Management

Establish Data Quality (DQ) foundations, with adoption of data quality management framework and data cleansing practices, prioritised to meet initial data quality targets.

Continue the data quality improvement programme to enhance the effectiveness of initiatives, with ongoing monitoring and proactive interventions to address data quality issues.

In the third phase, we will use AI to automatically assess data quality and make intelligent recommendations that streamline key tasks like data discovery and data quality rule creation across the organization.

Data integration, pipeline management & lifecycle management

Information and Data Lifecycle management is embedded in our Information Management processes. We have modern, managed, information management system and enterprise corporate information repository. Knowledge Management is integrated with information management lifecycle

We adopt standards-based approaches for organizing, storing, and managing our data, to ensure we can share data assets across the Ministry and with partners and other agencies

Data management and integration to establish the data fabric to support flexible, reusable and augmented data integration pipelines. Support real-time / event-based streaming of data from multiple applications / organisations.

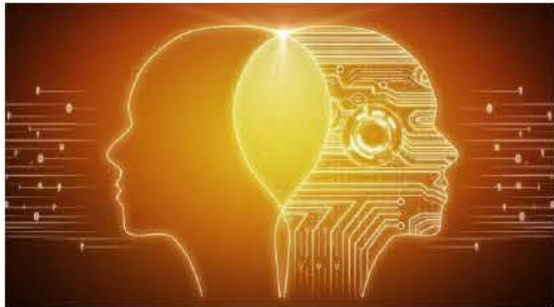
Master Data Management

Establish the organisation, roles and responsibilities, and metrics for Master Data Management (MDM). We have an authoritative source of truth for Party (client, iwi, staff, partner) so that clients do not need to re-tell their story.

We evolve this capability to have an authoritative source of truth for all of our data domains (eg Person, Whanau, Products/Services, Location etc). We can provide an integrated joined up view of our data and information across the ministry and services. We can effectively manage changes to the data across the Ministry to ensure accuracy and consistency.

In the third level of maturity we can scale our MDM through AI and ML to leverage algorithms to enhance our data matching, resolving differences, and providing recommendations. We extend the capability across the social sector. Where we have permission to do so, we validate the data we hold, directly with external authoritative sources rather than collecting mass data sets and ingesting them into our data system.

Ensuring we treat peoples’ information with respect and consider ethical implications as we leverage data to enhance customer experience.



Information Maturity (Enterprise Content Management)	<p>We will improve our Information Maturity, and deliver a modern, managed, information management system and enterprise corporate information repository.</p> <p>Our people can easily access and reference both published content as well as discoverable content across our digital collaboration channels.</p> <p>Our people are increasingly needing to communicate and collaborate with secure and responsible sharing of Ministry information with our partners and external agencies</p> <p>Information is classified and tagged across all our systems with automated management of access, retention and disposal based on this.</p>
Design information policies and treatment (legislative & responsible use)	<p>Design information policies to ensure we treat information about people as an extension of the person and use it fairly, with respect for the people it is about, and in a way that delivers clear benefits for the person and/or for New Zealanders.</p> <p>We consider privacy, ethical use, respect diversity and prevent bias and discrimination, in how we share information and insights, apply predictive analytics, and use algorithms to support automated decision and recommendations.</p>
Consent Management	<p>We will design and implement a comprehensive consent framework to ensure we are using peoples’ information responsibly and respectfully.</p>
Automated client data self-service	<p>Through our digital experience platform, clients will be able view the personal information they have shared with us, how it has been used within MSD and across the sector and update, manage or delete any information without interacting with an MSD staff member.</p> <p>Providing client data self service capabilities will provide our people and their whānau with transparency as to how and where their data will be used, control and choice over what data is shared across the sector and the purpose in which MSD is authorised to use it for.</p>

Enabling personalised, proactive and preventative services and an organisation that leverages insights to improve services, operations and policy



Te Haoroa – Data Warehouse, Visualisation & Reporting

Implement a new data warehouse with well defined data governance and management so that MSD has improved business intelligence, reporting and analytics capabilities. Te Haoroa Data Warehouse is a current in-flight programme of work to replace the existing ageing data warehouse.

Advanced Analytics / Data Science

Build upon our data platform, adding advanced analytics and data science capability to deliver real-time recommendations, personalised services and predictive analytics required to respond early. Our advanced analytics platform will support quick prototyping through to operational models that optimise service delivery, with capability for real-time streaming and analytics.

Better outcomes framework (system, communities, people)

We are measuring outcomes that matter to people and their whānau, so we have a holistic understanding of their specific needs, circumstances and communities. We enrich our understanding of the performance of the welfare system and the effectiveness of our interventions for the different groups we support.

Development of Data assets in line with business priorities

Having the right data is a key enabler for our future services in Te Pae Tawhiti, like an enhanced and personalised experience for customers, staff and partners. We will develop data assets as they're needed, such as data marts that provide up-to-date, accurate information for income support eligibility or local employment opportunities.

Embedded Analytics / Operational

Using our advanced analytics platform, we will deliver our analytics into our client, staff and partner platforms to enable integrated, real time decision support tools. These will complement and enhance in-built analytics delivered by platforms 'off the shelf'.

Self-service BI (Staff)

Build upon our data platforms to provide the tools to empower our staff with self service business intelligence capabilities. This requires tools and platforms to support business users in:

- Self service data preparation and discovery
- Interactive visualisation and creation of personal dashboards
- Geospatial and network analytics
- Appropriate data governance and processes to productionise successful data products

Secure & Efficient Data Sharing

We will build and implement data sharing tools, frameworks and processes so it's clear what we're sharing with partners, how it's authorised and that it's shared safely and efficiently.

Enabling personalised, proactive and preventative services and an organisation that leverages insights to improve services, operations and policy



Investment tools	Investment tools are the data and analytics products that help us understand where we're investing our resources, so we can assess and improve the outcomes we're achieving. This includes tools that give insight into our employment investment, so we can make national and regional purchasing decisions that reflect that changing needs of our clients and employers.
Support Employment platform data & Analytics	The Employment platform will provide self-service job matching and training recommendations, for jobseekers, employers and MSD staff who support them. Much of this functionality will be provided 'off the shelf', with additional data assets, analytics and research to enhance functionality and user experience.
Omnichannel Analytics	Omnichannel analytics let us understand end to end client journeys and provide consistent recommendations, regardless of how people switch between channels. They measure the performance of systems and identify pain points in our processes. Omnichannel analytics are enabled by good data management to maintain links between different workflows.
Enable Auto Decision Making	Automated decision making can improve the efficiency and effectiveness of our services, but needs accurate data to implement, assessment for bias and ongoing monitoring. This item covers the information and data support needed, including develop tools and processes.
Self Service BI (Client, Iwi, Partner)	Build upon our open data platform to provide self service reporting for clients, iwi and our partners. This requires tools and platforms to support: <ul style="list-style-type: none"> • Self service data preparation and discovery • Interactive visualisation, creation and sharing of personal dashboards • Appropriate security and data governance
Enable Recommendations	Develop the analytical models required to enable real-time recommendations and personalised services for clients and staff. Specific products and models will be driven by business priorities.
Early Intervention	Develop the analytical products required to respond early, including predictive analytics, segmentation or research to identify groups who need support and how to deliver it. Specific products and models will be driven by business priorities.
Collaborative Analytics and Data Science Platform	Establish a collaborative data science platform which will enable us to work with partners and other agencies on mutually beneficial data products. These products may be for research purposes, hosted as open data products, or to support joined-up operational delivery.



5.1	Developing Te Ao Māori data capability (data as taonga)	<p>We have built and have an ongoing focus on the capability of our staff and leaders to engage competently on Māori data issues and are aligned with cross-government approaches, like Mana Ōrite.</p> <p>We supporting whānau Māori and iwi, and Māori research organisations, to grow the capacity of the research sector.</p>
5.2	Capability development across data literacy, security and responsible use for staff, partners and tangata whenua	<p>Ministry staff, providers, vendors and partners are aware of the cyber security risks facing the Ministry and are appropriately informed and trained to protect and use information responsibly.</p> <p>We develop the culture and build the data literacy of staff and partners so they can use data products to make good decisions. We work with 'analytics by design', assessing the data needs when we make system or service changes, so we can create insights to make good decisions.</p>



Information Security Roadmap Initiatives



Identity and manage assets, risks and Environments



- Understand the assets services functions of MSD and its technology

I.1 Knowing our business v0	<p>The Ministry has a clear understanding of how its business operates and the context it operates in and this flows down into the data we collect, the assets we protect, our understanding of risks to our clients and business and what our roles and responsibilities are to the people of New Zealand. Includes:</p> <ul style="list-style-type: none"> • Documenting critical business processes including dependencies on systems, sites and external partners • ICT and Organisational Resilience requirements are understood • Critical systems and processes are identified • The Ministry's objectives are fed into all IT initiatives
I.2 Risk management v0	<p>The Ministry reviews and understands the risks of the environment its operating in and actively assesses and responds to the changes in security risks. The Ministry understands and manages its security risks. Security risks are fed into operational decisions and prioritisation. This horizon includes embedding Assurance Framework (INF-108)</p>
I.3 IT Asset Inventory and Lifecycle v0	<p>The Ministry knows and automatically tracks the state of all its technology so that we can be sure that we use our assets responsibly and ensure that our assets are ready and have appropriate protection to hold our client's information and ensure its is available for staff and clients.</p> <ul style="list-style-type: none"> • Inventory of servers, applications, user devices • Auto discovery of assets • Cloud and external systems inventory • Classification of technology assets based on classification, criticality and value • Cyber security roles clarified for staff and 3rd parties
I.4 Knowing our business v1	<p>Ongoing improvements to improve understanding and knowing our business</p> <ul style="list-style-type: none"> • The organization's role in the supply chain is identified and communicated • The organization's place in critical infrastructure and its industry sector is identified and communicated
I.5 Risk Management v1	<p>Further improvements including Threat Intelligence and Threat Information Sharing</p>
I.6 Risk Management v3	<p>Further improvements in risk management include:</p> <ul style="list-style-type: none"> • The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis • Security risks and controls are centrally managed • Security risks and controls are fed into enterprise risk assessments

Protect information and systems through process, procedures, access control, training and technology



P.1 Identity and Access Management v0	<p>The Ministry can manage identity and use it as the front-line protection of information and systems, providing enforcement of access across devices, environments and applications. Includes:</p> <ul style="list-style-type: none"> • Privileged Access Management • Multi-factor Authentication rollout for front line applications • IGA rollout • Access Control for APIs • Client Identity and Access Management • Partner Lifecycle Management and Governance • Workforce Capability Rollout and Onboarding Authentication • Maturing the Identity Capability • Decentralised Identity • Strengthen Key Management Processes
P.2 Data Protection v0	<p>The Ministry can protect information on any device anywhere by establishing trust and applying automated, risk-based controls. Includes:</p> <ul style="list-style-type: none"> • Corporate Web Proxy • Data Loss Prevention for M365 and Exchange Online
P.3 IT Maintenance v0	<p>The Ministry maintain and repairs its IT systems inline with policies. Includes:</p> <ul style="list-style-type: none"> • Patch Management (INF-120)
P.4 Identity and Access Management v1	<p>Completion of all epics initiated in Horizon 0 (Identity & Access Management v0)</p>
P.5 Information Protection Processes v1	<p>The Ministry has an information protection processes and procedures in place across all IT and business capabilities including change, configuration and system deployment. Includes improvements to establishing a Secure SDLC.</p>

Protect information and systems through process, procedures, access control, training and technology



P.6 Data Protection v1	Further improvement to Data protection including: <ul style="list-style-type: none"> • Data Loss Prevention Endpoint • Data Loss Prevention Network • Extend BYOD access to existing service • Extended BYOD to include android devices
P.7 IT Maintenance v1	Further improvement to IT Maintenance including: <ul style="list-style-type: none"> • Configuration Management • Microsoft Defender for Servers
P.8 Data Protection v2	Further improvement to Data protection including: <ul style="list-style-type: none"> • Application Proxy for business-critical applications
P.9 Identity and Access Management v2	Further IdAM improvements including; <ul style="list-style-type: none"> • Application Access Control and Entitlement Enforcement
P.10 Data Protection v3	Further improvement to Data protection including: <ul style="list-style-type: none"> • Anywhere, any device

Detect anomalies and events and continuously monitor systems and devices



D.1 Detection, Monitoring and Events v0	<p>The Ministry has tools in place to detect security incidents and assess the potential impacts to information and systems. Ministry assets are actively and automatically scanned and monitored for vulnerabilities. Centralised device and network telemetry</p> <p>Includes:</p> <ul style="list-style-type: none">• Security Information and Event Management (SIEM) (INF-98)• Vulnerability Scanning (INF-97)
D.2 Detection, Monitoring and Events v1	<p>Further improvements for detection monitoring and events, include:</p> <ul style="list-style-type: none">• Security Orchestration Automation and Response (SOAR) to define incident analysis and response procedures in a digital workflow format.• Risk based alerts• Cloud Access Broker (CASB) - Possible move to V0• Vulnerability identification on servers• Network vulnerability scanning• Centralised device and network telemetry
D.3 Detection, Monitoring and Events v2	<p>Further improvements for detection monitoring and events, include:</p> <ul style="list-style-type: none">• Centralised device and network telemetry
D.4 Detection, Monitoring and Events v3	<p>Further improvements for detection monitoring and events, include:</p> <ul style="list-style-type: none">• Threat Hunting• Attack simulation• AI/ML based Anomaly Detection

Respond to events using playbooks, event analysis, mitigations and continuous improvement.

Recover from events



<div>R.1</div> <div>Response & Recover</div> <div>v0</div>	<p>The Ministry has processes in place to respond to security incidents. These processes are regularly tested against risk-based scenarios and are maintained.</p> <p>The Ministry has business and technology recovery plans in place to recover from incidents. These recovery plans are regularly tested against risk-based scenarios and are maintained.</p> <p>Includes:</p> <ul style="list-style-type: none">• Security Incident Management improvements (INF-126)• BCP Framework• DR for core functions• Establish a Data Bunker• BCP Communications Framework
<div>R.2</div> <div>Response & Recover</div> <div>v1</div>	<p>Further improvements include:</p> <ul style="list-style-type: none">• Baselined BCPs• "Alternate IT" solution• Embed Resilience NFRs in solution designs

IT Security Enablers

IT Investments that contribute to the maturity improvements in the previously listed capabilities

IT Security Enabler	NIST Capability Initiatives	
Vulnerability Management (desktop & servers)	I.5 Risk Management v1	Automated alerting of vulnerabilities, known threats and breaches of security guardrails. Microsoft Defender
Vulnerability Management (servers)	P.5 Information Protection v1	Scanning testing, and implementation of vulnerability plan
	P.7 IT Maintenance v1	Microsoft Defender for Servers
	D.1 Detection, Monitoring and Events v0	Vulnerability Scanning (INF-97)
	D.2 Detection, Monitoring and Events v1	Vulnerability identification on servers
Data loss prevention	P.2 Data Protection v0	Data Loss Prevention for M365 and Exchange Online
	P.6 Data Protection v1	Data Loss Prevention Endpoint Data Loss Prevention Network
Exchange online security	P.2 Data Protection v0	Data Loss Prevention for Exchange Online
Advanced threat protection (identity)	P.1 Identity and Access Management v0	Microsoft Defender for Identity (Advanced Threat Protection)
	D.1 Detection, Monitoring and Events v0	Detect anomalies in Azure AD
Build identity BAU capability	P.1 Identity and Access Management v0	IDAM capability stood up in IT, Internal (staff) and external (clients, partners) identities managed throughout the lifecycle
Cloud Application Security	I.3 IT Asset Inventory and Lifecycle v0	Auto discovery of assets. Cloud and external systems inventory
	P.9 Identity and Access Management v2	Application Access Control and Entitlement Enforcement
	D.2 Detection, Monitoring and Events v1	Cloud Access Security Broker (CASB) - Microsoft CAS
Automated compliance & configuration verification	P.7 IT Maintenance v1	Further improvement to IT Maintenance for Configuration Management
	P.5 Information Protection Processes v1	Configuration change control processes are in place
Incident response for recovery	R.1 Response & Recover v0	
Event correlation and detection	D.1 Detection, Monitoring and Events v0	Security Information and Event Management (SIEM) (INF-98)
Automated response orchestration	D.2 Detection, Monitoring and Events v1	Security Orchestration Automation & Response (SOAR) to define incident analysis and response procedures in a digital workflow format.
	R.2 Response & Recover v1	Further improvement response processes

Information Governance Policy

Last Review Date:	November 2024
Next Review	November 2026
Date:	
Approved by:	Organisational Health Committee
Owner:	General Manager Information (CISO, CPO)

Purpose

This policy defines the principles, roles, and responsibilities which support the Ministry of Social Development (the Ministry) in upholding its Information Governance responsibilities to the New Zealand Government and public. The principles found in this policy set the governing direction and intent for Information Governance. Underpinning this policy are standards, patterns, processes, and guidance material which collectively operationalise the principles in this policy and align the Ministry's Information culture and decision-making.

Policy Statement

The Ministry holds and uses information (including personal information and data) about people that impacts their lives. Information is taonga, and as its stewards we must both use it responsibly and protect it while it is in our care.

Effective information governance requires the Ministry to understand the information it holds, define who is responsible for that information, and know how that information is being used. Additionally, it requires the Ministry to have assurance that its information is protected, is managed appropriately, and its staff are acting responsibly when using information.

Scope

This policy applies to all Ministry staff including contractors; all information and data held and used by the Ministry; and all activity conducted by third parties on behalf of the Ministry.

Policy Principles

The following principles must be understood and followed to ensure alignment with the purpose of this policy.

1. The Ministry's information assets are identified and appropriately protected based on legislative requirements, information value and risk culture

The Ministry manages information assets in accordance with the requirements defined in key legislation such as the [Public Records Act 2005](#), [Privacy Act 2020](#), and the [Official Information Act \(1982\)](#), along with policy guidance such as the [Protective Security Requirements](#) (PSR). The Ministry's standards and other guardrails define the measures which set the baseline for how information assets are collected, secured, stored, used, and managed using a risk-based approach.

2. All information assets held by the Ministry have responsible Information Asset Owners to ensure they are managed and used appropriately

An information asset has value to the Ministry from the point of creation or collection through to its eventual disposal. Information Asset Owners are responsible for ensuring the risks to, and the opportunities for, their corresponding information assets are understood, managed and monitored throughout the information asset's lifecycle. Information Asset Owners are also responsible for how their information assets are used, including use with algorithms or other tools. Any legal and regulatory requirements applicable to the collection, storage, use, disclosure or disposal of the information must be understood by the Information Asset Owner.

3. Information assets are fit-for-purpose to promote informed decision-making

Consistently and continuously maintaining the quality and integrity of Ministry information assets ensures people use authoritative information. The information collected, used, and shared by the Ministry is appropriate for the purposes it is intended and collected for, and contributes towards better insights, better decisions, and better lives.

4. The Ministry partners with tangata whenua in decision-making about information held by the Ministry to support Māori

The Ministry fosters collaborative relationships with Māori communities to ensure their voices are heard and respected in decisions about information held by the Ministry that impacts their lives. The Ministry values the trust placed in it by Māori and is dedicated to embedding Māori perspectives into the way it cares for and manages Māori information. Upholding its responsibilities to its Accord partners, the Ministry is committed to working alongside key partners to support decisions about how Māori information is governed.

5. The protection and responsible use of Ministry information is everyone's responsibility

Ministry staff are responsible for handling information appropriately while it is in our care. Ministry technology and processes play a key role in providing a layer of protection over information, and our awareness of information risk and its acceptable use is just as important. The Ministry expects staff to act in a timely and coordinated manner to prevent or respond to breaches of, and threats to, information.

Roles and Responsibilities

Everyone that works for or is contracted to the Ministry has a responsibility to comply with this policy. The responsibility of each role specifically relevant to this policy is set out in the table below:

Person/Party	Responsibility
All Staff	<p>All staff are responsible for:</p> <ul style="list-style-type: none"> • Complying with the Ministry's information policies • Following information guidance and training • Identifying and reporting information security, information management, and privacy incidents • Escalating risks, as needed, to their manager
Managers	<p>All managers are responsible for:</p> <ul style="list-style-type: none"> • Leading and facilitating regular information discussions with their teams • Ensuring their teams are familiar with the Ministry's information policies and guidance; use approved tools, and comply with the Ministry's information governance approach • Providing direction on acceptable behaviours to their teams • Modelling good information practice through their actions and behaviour • Identifying and escalating information risks, as appropriate, to ensure information is managed effectively at the appropriate level and in a timely way • Reporting any information security or privacy incidents to their line manager

Person/Party	Responsibility
Information Asset Owners	<p>All information assets owners are responsible for:</p> <ul style="list-style-type: none"> • Leading and championing a culture that values protection and responsible use of information; • Understanding which information assets, they are accountable for, their value, where they come from, and how they are used; • Knowing who has access to that information and why and ensuring that access is controlled and reviewed continuously; • Ensuring the risks to, and the opportunities for, their corresponding information assets are managed and monitored; and • Ensuring their information assets are fully utilised in line with responsible information use. <p>The information asset owner must understand the value of each information asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information asset.</p> <p>At the Ministry, Information Asset Owners will typically be assigned at the Tier 3 senior leader level, reporting directly to Deputy Chief Executives (DCEs).</p>
Information Stewards	<p>Information Stewards are responsible for:</p> <ul style="list-style-type: none"> • Maintaining specialist knowledge about the information in their business area. • Ensuring information is available for its intended purpose; • Managing and maintaining information assets based on MSD standards, policies, and other guardrails, including data quality, integrity, and metadata; • Maintaining and updating an inventory of information assets; • Monitoring and optimising the lifecycle of information to effectively manage risk and opportunities; • Collaborating with stakeholders across the business (System Owners, other Information Stewards, Business

Person/Party	Responsibility
	<p>Capability owners, and Line 2 assurance functions, etc.) to implement the necessary guardrails;</p> <ul style="list-style-type: none"> • The responsible use of information assets, enabling the organisation and other agencies where appropriate to gain maximum value from the information; and • Supporting information asset owners to make informed decisions about the management and use of their asset for the duration of its lifecycle. <p>The Information Steward must keep the Information Asset Owner informed and aware of any risks or concerns surrounding the integrity or safety of the information.</p> <p>At the Ministry, Information Stewards will be assigned by the Information Asset Owners and are typically senior subject matter experts in their respective business areas.</p>
Information Governance Committees	<p>Information governance committees are responsible for overseeing and tracking the achievement of the Ministry's strategic objectives relating to information governance. They set the overall risk culture for the Ministry, which guides the way it responds to information risk and opportunity.</p> <p>These governance bodies must have membership from the Ministry's Leadership Team, as well as appropriate Māori representation, and have oversight of:</p> <ul style="list-style-type: none"> • Information and IT security policies and strategies • Information standards and architecture • Obligations contained in the Protective Security Requirements (PSR), the Privacy Maturity Assessment Framework (PMAF), and the Archives New Zealand Information and Records Management Standard • Ministry decisions about ensuring there are adequate systems, processes, and controls in place to identify and manage information risk. <p>At the Ministry, the Information Governance Committees consist of the Leadership team (LT), Organisational Health Committee (OHC), the Information and Protective Oversight Committee (IPSOC), the Transformation and Investment Committee, and Tai Nuku Design Committee.</p>
Executive Sponsor Information	<p>The Executive Sponsor champions the importance of information management among the organisation's leadership. The aim is for everyone in the organisation to see information management as an integral part of a business operating</p>

Person/Party	Responsibility
	<p>effectively. The Executive Sponsor Information is responsible for:</p> <ul style="list-style-type: none"> • Ensuring that the strategy and policy adopted by the organisation supports information management • Being involved in strategic and operational planning to align information management with the corporate objectives and business activities of the organisation • Liaising with business units to ensure that information is integrated into work processes, systems, and services • Overseeing the budget for information and ensuring the resources needed to support information are known and sought in funding decisions • Ensuring that staff with appropriate skills to implement information strategies are employed, and regular upskilling is available • Monitoring and reviewing information to ensure that it is implemented, transparent and meets business needs <p>The CE has delegated the Executive Sponsor Information role to the DCE Organisational Assurance and Communication (OAC).</p>
Chief Security Officer	<p>The Chief Security Officer (CSO) is responsible for having oversight of the Ministry's protective security practices in line with Protective Security Requirements (PSR).</p> <p>At the Ministry, the CSO is the DCE OAC.</p>
Chief Information Security Officer	<p>The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency. The CISO is responsible for cyber security requirements, and accountable for representing cyber security, leading a programme of cyber security continuous improvement, and managing a virtual team through a distributed security function.</p> <p>At the Ministry, the CISO is the General Manager (GM) Information. The GM Information is responsible for implementing and having assurance over this policy.</p>

Person/Party	Responsibility
Chief Privacy Officer	<p>The Chief Privacy Officer (CPO) sets the strategic direction for Privacy within their agency. The CPO is responsible for:</p> <ul style="list-style-type: none"> • Dealing with any complaints from the Ministry staff or clients about possible privacy breaches • Dealing with requests for access to personal information, or correction of personal information • Acts as the liaison for the Ministry with the Office of the Privacy Commissioner • Advising the Ministry on the potential privacy impacts of changes to the organisation's business practices • Overseeing the function governing what the Ministry can and cannot do with personal information. <p>At the Ministry, the CPO is the GM Information.</p>
Information, Security and Identity Group	<p>The Information, Security and Identity Group is responsible for:</p> <ul style="list-style-type: none"> • Supporting MSD's strategic future – providing thought leadership on information security, privacy and information management across, as well as influencing information maturity growth across MSD and all of government • Delivering assurance - providing support to MSD in meeting its compliance responsibilities through an assurance programme to manage defined information risks. • Providing expert advice - providing specialist skills to ensure business processes and systems design align to good practice, including responsible use and protection of information assets and comply with information legislation and related regulations. • Delivering a foundational capability - providing direction, guidance tools, training and support for information capability improvements.
Strategy & Insights	<p>The Strategy & Insights Group is responsible for:</p> <ul style="list-style-type: none"> • Maintaining enterprise data resources, such as an enterprise data catalogue, enterprise data model, and their implementation into MSD's data warehouse, ensuring we can understand and

Person/Party	Responsibility
	<p>access our authoritative data sets with confidence in their quality, timeliness, and consistency.</p> <ul style="list-style-type: none"> • Driving MSD's approach to data and analytic products which support decision making, and ensuring we are recognising the potential value of a given use of data in trading off against risk. • Setting requirements for new data collection and standards around that data's quality and structure in order to be useful for analytics. • Supporting the Ministry to use and manage Ministry data, analytics, and evidence • Client and Business Intelligence and data science • Research and Evaluation to analyse data and produce insights that inform decision-making and provide evidence on what interventions work for whom • Data Management and data reporting.
Improvement, Systems and Technology (IST)	<p>IST is responsible for enabling people and partners with improved services and effective technology so New Zealanders can easily access the support they need.</p> <p>IST, as system owners, are responsible for the overall operation of the system, including any outsourced services, telecommunications, and cloud. IST is part of the Transformation Group and are made up of service improvement and technology experts, including Technology Security and Identity</p>
Ethics Advisor	<p>The Ethics Advisor is responsible for:</p> <ul style="list-style-type: none"> • Formulating, reviewing, and disseminating ethics-related documents, and providing guidance related to all ethical issues, including those relating to information (code of conduct, conflicts of interest, outside activities, etc.) <p>At MSD, the Ethics Advisor is an independent ethics advisor commissioned by the GM Information.</p>

Definitions

Word/ phrase	Definition
Algorithm	Algorithms are sets of instructions that enable computers to solve problems or complete tasks. There are many different types of algorithms for different purposes and outcomes. Algorithms can be simple or complex. All forms of 'AI' are complex algorithms.
Archiving	The process of preserving information that needs to be held over the medium or long term with low frequency of access, so that it retains its integrity and remains available for use by MSD and others until it is able to be disposed.
Information	Recorded information (including both personal information and data) in any form created or received and maintained as evidence of Ministry business. It includes, but is not limited to, documents, email correspondence, datasets, audit logs, metadata (including reaction emoji 🐱), text messages, voice recording, social media, and web pages.
Information Asset	An Information Asset is an identifiable collection of information and data recognised as having value to the agency. Information assets have recognisable and manageable risk, content, and lifecycles. Assets are defined at the broadest level that permits effective governance, description, and comparability to other assets (including equivalent assets held by other agencies).
Information Lifecycle	The stages through which information passes, such as creation or collection, storage, access and sharing, use, maintenance and archiving, and disposal through destruction or transfer.
Information Governance	Enterprise Information Governance is a structured, consistent, and deliberate approach to managing, protecting, and using our information to support the Ministry's strategic objectives and fulfil mandated obligations. It unifies existing governance structures, clarifies decision-making processes, and identifies gaps across information-related capabilities. By embedding Te Ao Māori values and integrating the Information Accountability Framework and Information Policy Framework, it drives effective and accountable information management practices
Information Use	Information Use means everything that is done with information. This means not just active use, but also all parts of the information lifecycle (including collection and disposal). For the avoidance of doubt, information is being used when it is held in a database, even when that database is not actively being accessed.

Information Management	The process by which the Ministry ensures that information is managed across its lifecycle, such that it is accurate, relevant, and accessible; and that it is retained and disposed of appropriately in line with its value and its risk profile.
Information Security	Information Security relates to the protection of information regardless of its form (electronic or physical). The accepted definition of information security within government is: "measures relating to the confidentiality, availability and integrity of information".
Personal Information	Personal Information is defined under the Privacy Act 2020 as "Information about an identifiable individual...". It includes anything that relates to an identified person to be identified directly or indirectly, such as, but not limited to name, address, contact details, date of birth, signature, photographic image, Social Welfare Number, information about someone's health, sex life or orientation, their finances, religious, political or philosophical beliefs, race, biometric or genetic data.
Privacy	Privacy relates to the rights an individual has to control their personal information and how it's used. There is an obvious overlap between information security and privacy. This policy recognises the interdependence of one to the other.
Risk culture	The level of risk that an organisation is prepared to accept in pursuit of its objectives.

Information Group



**MINISTRY OF SOCIAL
DEVELOPMENT**

TE MANATŪ WHAKAHIATO ORA

Poutiaki

Poutiaki Model for Information Governance

Trust | Protect | Serve | Partner

The Ministry of Social Development

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Executive Summary

The Poutiaki model is a strategic approach that will help ensure MSD's Information Governance Framework (Tiaki) is inclusive of Māori values, needs, and expectations.

The operating model is designed to bridge mātauranga Māori or Māori knowledge systems and values with information governance, with a strong emphasis on shared commitment and mutual respect.

This proposal seeks endorsement of Poutiaki, the plan to engage, and the general direction. A draft risk management plan has also been provided for your consideration.

Background

Information governance is crucial for MSD due to the vast amount of sensitive information and data it collects, uses, and stores to provide taxpayer-funded income and other support to New Zealand citizens.

However, information governance also holds great significance for Māori people. Over the past decade, we have seen an emergence of literature on Māori data sovereignty and Māori data governance. Māori leaders like Kirikowhai Mikaere and Professor Tahu Kukutai have developed reports and approaches to Māori data sovereignty, cloud storage, and even data governance.

There are notable areas of tension between the systems operated by MSD and the aspirations and demands of Māori groups such as Te Kāhui Raraunga (Iwi Leaders Technical Advisory Group on Māori data) and Te Mana Raraunga (Māori Data Sovereignty Network). These tensions arise from differences in perspectives and values. For instance, Māori groups like Te Kāhui Raraunga and Te Mana Raraunga believe full and informed consent is required before an agency uses any data belonging to a Māori individual; they advocate for local data storage solutions and do not support data offshoring; they aim to have all Māori data transferred to their care and authority over time.

On the other hand, there are also areas of overlap and alignment between MSD and Māori groups. In these areas, it is essential to engage with Māori when designing solutions. Examples include the classification of data and the updating of guardrails and tools like the MSD Privacy, Human Rights and Ethics (PHRaE) framework.

While there is a clear distance between the parties on certain issues, there is also a notable closeness on other matters. To bridge these gaps and make progress, a 'platform' is needed where both parties can jointly identify and advance the areas of overlap. This is precisely what the Poutiaki model aims to provide. The Poutiaki model seeks to establish a collaborative partnership between MSD and Māori groups, with the goal of developing and implementing information governance solutions that are aligned with the values and aspirations of both parties. This model recognizes the importance of respecting Māori data sovereignty and ensuring that Māori have a meaningful say in how their data is collected, used, and stored. By working together through the Poutiaki model, MSD and Māori groups can incrementally overcome the challenges of information governance and create a more inclusive and equitable system that benefits all New Zealanders.

Poutiaki: The Objectives

The Poutiaki operating model is designed to:

- **Integrate:** Integrate Te Ao Māori principles into the Tiaki framework.
- **Engage:** Provide a structured platform for meaningful dialogue and collaboration between the Ministry and Māori stakeholders.
- **Progress:** Identify and collaboratively achieve common priorities in information governance.

Poutiaki: Operating Model

The Poutiaki operating model has three key features:

- **A Māori Technical Advisory Group on Information Governance (Te Ohu):** A group of five experts offering strategic and practical advice on integrating Te Ao Māori principles into the Tiaki framework.
- **Working Meetings to Identify Shared Priorities (Wānanga):** Quarterly meetings between the Ministry and Te Ohu to foster open dialogue, knowledge exchange, and the identification of shared priorities.
- **Progressing the Shared Priorities (Mahi Tahī):** Collaborative implementation of initiatives to address shared priorities, upholding Te Ao Māori principles, and improving information governance for all.

The operating model is strategic and practical. It provides a bridge between mātauranga Māori or knowledge systems and values with information governance. It enables a collaborative process of shared prioritization. It also provides a way to progress the shared priorities, with an emphasis on shared commitment, and mutual respect.

Poutiaki: The Criticality of Te Ohu

The external and independent Māori technical advisory is critical. A draft Terms of Reference is attached in Appendix 1 of this paper. In summary, Te Ohu is a platform for ensuring MSD's information governance work is inclusive of the Māori perspective. Te Ohu will be instrumental in ensuring the information governance framework is culturally responsive and meets key needs of Māori communities. Te Ohu will also likely play a key role in building Māori capability and capacity within the Ministry through knowledge sharing.

The proposed objectives of Te Ohu are:

- Integrate Te Ao Māori principles into the Tiaki framework.
- Provide advice on MSD and Māori priorities and relevant issues, to identify shared priorities.
- Support MSD in advancing shared priorities.

The proposed skillsets of Te Ohu members are:

- Technical expertise in information and data governance, or management.
- Knowledge of Te Reo and Tikanga Māori.
- Experience in working well with others.

MSD will ensure Te Ohu membership reflects the diversity of the Māori population across various dimensions such as age, gender, rural/city, iwi/hapu, business and community. We expect Te Ohu will meet four to five times a year. Members will be paid according to the Cabinet

Fees Framework. We will cover necessary travel costs. We may also ask individuals to assist us on specific projects (paid separately). MSD will provide administrative support for Te Ohu.¹

Being clear on what Te Ohu is and is not

To be clear, Te Ohu is not and cannot be a substitute for the voices and views of Iwi as Treaty partners. Nor is Te Ohu intended as a substitute for the MSD Māori Reference Group. The Treaty relationship is complex, and Te Ohu will exist alongside all other Iwi and Māori relationships that MSD has. Moreover, Iwi and Māori will continue to share their views and opinions with MSD as Treaty rights holders.

Te Ohu is a specific Māori technical advisory group for this area of work. They will help us both understand, and advance Māori needs and expectations in the information governance domain. They may also raise areas of concern where our opinion may differ. As the Treaty relationship requires, we will listen, respond as appropriate, but most of all work hard to maintain a respectful and honourable relationship.

Huihui: The Engagement Plan

We have developed a high-level engagement plan. This aim is to leverage MSD's existing relationships and networks within Māori communities. Targeted outreach to specific Māori organizations will ensure the model is informed by diverse perspectives and needs. Formal hui (face-to-face meetings) will offer structured discussions, while informal "1000 cups of tea" conversations will foster trust and understanding on a personal level.

We are very fortunate at MSD to have strong relationships and networks with Māori because of the work we do. We have already started planning with Māori, Communities and Partnerships (MCP) to identify Iwi, partners, providers, and communities who we might engage with. These discussions are ongoing.

Our primary plan is to leverage off MCP networks to hold three hui (face-to-face meetings) on the Poutiaki model. We would aim to have between five and 15 key Māori leaders at each wānanga.

Separate but related, we plan to utilise the community approach of "1000 cups of tea". These are less structured but deeper conversations with up to 30 key Māori informants. These will include conversations with Iwi and Māori from across NZ who we have relationships with or interact with as a partner or provider of services.

¹ Please note that this is a proposal only at this stage, and upon receiving feedback from Tai Nuku, we intend to seek advice from relevant parts of the MSD business to ensure that this Group is set up in a way that complies with all relevant MSD policies and protocols.

Huihui: High Level Engagement Plan

Timeframe	Action
July 2024	Collaborate with MCP to identify Iwi, partners, providers, and communities for engagement. Engage with relevant areas of MSD to set up Te Ohu in accordance with all appropriate policies and protocols.
Aug-Oct 2024	Hold three hui (face to face meetings) on the Poutiaki model, with venue, kai, and facilitation provided by MSD. Feedback and themes will be shared with participants post each of the sessions. Conduct informal engagements with up to 30 key Māori informants, sharing feedback and themes with participants.
Oct-Nov 2024	Synthesise feedback gathered during the engagement process.

Partnership and Engagement Risks

A risk management plan has been developed to identify and mitigate potential risks associated with the implementation of the strategic partnership between MSD and Māori stakeholders. The plan outlines potential risks, including insufficient engagement with Māori stakeholders, misalignment of priorities between MSD and Māori, and limited capacity within MSD to implement shared priorities.

Risk Identification	Mitigation
Insufficient engagement with Māori stakeholders This risk arises from the need to ensure that Māori stakeholders are actively engaged and have a meaningful say in the development and implementation of the partnership. Insufficient engagement could lead to a lack of buy-in from Māori stakeholders, which could undermine the effectiveness of the partnership.	Robust engagement plan with alternative approaches for feedback Huihui plan includes different channels through which Māori will be engaged. The plan includes face-to-face meetings, hui, workshops, and online engagement.
Misalignment of priorities between MSD and Māori This risk arises from the potential for different interpretations of the partnership's goals and objectives. Misaligned priorities could lead to conflict and disagreement between MSD and Māori stakeholders, which could hinder the partnership's progress.	Ongoing communication and collaboration with Te Ohu This strategy involves establishing and maintaining ongoing communication and collaboration with Te Ohu. Te Ohu will play a key role in ensuring Māori voices are heard.
Limited capacity or capability within MSD to implement shared priorities. This risk arises from the need to ensure that MSD has the necessary capacity and capability to implement the shared priorities of the	Strategic selection of opportunities Consideration will be made in the mahi tahi phase of need to be smart when selecting priorities to focus on, where the quick wins can be made, as well as where

partnership. Limited capacity could delay or derail the implementation of the partnership, which could have a negative impact on its outcomes.	the priority is important but will take longer. Critical to this is the partnership between Te Ohu and MSD and being clear, upfront but also supporting the shared priorities and committing to progressing these.
--	--

Budget

We have identified likely costs to cover Te Ohu member fees, travel reimbursements, and Huihui engagement. Following engagement with relevant areas of MSD's business, these costs will be confirmed in the next phase of work.

Next Steps

By November 2024, a refined Poutiaki model will be finalized, incorporating feedback from stakeholders. It will be shared with the Māori Reference Group (MRG), Tai Nuku, and participants. Following necessary approvals, the model is anticipated to be fully operational by February 2025.

Consultation

The MCP team has been involved, and their feedback incorporated in the development of this proposal. Their involvement is ongoing.

Tiaki – Our Enterprise Information Governance Framework

Tiaki: The Four Pou Model of Enterprise Information Governance



Framework Core Areas and Elements

Framework Core Areas organise the various elements of governance into overarching capabilities. Each core area has multiple elements, with each element having a people, process and technology lens.

Core Areas

Elements

Obligations & Drivers

WHAT WE MUST DO

The various influences that mandate how we create, manage and dispose of information. This includes legislation, organisational strategies and purpose.

Legislation and Regulation

AOG Directives

Emerging Risks

Organisational Strategy

Emerging Environmental Factors

Principles

Foundations

OUR VALUES & TIAKI

The essential underpinning ways of respecting people and their information. This includes, application of Māori values and ethics as well as good information management practices.

Te Ao Māori

Privacy

Te Tiriti o Waitangi

Metadata

Ethics and Human Rights

Data Quality

Security

Leadership & Governance

HOW WE ADD VALUE & LEADERSHIP

Where the foundation for effective information governance is established through defining information, governance roles, responsibilities, accountabilities, and decision-making processes.

Governing Bodies

Decision Making Rights

Information Stewardship

Information Strategies

Roles, Responsibilities and Accountabilities

Operating Model

Guide, Design, Assure

GOVERNANCE SERVICES & ENABLEMENT

Focus Areas to ensure information governance is delegated and assured on behalf of leadership, guardrails and assurance processes. This includes standards and policies as well as ongoing assurance processes.

Guide

Policies

Processes

Training

Standards

Patterns

Awareness

Guides

Advice

Change Management

Design

Information Strategies

Enterprise Capabilities

Information Lifecycle

Design and Modelling

Information Use

Enabling Services

Assure

Compliance

Feedback

Risk Management

KPIs

Controls

OKRs

Monitor

Ministry-Wide Risks

Draft Terms of Reference – Te Ohu

1. Introduction

Te Ohu, the Independent Māori Technical Advisory Group on Information Governance, is being established by the Ministry of Social Development (MSD) to ensure the Tiaki Information Governance Framework is inclusive of Māori needs and expectations.

The mandate of Te Ohu is to collaborate with MSD to ensure the integration of Te Ao Māori perspectives into the Tiaki framework.

2. Purpose

Te Ohu's primary purpose is to work alongside MSD to identify and advance shared work priorities that embed Te Ao Māori perspectives and values within the Tiaki framework.

3. Objectives

Te Ohu aims to:

- Ensure the Tiaki framework authentically reflects Te Ao Māori perspectives and values.
- Integrate Te Ao Māori principles into all levels of information governance and stewardship within the Tiaki framework.
- Collaborate with the MSD to identify shared work priorities.
- Progress these priorities effectively and promptly.

4. Operating Principles

The members of Te Ohu and members of MSD commit to the following principles:

- **Rangatiratanga** – The MSD respects that Te Ohu members are independent, not MSD staff, and are descendants of those who signed the original Te Tiriti o Waitangi. MSD honours and acknowledges the members of Te Ohu and their role.
- **Kawanatanga** – Te Ohu members respect that MSD staff represent the Crown signatories of Te Tiriti o Waitangi. Te Ohu members honour and acknowledge the role of MSD staff.
- **Manaakitanga** – Te Ohu and MSD staff agree that mutual respect between partners is essential for finding and advancing shared priorities.
- **Mahi Tahi** – Te Ohu and MSD staff will use their best endeavours to collaborate and be constructive in identifying and progressing shared information governance priorities, while also acknowledging it is acceptable to disagree and have differences of opinion.

5. Composition and Membership

5.1 Composition

Te Ohu members shall:

- Be affiliated with an Iwi or Hapū.
- Have experience in information data governance and/or management.
- Possess expertise in Māori information data governance and/or management.
- Be knowledgeable in tikanga and te reo Māori.

5.2 Membership Appointment

Appointments will be made by the General Manager Information and the General Manager Māori, Partnerships and Programmes, based on expertise, experience, and commitment to Te Ao Māori principles.

5.3 Term of Membership

Members will serve a 12-month term, with the possibility of reappointment.

6. Roles and Responsibilities

6.1 Chairperson

The Chairperson will:

- Facilitate and lead Group meetings (or Wānanga).
- Ensure decisions are made through a consensus-driven approach.

6.2 Group Members

Te Ohu members will:

- Participate actively in meetings or wānanga.
- Contribute their expertise and insights.
- Engage with their communities to bring their perspectives to Te Ohu.

7. Meetings or Wānanga

7.1 Frequency

Te Ohu will convene five meetings or wānanga and meet as necessary to fulfil its objectives.

7.2 Quorum

A quorum will require at least three members, including the Chairperson.

7.3 Decision-Making

Decisions will be made by consensus or, if that is not possible, by a majority vote. Te Ohu maintains the right to share independent views with MSD, even if they diverge from the Ministry's stance.

8. Reporting and Accountability

The Chairperson will meet with the General Manager Information and General Manager Māori, Partnerships and Programmes biannually to discuss updates and strategic advice.

9. Confidentiality and Conflict of Interest

9.1 Confidentiality

Members must keep sensitive discussions within Te Ohu confidential.

9.2 Conflict of Interest

Members must declare any conflicts of interest and may be required to step back from related discussions or decisions.

10. Amendments

The Terms of Reference can be amended with the agreement of the General Manager Information.

11. Adoption and Effective Date

These Terms of Reference are effective from [dd/mm/yyyy] and will continue until amended or replaced.



Te Haoroa Data Governance

May 2024

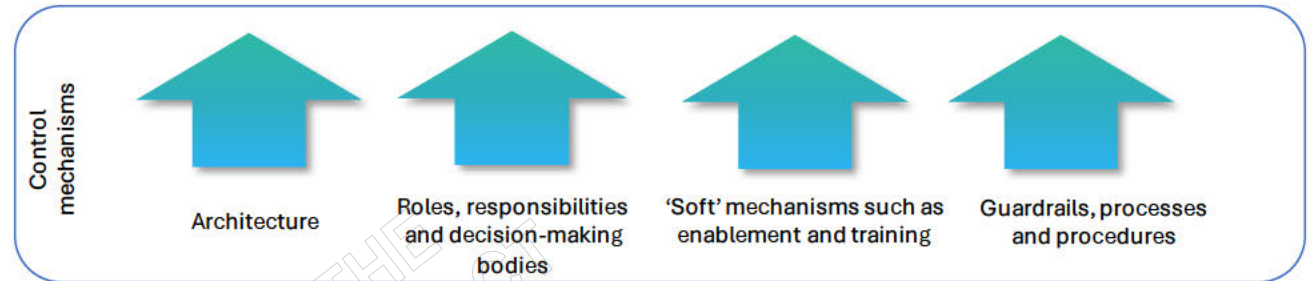
RELEASED UNDER THE
OFFICIAL INFORMATION ACT



What is data governance?

In its simplest terms, data governance refers to the mechanisms stakeholders use to exercise control over data through its lifecycle.

How do we govern data in Te Haoroa?



Why govern data?

- Improved data quality
- Increased trust in data
- Improved data literacy
- Improved trust in decisions
- Enhanced decision-making
- Regulatory compliance
- Increased operational efficiency
- Better risk management
- Improved data security

What are the benefits of well governed data?

Metadata management (a collection of policies, procedures and systems used to administer the data that describes other data) is part of data governance. Metadata gives data a context. When data has a context, **users have a better understanding** of what data exists, where it comes from, when it is used, how it is used. This helps them **work faster and more effectively**.

Metadata management **improves data quality** by identifying and resolving data issues, duplicates or gaps and by providing clear and accurate information about data elements.

Defining and assigning data roles and responsibilities is part of data governance. When a specific role is given specific data responsibilities, they take ownership for the quality performance of that responsibility. This accountability ensures that **data decisions are made faster and more effectively**. Assigning accountability to data also **improves data quality** by assigning roles to create and maintain metadata.

Accountability across roles sets a starting point for **building data literacy** – the ability to read, write and communicate about data in the MSD context.

Enablement and training activities educate people on their roles and responsibilities and on how to fulfil them. Training and enablement resources demonstrate how tasks should be performed, communicate criteria and develop shared understanding. These are a starting point for building **data literacy** and a **positive data culture**.

Compartmentalised architecture **improves data security** by allowing user access to be controlled and restricted to certain defined areas.

Defining, documenting and communicating consistent and uniform data policies and processes is part of data governance. When data providers, managers, analysts and consumers can all see where they fit into a process and that the process is transparent and consistent, it **increases their trust in the data outputs**.

Through data governance, different areas of the business resolve data definition disputes and achieve alignment when conceptualising what data means and how to use it, **improving trust in data, and enhancing decision-making**.

Te Haoroa data governance

Data governance

In its simplest terms, data governance refers to the mechanisms stakeholders use to exercise control over data. The scope of data governance in this context is Te Haoroa ; a data and analytics platform that exists within MSD's broader data and information ecosystem. There are broadly four types of mechanisms available for exercising control over data within Te Haoroa platform. These are:

Architecture

Te Haoroa's compartmentalised technical architecture enables Te Haoroa Security Model, Role Based Access Model and Information Product assurance levels. Code is managed using Azure Dev Ops and Data is catalogued using Informatica EDC, which holds contextual information about the data in Te Haoroa system, enabling users to understand its technical and business context and its quality and conduct metadata management. Te Haoroa's data architecture uses a domain-driven design method to describe the system.

Roles, responsibilities and decision-making bodies

The division of authority and responsibilities between the platform owner and other parties. These are detailed in the following documents:

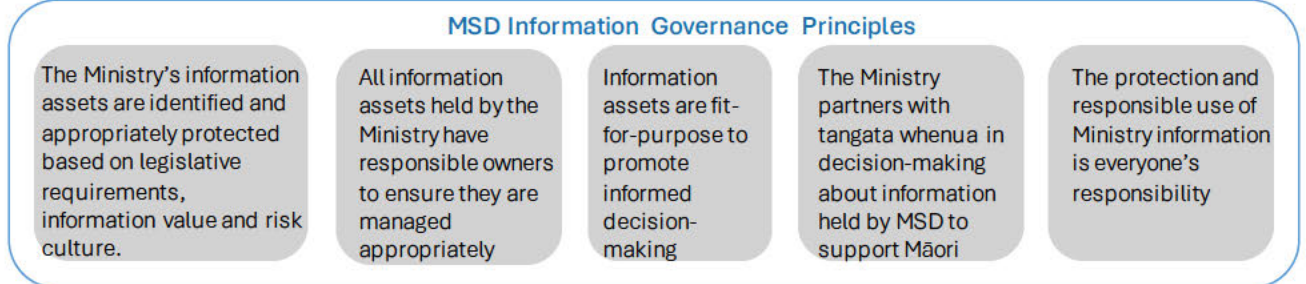
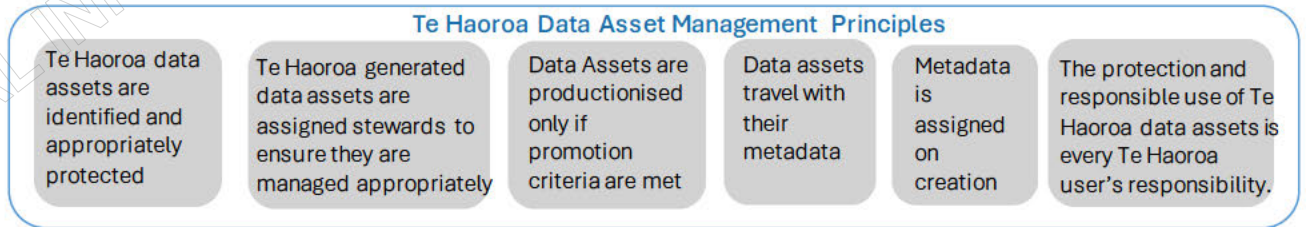
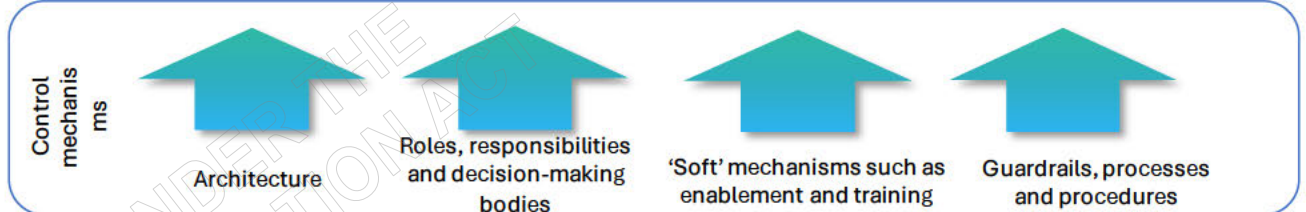
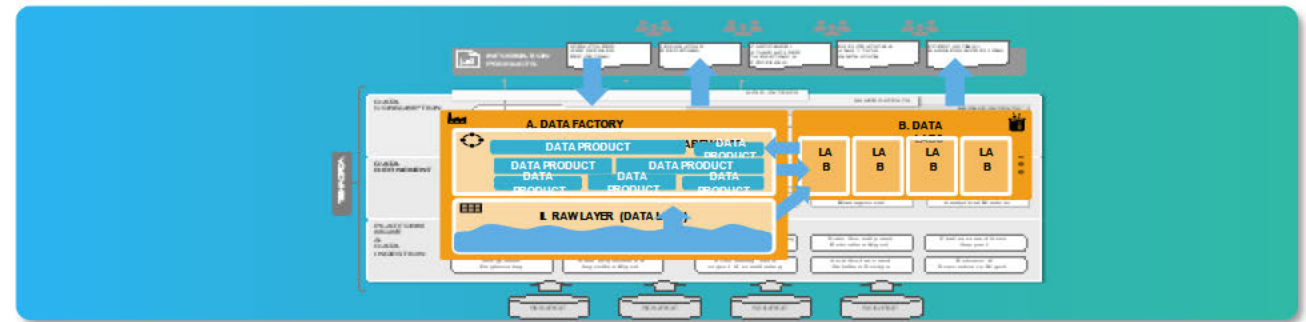
- Te Haoroa governance overview
- [Te Haoroa decision matrix](#)
- [Te Haoroa roles and responsibilities](#)

Guardrails, processes and procedures

Processes are an important supporting element for the data governance framework. The right processes encourage desirable behaviour in all the participating groups to mitigate business risks. The Information Product Development Process and supporting sub-processes are summarised in the following document: [Te Haoroa The Information Product Build Process v2.1.pptx](#)

Enablement, training and culture

The community-based nature of a platform ecosystem like Te Haoroa heightens the importance of 'soft' control mechanisms such as influence and culture change-based approaches. Key documents can be found in Te Haoroa Training Hub.



Architectural

Architectural choices made in the construction of a platform are important to enable data governance. Te Haoroa's compartmentalised technical architecture (separate controlled environments) means data can be managed in a controlled manner. Architectural mechanisms that influence/enable data governance within the platform include:

Assurance levels

The compartmentalised architecture allows assurance levels to be enforced. Assurance levels are labels that are put on Information Products to indicate the quality of the data used to build them. If the data came from the lab, it is BRONZE. If the data came mostly from the Data Factory, it is Silver. If the data came only from the Data Factory, it is GOLD.

Te Haoroa Security Model

The compartmentalised architecture enables Te Haoroa Security Model,

Access Model

The compartmentalised architecture enables the application of role-based access controls.

Code Management

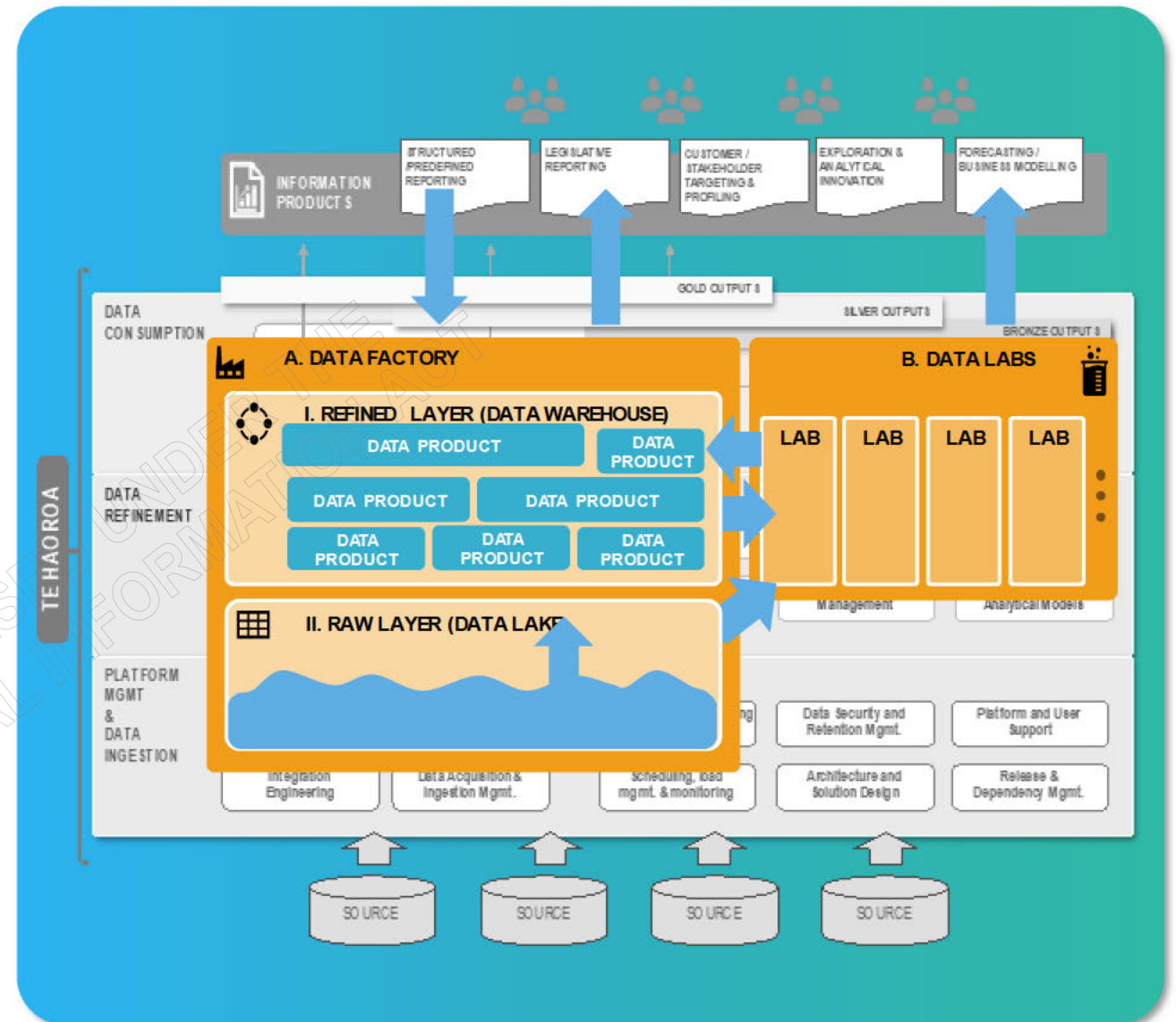
Code is managed using Azure Dev Ops

Data Catalogue

Data is catalogued using Informatica EDC, which holds contextual information about the data in Te Haoroa system, enabling users to understand its technical and business context and its quality.

Data Architecture

Te Haoroa's data architecture uses a domain-driven design method to describe the system. This architecture is implemented within the data factory – the compartmentalised architecture and Role Based Access Model keeps the data factory locked down and protected from unauthorised changes.



Governance and management structures

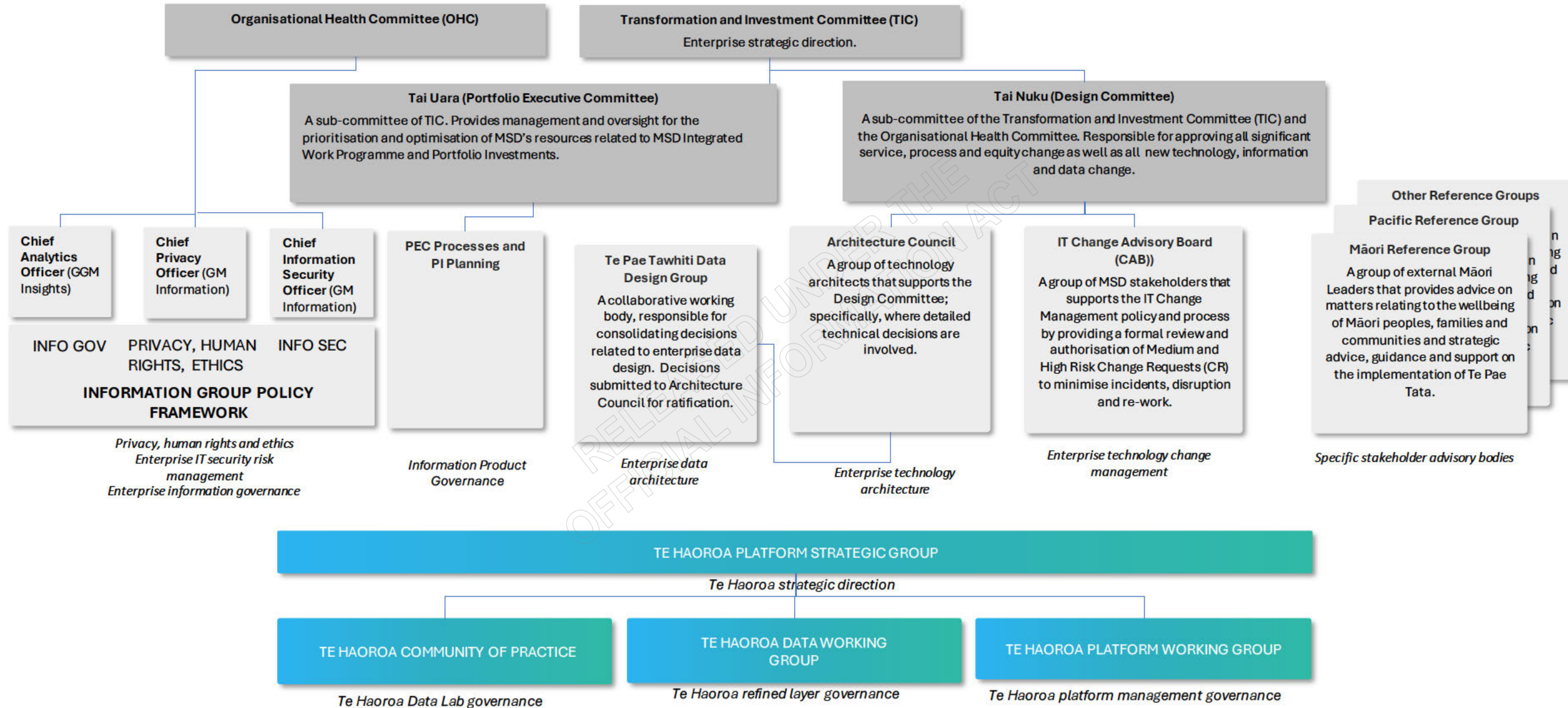
Te Haoroa governance system consists of a strategic group that sets the direction and guardrails for platform technology and data, two working groups and a proposed Community of Practice. At a high level, Te Haoroa Data Working Group supports the development of the Refined Layer, Te Haoroa Platform Working Group ensures effective platform management and the proposed analyst-led Community of Practice to maintain a collaborative learning and sharing culture within Te Haoroa.



The data governance and management structures within Te Haoroa ecosystem:

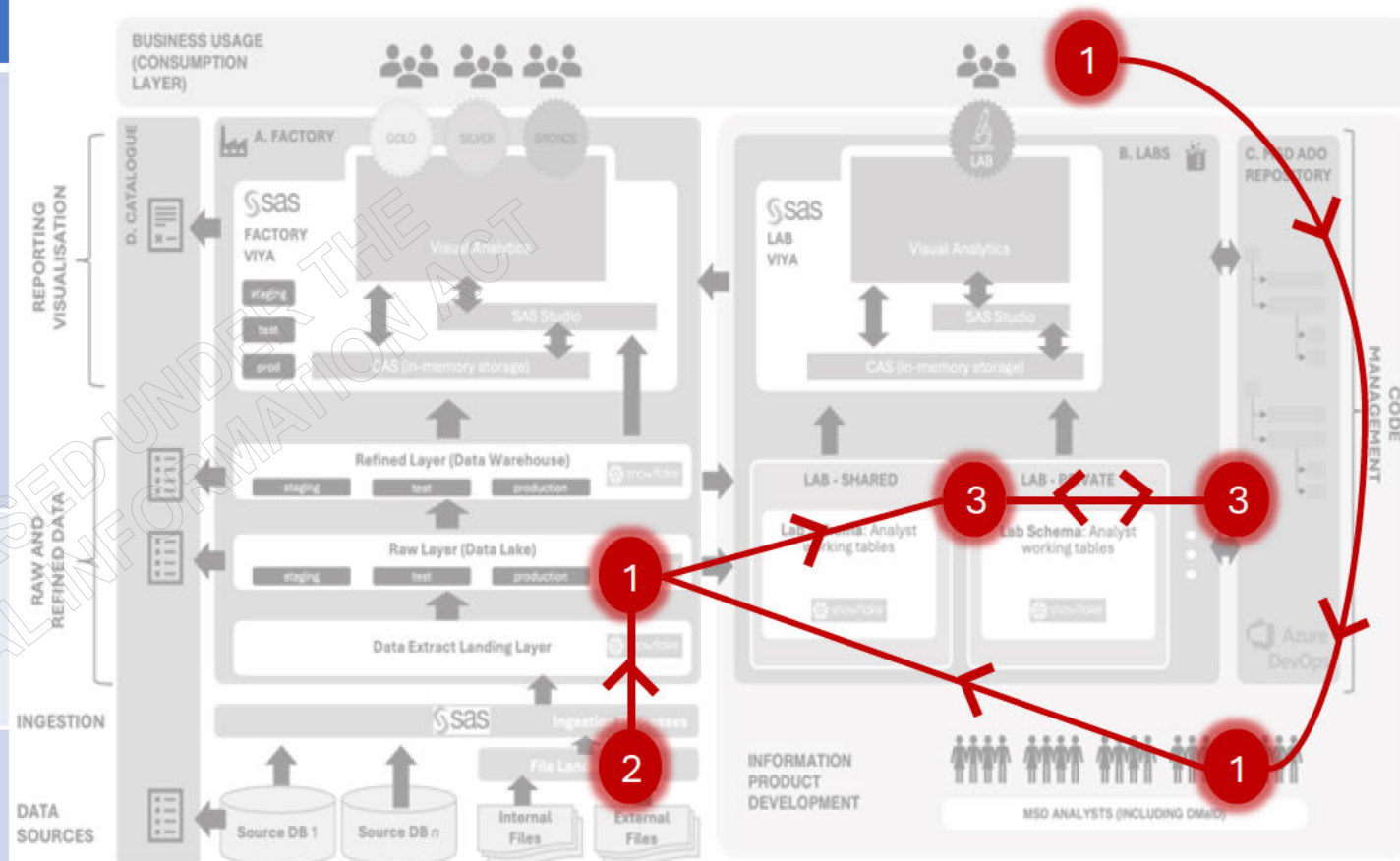
- A** **Te Haoroa Strategic Platform Group**
To set strategic direction and guardrails for technology and data for Te Haoroa.
- B** **Te Haoroa Data Working Group**
To support the design and development of the Te Haoroa data warehouse with MSD subject matter expertise.
- C** **Te Haoroa Platform Working Group**
To oversee the effectiveness of processes and information security controls, adjusting as necessary.
- D** **Te Haoroa Community of Practice (proposed)**
To set guidelines for Te Haoroa Community in the Lab environment and monitor the health of the data labs.

Te Haoroa governance context



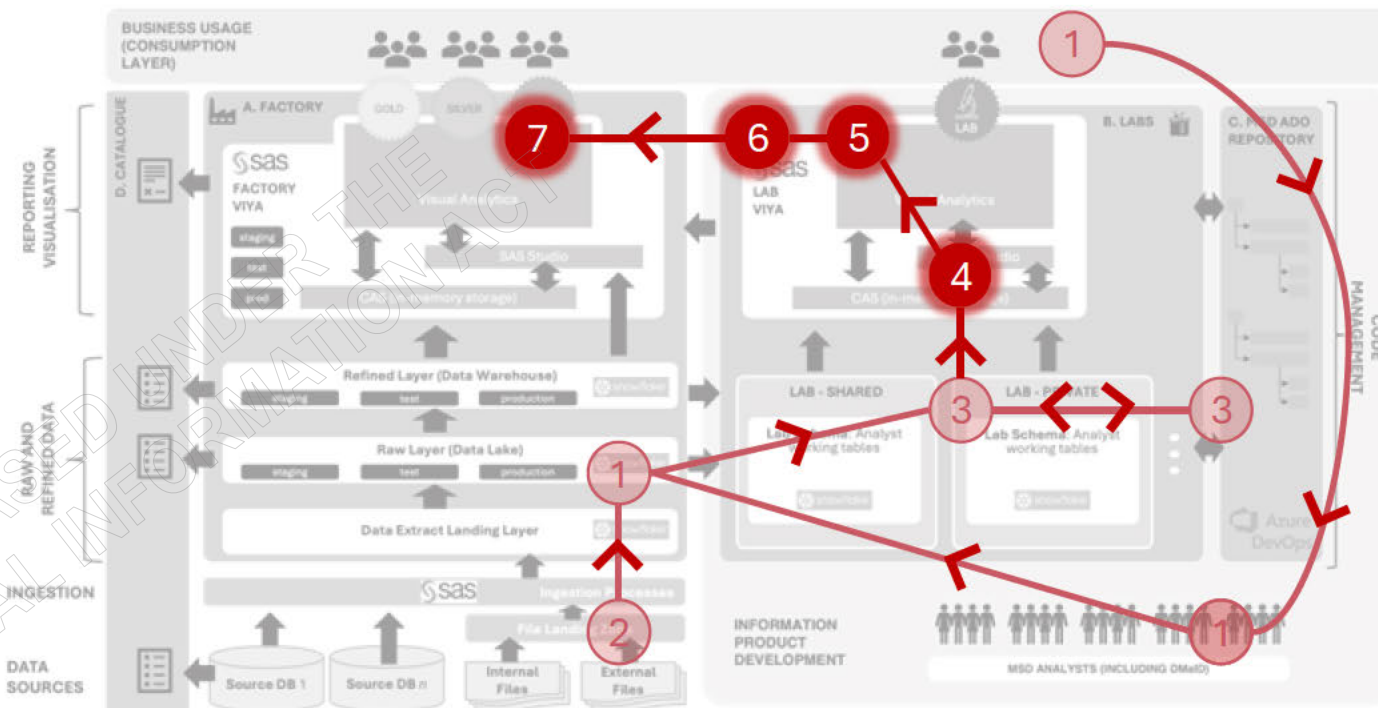
Guardrails, processes and procedures (1 of 2)

	What is undertaken?	Data Governance elements
1	<p>Upon understanding what the information product request requires the data analyst will scope out the work into Proof of Concept and Pilot phases. At this stage, the development team will review the data available at the Refined and Raw layer, including the Analysis and Design resources.</p> <ul style="list-style-type: none"> Once developed, the development team will be able to use the Data Catalogue to review what data sits at the Raw and Refined layer. Until then, the data analyst can query the Raw and Refined layers to assess what data exists. The development team may engage with DMaID to assist with understanding what data exists at the Refined layer, and what is scheduled to be added to the Refined layer. 	<ul style="list-style-type: none"> Information Product metadata recorded in central location, enabling search Data asset metadata recorded in central location, enabling search Community of Practice raises awareness among analyst community about new Information Products
2	<p>The development team may require data that does not sit yet within the raw or refined layer (for example, an external dataset, or a dataset not yet ingested from an MSD Source System). They can request this data be ingested using the "External Data Request" [see: PRJ-Te-Haoroa -> General -> Raw Ingestion -> External Data Request_Process]. If this data has or may contain sensitive data or PII data an approval process is required.</p>	<ul style="list-style-type: none"> Defined external data request process including sensitive/PII data process
3	<p>1. Upon deciding what type of lab is required (shared vs. private), the development team will:</p> <ol style="list-style-type: none"> Create new feature branch within MSD's Azure DevOps for code management Go through an initial model design and table build process by developing a SAS Studio programme or writing Snowflake SQL(in Snowsight) to pull data into the Lab schema. They check this code into ADO as they go. 	<ul style="list-style-type: none"> Decision point – sensitive projects go into a secure lab. Code is managed as an asset via ADO. Data is managed as an asset via raw/refined/lab environments and TEST DEV PROD environments.



Guardrails, processes and procedures (2 of 2)

	What is undertaken?	Data Governance elements
4	The development team uploads the data from the lab schema into CAS so they can use Visual Analytics to develop an output. At this stage the development team may have already developed some wireframes to define the scope and look & feel of the output. Any changes to the underlying code should be developed in either SAS Studio or Snowpark in the lab schema, not CAS (as CAS is in-memory, and refreshed frequently).	
5	The development team develop the required visual output (e.g. Dashboard) in Visual Analytics. It is important that MSD's visualisation standards are adhered to, ensuring a similar look and feel, particularly for 'gold' products. Anything developed here should be pushed into the ADO branch.	<ul style="list-style-type: none"> MSD visualization and information design standards
6	The development team will check the information product for technical issues (e.g. the script runs without errors, the pipeline works, it is generally error free). Once the development team are satisfied, they will ask for feedback from the Information Product (Business) Owner. There could be several iterations of validation, refinement and redeployment as the product is tested by the business owner, and refined across the Proof of Concept and Pilot phases of development.	<ul style="list-style-type: none"> Technical QA Validation from Business Users
7	Depending on the type of product developed it is likely it will go through a deployment process. This is explained more fully in the 'Information Product Development process'. This involves DMaID pulling the code from ADO into a Factory test environment, deploying the information product into Factory test for validation, and once validated, deploying the information product into Factory Prod for wider access.	<ul style="list-style-type: none"> Defined assurance levels and staged development process



Enablement, training and culture

Key Changes and New Ways of Working

Nainpreet Dhillon
Change Lead

Introduction

To support the Data lab key changes please read the below key changes and new ways of working.

Find out more how working in Te Haoroa is different

Key Changes

Key Changes:

Te Haoroa aims to modernise MSD's data analytics capability, by investing in our capabilities and ensuring that our data related products are engineered for reuse and scalability. Also, that there are sound data governance, standards, and processes.

Key Changes on a Page

Learn more →

Find out more about Modular Coding

Modular coding

Find out more about commissioning

Commissioning

Find out more about end-to-end visualisation

Building end-to-end visuals

Find out more about the capability uplift

Capability Uplift

Find out more about needing to collaborate

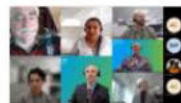
Collaboration

Find out more about data governance

Data Governance



Workshop recordings



Te Haoroa Workshop 3



Te Haoroa workshop 2



Te Haoroa workshop 1

Start learning



Find learning opportunities in the digital training library.

Get started

Popular portals

Te Haoroa

Te Haoroa Training Hub
Welcome! We are so happy you are here. Consider this your home base to find the support and resources you need to be successful working on the Te Haoroa platform.

Te Haoroa
The extendable net

Ka pu te ruha,
ka hua te rangatahi
As the old net withers,
the new net goes fishing

2/23

News & announcements



Training Hub Updates
Ka Ora team, first and foremost...
Nainpreet Dhillon 19 April



Access to Training Hub Notification
Ka Ora Kaitiaki, Firstly, thank you...
Nainpreet Dhillon 14 March

Upcoming events

4 - Add event

See all

Te Haoroa digital training library

We want to make sure you have the resources you need to be successful in your new role. Training resources have been specifically curated to help new team members learn more about Te Haoroa.

Te Haoroa

Learn more about Te Haoroa platform and its various areas.



Te Haoroa Platform



Key changes and new ways of working



Data Lab

Technology

Learn more about the tools and technology that you will be using when working on Te Haoroa.



SAS and Snowflake - How they work together



SAS Visual Analytics



Snowflake



Microsoft Azure



Informatica Data Catalogue

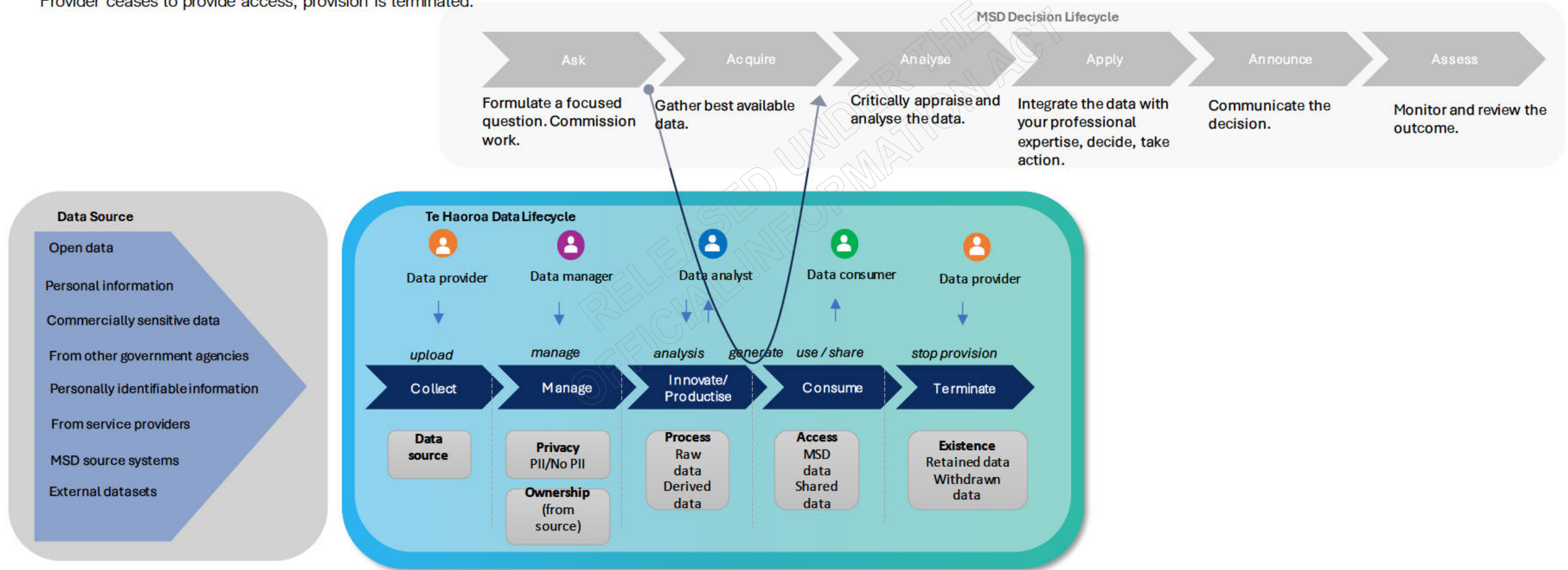


**MINISTRY OF SOCIAL
DEVELOPMENT**
TE MANATU WHAKAHIAATO ORA

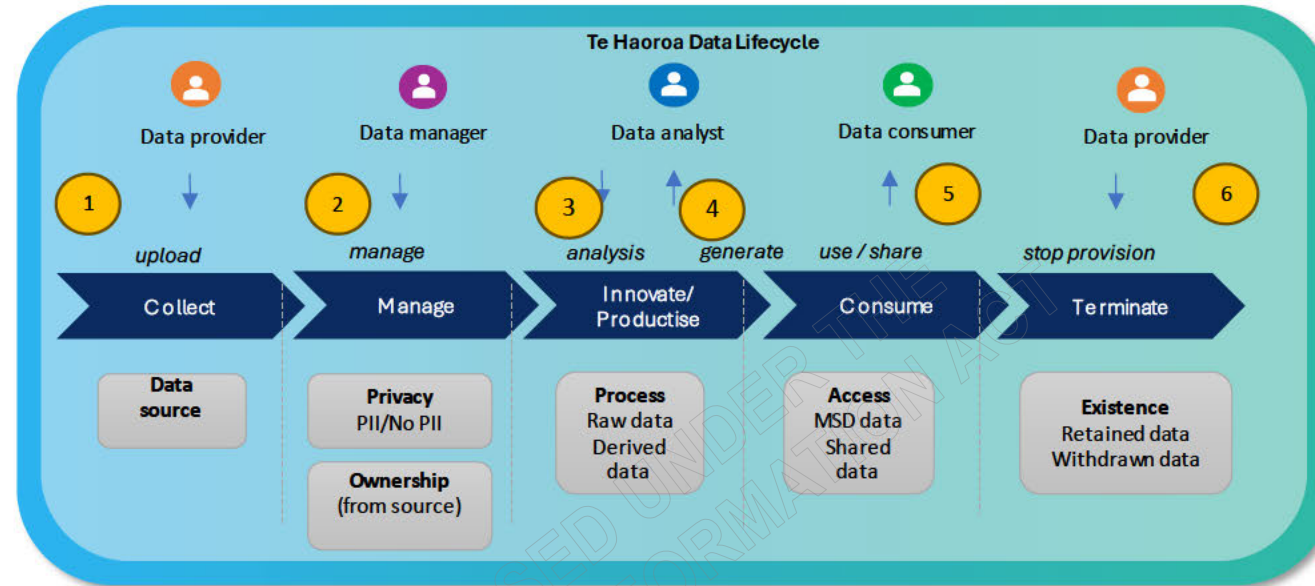
Te Haoroa data lifecycle

Te Haoroa is a data and analytics system, with data flowing through it in a specific data lifecycle. Te Haoroa data lifecycle interacts with other MSD information and decisionmaking support lifecycles. The diagram below illustrates the relationship between Te Haoroa data and broader MSD decision support mechanisms.

Te Haoroa data lifecycle begins when data is uploaded from a source. Data is then cleansed and organised. Data analysts work with the data to address focused business questions, generating Information Products and other decision support outputs. Data Consumers use outputs from Te Haoroa to contribute to their decision making. When a data source ceases production, or a Data Provider ceases to provide access, provision is terminated.



Data governance elements in Te Haoroa data lifecycle



Data governance touchpoints

- 1 Data sources are ingested if they meet clear ingestion criteria. Source metadata is maintained. Technical metadata is added automatically. Business metadata is added manually. R&D Schedule can be included in business metadata.
- 2 Data is managed by a small set of individuals holding specific RBAC roles. Data is cleansed and documented. Rules [Te Haoroa domain model] are applied. Data domain SMEs are documented here: [Copy of Induction \(2023.11.22\) Refined Layer Work - incl Lab roles.xlsx](#)
- 3 Data is used to generate Information Products. Technical metadata added automatically. Business metadata added manually. Information Products travel with their metadata.
- 4 Information Product commissioning process identifies clear data use purpose, Information Product Owner. Info Products involving sensitive/private data are built in a secure lab.
- 5 RBAC model applies appropriate role-based access to data (masking/aggregation where required). Information Products have owners (the business representative who commissioned it) and stewards (while in labs or Bronze, the steward is the data analyst who developed the Info Product. Once in Gold, stewardship is transferred to DMAID).
- 6 Data provider may stop provision. If R&D schedule has been included in business metadata, R&D schedule can be applied.

- Ability to manage and audit network access
- Allows an organisation to maintain privacy and security by limiting unnecessary access to sensitive information based on each user's established role within the organisation.
- reduces the need for paperwork and password changes when an employee is hired or changes their role because you can use RBAC to add and switch roles quickly and implement them globally across operating systems, platforms and applications.
- reduces the potential for error when assigning user permissions.
- helps to more easily integrate third-party users into the network by giving them pre-defined roles.
- Aligns roles with organisational structure of the business to make operations more efficient. Removes the need to ask for permissions individually for each tool.
- Makes it easier to meet statutory and regulatory requirements for privacy and confidentiality by giving the ability to manage how data is being accessed and used.

Within Te Haoroa, system datasets are tagged as either 'PII' (contains personally identifiable data) or "NON-PII" (does not contain personally identifiable data). This allows access to PII data to be restricted to only those who need to see it. (Need to see is identified up front in Ideation and Prioritisation Stage. If a need to work with PII is identified, a secure lab is set up).

Example:

[illegible]

Privacy controls (inside Te Haoroa and beyond)

Sensitive and private data identification

Te Haoroa uses ingestion criteria to manage identification and tagging of sensitive and private data. Before data is ingested into Te Haoroa, it goes through an ingestion process where PI data is identified. If PI data is present, the ingestion request is escalated to the Information Group.

Data security measures

Because only appropriately tagged data is ingested, private or sensitive data is consistently identified and secured in a Secure Lab - an environment where a specific team has their own separate and isolated area to create data structures for the purpose of individual analysis and modeling. In a Secure Data Lab, the team have exclusive access to their own data and analysts who do not have clearance for this data have no access. Access is managed via access controls. Security is monitored and enforced by Te Haoroa Platform Working Group. Changes are managed via MSD IT change governance processes.

Access controls

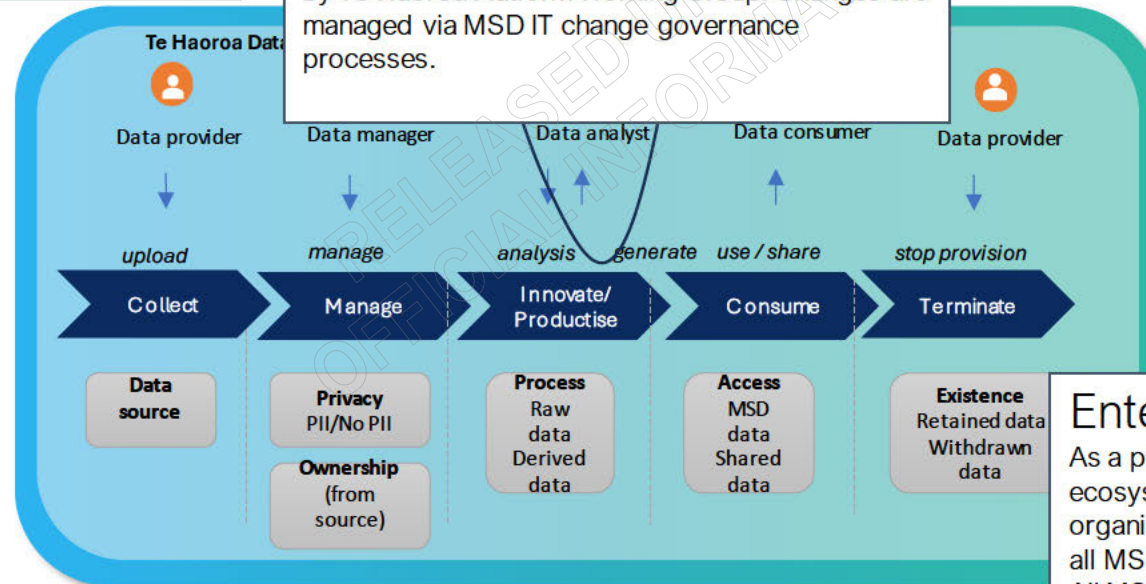
Because only appropriately tagged data is ingested, access can be securely managed via Role Based Access Controls. Access controls are monitored and enforced by Te Haoroa Platform Working Group. Changes to RBAC model are approved by Strategic Platform Group.

Role Based Access Control mechanisms allow controlled application of appropriate data protection techniques such as masking, aggregation and anonymisation as required.

Consent management

Consent occurs on collection. Te Haoroa uses ingestion criteria to manage consent risk..

From other government agencies
Personally identifiable information
From service providers
MSD source systems
External datasets



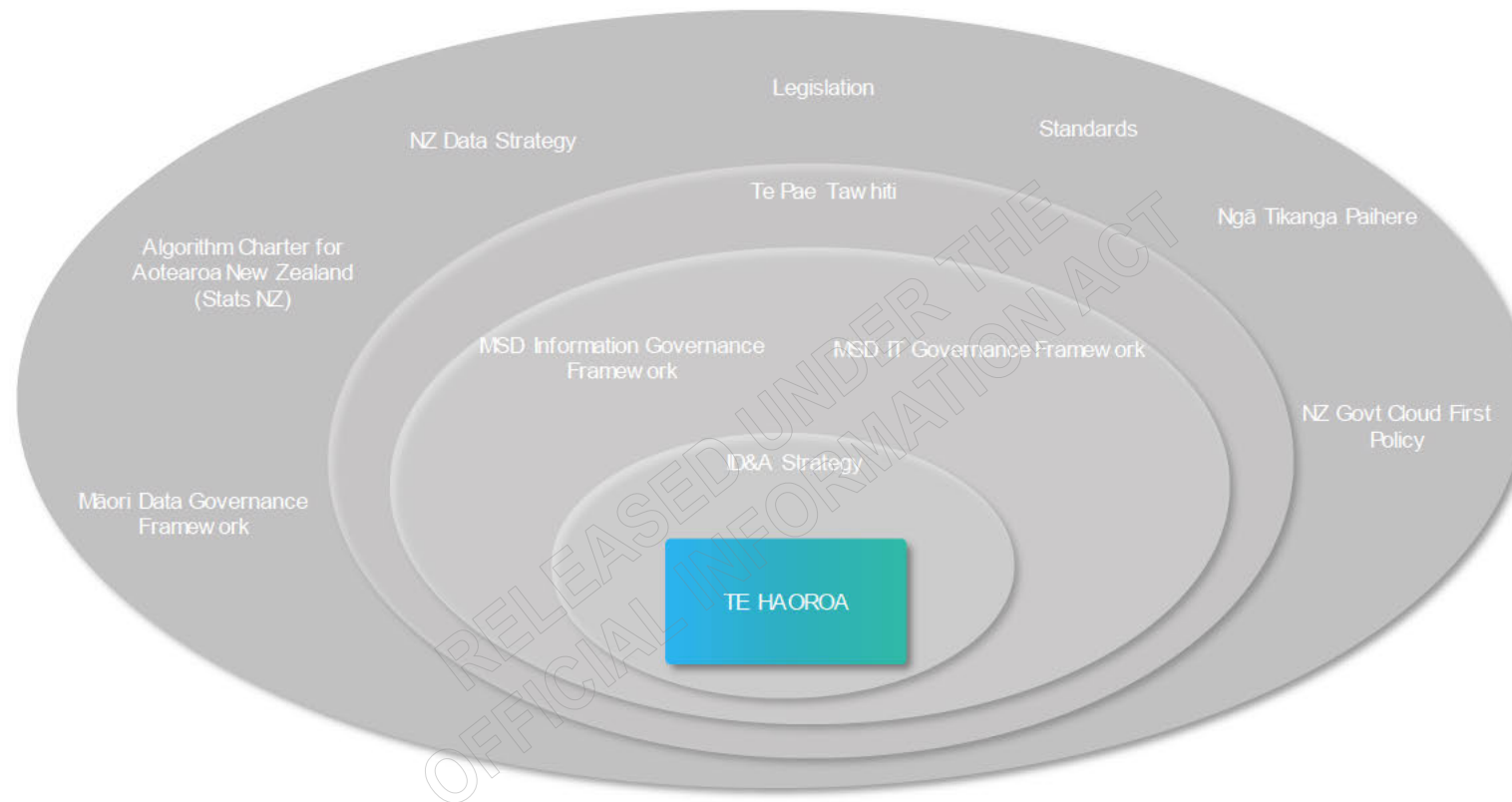
Regular Monitoring

Use of modern architectures such as snowflake allows logging, monitoring and automated alerting if unexpected behaviours occur or rules are breached so appropriate action can be taken. Logs are monitored by Platform Working Group and issues escalated to Strategic Platform Group as appropriate.

Enterprise Privacy Framework

As a platform within MSD's broader information ecosystem, Te Haoroa exists within MSD's organisational privacy framework and complies with all MSD enterprise level privacy policies. All MSD staff are subject to MSD's Code of Conduct and complete mandatory information privacy and ethics training as provided by MSD's Information Group.

Te Haoroa data governance context



Te Haoroa is a data and analytics platform that exists within MSD's broader data and information ecosystem.



Information Group



**MINISTRY OF SOCIAL
DEVELOPMENT**
TE MANATŪ WHAKAHIATO ORA

Tiaki

Enterprise Information Governance Framework

Trust | Protect | Serve | Partner

The Ministry of Social Development

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Document Purpose

The purpose of this document is to describe the Ministry of Social Development's Enterprise Information Governance framework purpose and scope.

This document will be used to gain approval of the concepts underpinning the framework, the language used to describe it and the diagrams used to help articulate the core concepts and how the framework will be used.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Overview

The Ministry of Social Development's (the Ministry) Enterprise Information Governance (EIG) framework, Tiaki, has been developed to give effect to the principles of the Information Governance policy, which set the governing direction and intent for how information should be governed, and the Information Data & Analytics (ID&A) Strategy which sets how to lift the maturity of our information and analytics practices to support the delivery of Te Pae Tawhiti - our Future strategic direction.

Functional ownership of the Tiaki Framework sits with the General Manager Information (CISO, CPO), and its implementation is the responsibility of the Information Group (specifically in terms of maintaining it, championing the Ministry's implementation and adoption of it, and providing the necessary services to support decision-makers to interact with it). Noting that other enabling functions, such as Improvement, Systems and Technology (IST) and Strategy and Insights, will support aspects of the implementation as they relate to their respective functions.

Scope¹

This Framework applies to all Ministry staff including contractors that, by agreement, have responsibility for any aspects of the Ministry's information collection, maintenance, protection, or disposal and all information². Information in this context means recorded information (including data) in any form created or received and maintained as evidence of Ministry business. It includes, but is not limited to, documents, email, the Ministry Information Governance Policy correspondence, datasets, audit logs, text messages, voice recording, social media, and web pages.

Information Governance Principles³

The Information Governance policy defines the following principles that guide all staff in managing the Ministry's information assets:

- the Ministry's information assets are identified and appropriately protected based on legislative requirements, information value and risk culture.
- all information assets held by the Ministry have responsible owners to ensure they are managed appropriately.
- information assets are fit-for-purpose to promote informed decision-making.
- the Ministry partners with tangata whenua in decision-making about information held by the Ministry to support Māori.
- the protection and responsible use of Ministry information is everyone's responsibility.

¹ Ministry of Social Development - Information Governance Policy 2022

² Information means: "Recorded information (including data) in any form created or received and maintained as evidence of Ministry business. It includes, but is not limited to, documents, email the Ministry Information Governance Policy correspondence, datasets, audit logs, text messages, voice recording, social media, and web pages".

³ Ministry of Social Development - Information Governance Policy 2022

Introduction

Establishing an EIG Framework stems from The Information Governance policy, which defines the guiding principles and directives for information management within the Ministry. The policy requires the Ministry to understand the information it holds and how it is used, allocate responsibility for its stewardship, and ensure it is protected and managed appropriately.

Furthermore, the importance of governing our information-related activities and obligations is underscored in the objectives outlined in Te Pae Tawhiti – Our Future⁴, which sets our strategic direction and the three strategic shifts essential for achieving our desired outcomes.

The Te Pae Tawhiti programme aims to deliver a new insights-driven service model tailored to our client's needs, whānau, and communities. This requires a transformation of our systems, processes and information. Quality, accessible, reliable and effectively used and protected information is a fundamental enabler for achieving our outcomes.

The Information Data & Analytics (ID&A) Strategy outlines some of the current gaps in our information maturity, for example, there are gaps in the Ministry's understanding and governance of its information assets, it lacks a clear stance on Māori data governance and adequate high-quality, timely insights to support the goals of Te Pae Tawhiti. Furthermore, it highlights that our privacy and security practices need improvement to ensure compliance with legislative requirements, and we are moving to a proactive and risk/value approach.

Introducing a comprehensive Enterprise Information Governance (EIG) framework that embeds Te Ao Māori values will serve to provide a structured, consistent, and deliberate way of managing, protecting, and using our information to support the delivery of Te Pae Tawhiti and to meet our mandated obligations. The framework aims to unify existing governance structures, identify gaps across all information-related capabilities, clarify decision-making processes, and drive effective information management practices.

Embedding a Te Ao Māori Perspective

Information governance is ultimately about the stewardship of people's information. Te Ao Māori provides a valuable way of conceptualising data, and people's relationships that we have adopted in our approach, including:

- **Kaitiakitanga:** Stewardship of resources, symbolising responsible information guardianship.
- **Taonga:** Information is a treasured asset, demanding careful protection.
- **Rangatiratanga:** Respecting the interests of those whose data we are utilising and being open to working with them on key matters.

Māori values like **manaakitanga** (care and respect), and **whanaungatanga** (relationships) can be further utilised to give life to this approach.

Te Ao Māori is inherently people-centred and collaborative. To truly embed these perspectives in the implementation of the framework, we need an approach where we are actively listening, learning, informing, sharing, and co-creating an inclusive and ethical system. This requires

⁴ Underpinned by the Te Pae Tata and Pacific Prosperity Strategies

identifying opportunities for collaboration with communities, joint decision-making, and greater community control over information usage.

Implementing the core elements of the Framework will allow us to give effect to our intentions, laid out in the Information Governance policy and ID&A strategy, to partner with Māori to ultimately ensure the framework is fully fit for purpose.

Tiaki: The Four Pou Model of Enterprise Information Governance

Te Pae Tawhiti will drive the Ministry to become an increasingly information-driven organisation, especially considering the aspirations of the future services model. Our EIG framework is called Tiaki and must allow us to leverage greater value from our information, while equally prioritising the protection of our clients' privacy, human and ethical rights.

"Tiaki" is a powerful Māori verb meaning "to look after, care for, and steward." This resonates deeply with the core values of good governance and the very purpose of this work - being responsible stewards of the information and data entrusted to us by the public.

"Tiaki" is not merely a label; it embodies the aspirations of this framework - to nurture trust, foster collaboration, and ensure that data serves the collective well-being of all New Zealanders.

The four Pou are the guide posts that can help us achieve the above while still reflecting the core of our information governance principles.

- **Trust:** Building trust through managing our information responsibly, securely, and in compliance with regulations and tikanga, thus demonstrating transparency, integrity, and accountability to our clients, their whānau and communities.
- **Protect:** Ensure information is treated like taonga by implementing policies, procedures, and controls to protect it from unauthorised access, loss, or misuse while also ensuring its accuracy, reliability, and confidentiality throughout its lifecycle.
- **Serve:** We serve by ensuring that information delivers the right value to our clients, their whānau, communities, key stakeholders, and the Ministry. This involves making information accessible and usable for better decision-making, better service design, strategic planning, and operational efficiency. It includes supporting and sharing information with community partners like Iwi and other providers to assist them in understanding their clients and communities to enable better outcomes.
- **Partner:** We collaborate with stakeholders, including employees, clients, partners (such as our Iwi Treaty Accord partners), and the broader community to understand their views and needs (including information needs) and build trust and support in how we deliver services.

Tiaki has been organised into seven core areas, each with its own overarching functions, distinct in purpose and role but collectively supporting each other to act as the governance framework.

- **Obligations & Drivers:** This area captures the legislative and regulatory frameworks within which our information operates, expectations from an All-of-government perspective, and the strategic drivers for change.
- **Foundations:** This area captures the lenses through which we must view all information management activities to achieve our Trust, Serve and Protect outcomes.
- **Governance & Leadership:** This area establishes the foundation for effective information governance by clearly defining the information governance roles, responsibilities, accountabilities, and decision-making processes.

- **Guide, Design & Assure:** These three areas collectively offer the necessary direction, resources, and confidence in our information use, management and protection practices.

Each core area consists of multiple elements that, when established and matured, will contribute to the successful governance of the Ministry's information.

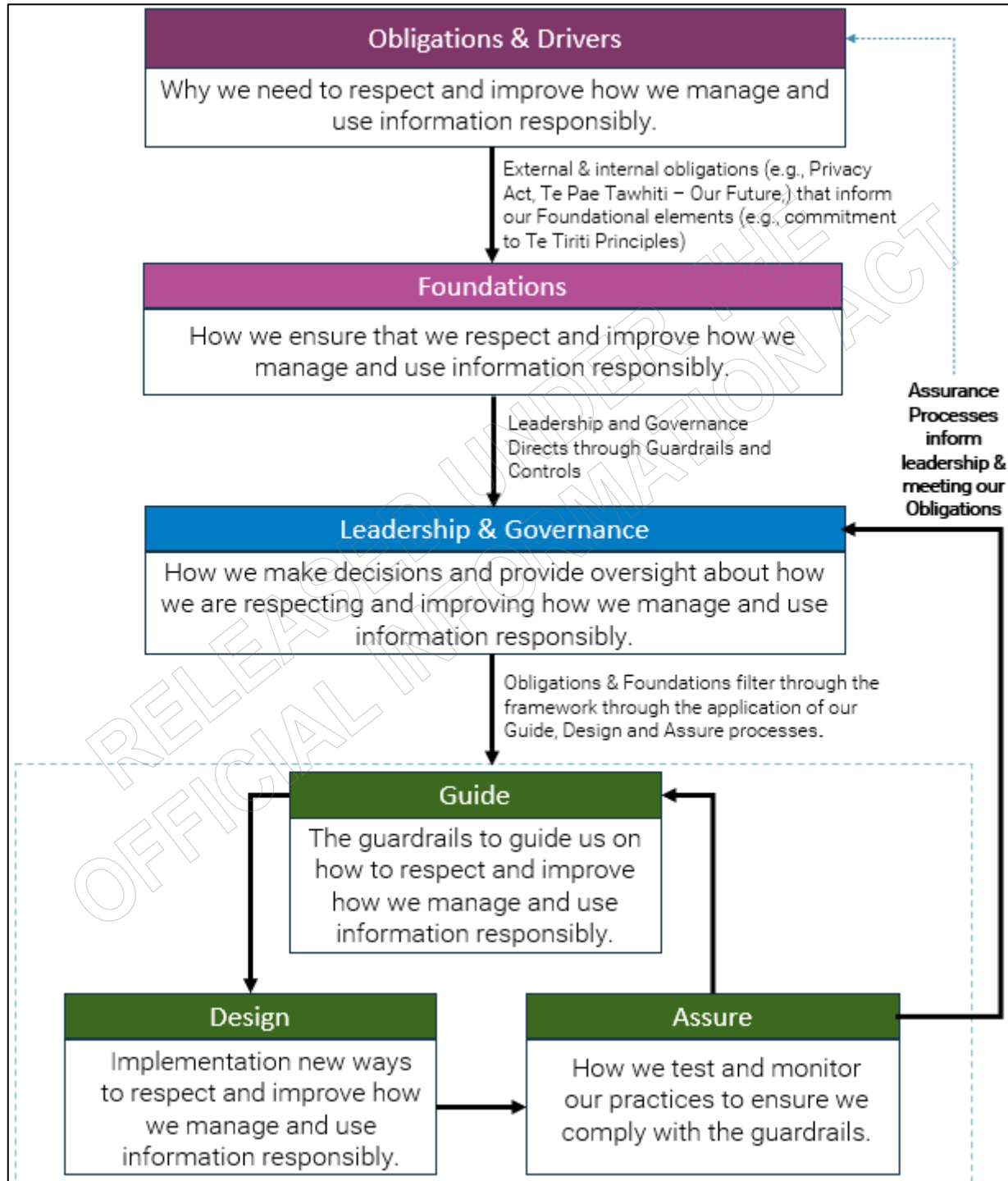


Figure 1 Core Areas of the Tiaki Framework

The **Obligations & Drivers** and **Foundations** elements allow our **Leadership & Governance** elements to set the expectations and direction for our information assets. These are then applied through the **Guide, Design** and **Assure** areas to empower our people to protect, manage, and use our information consistently and in a way that manages risk, while leveraging the full extent of opportunity from our information. This will in turn help the Ministry achieve the strategic shift as set out in the ID&A Strategy and contribute to organisational transformation.

Currently, the Ministry has some of all seven core areas, but maturing them is essential to supporting organisational transformation.

However, even today, by connecting all seven core areas, we can support leaders in making better and more informed decisions about the information we hold and use today and as we transition towards our target state.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Tiaki – Our Enterprise Information Governance Framework

Tiaki: The Four Pou Model of Enterprise Information Governance



Framework Core Areas and Elements

Framework Core Areas organise the various elements of governance into overarching capabilities. Each core area has multiple elements, with each element having a people, process and technology lens.

Core Areas

Elements

Obligations & Drivers

WHAT WE MUST DO

The various influences that mandate how we create, manage and dispose of information. This includes legislation, organisational strategies and purpose.

Legislation and Regulation

AOG Directives

Emerging Risks

Organisational Strategy

Emerging Environmental Factors

Principles

Foundations

OUR VALUES & TIAKI

The essential underpinning ways of respecting people and their information. This includes, application of Māori values and ethics as well as good information management practices.

Te Ao Māori

Privacy

Te Tiriti o Waitangi

Metadata

Ethics and Human Rights

Data Quality

Security

Leadership & Governance

HOW WE ADD VALUE & LEADERSHIP

Where the foundation for effective information governance is established through defining information, governance roles, responsibilities, accountabilities, and decision-making processes.

Governing Bodies

Decision Making Rights

Information Stewardship

Information Strategies

Roles, Responsibilities and Accountabilities

Operating Model

Guide, Design, Assure

GOVERNANCE SERVICES & ENABLEMENT

Focus Areas to ensure information governance is delegated and assured on behalf of leadership, guardrails and assurance processes. This includes standards and policies as well as ongoing assurance processes.

Guide

Policies

Processes

Training

Standards

Patterns

Awareness

Guides

Advice

Change Management

Design

Information Strategies

Enterprise Capabilities

Information Lifecycle

Design and Modelling

Information Use

Enabling Services

Assure

Compliance

Feedback

Risk Management

KPIs

Controls

OKRs

Monitor

Ministry-Wide Risks

Framework Development - Following Best Practice

The Framework has been developed based on national and international best practice models (refer to [Bibliography](#)). A review of multiple frameworks showed alignment across them, with the same components consistently being listed:

- Goals and Objectives, aligned with business outcomes
- Governance Structure
- Policies and Standards
- Information ownership and stewardship
- Data lifecycle and management
- Training and communication
- Monitoring and measuring.

Our Framework accounts for all these components within our seven core areas, however we also drew inspiration from the DAMA (Data Management Association) Data Management Framework Evolved as defined in the second edition of the DAMA Guide to the Data Management Body of Knowledge ([DAMA-DMBOK2], Earley S. Henderson D. & Data Management Association, 2017, p.41).

In addition to the traditional data governance components listed above, it includes information handling ethics as a foundational component and it also recognises other foundational activities such as Metadata, Data Quality, and Data Protection upon which all other functions are dependent; implementation of foundational activities should be considered at all stages of the lifecycle, including the planning phase.

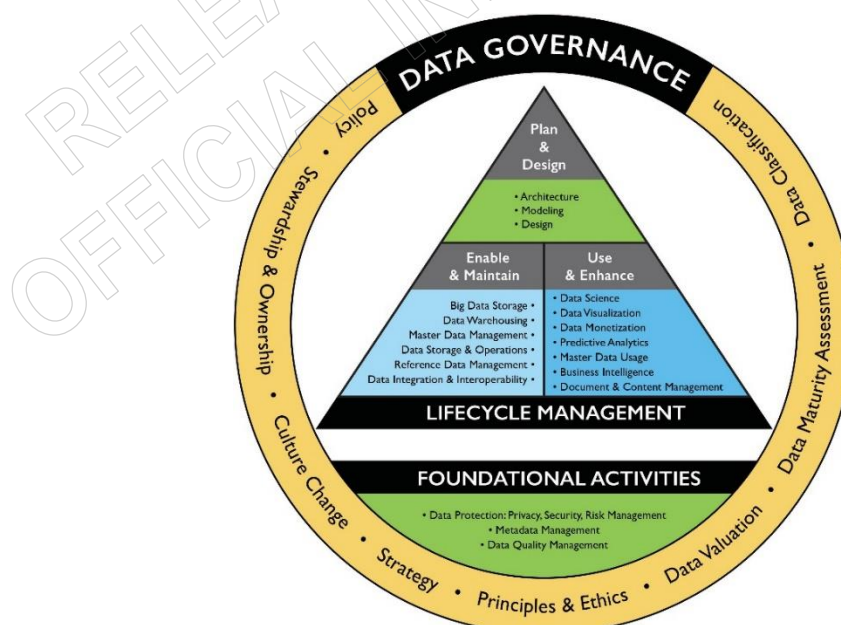


Figure 2 Figure 2 DAMA Wheel Evolved

Definitions

Information	Recorded information (including data) in any form created or received and maintained as evidence of Ministry business. It includes, but is not limited to, documents, email, the Ministry Information Governance Policy correspondence, datasets, audit logs, text messages, voice recording, social media, and web pages.
Information Lifecycle	The stages through which information passes, typically characterised as creation or collection, processing, dissemination, use, storage, and disposition, including destruction and deletion.
Information Governance	The capabilities, processes, controls, oversight, and assurance relating to information security, privacy, sharing and management. Information governance requires the specification of decision rights and an accountability framework to ensure appropriate behaviour across the information lifecycle. It includes the processes, roles, policies, standards, and metrics that ensure the effective and efficient use of information to enable an organisation to achieve its goals.
Information Use	Means everything that is done with information. This means active use and all parts of the information lifecycle (including collection and disposal). To avoid doubt, information is used when it is held in a database, even when that database is not actively being accessed.
Information Management	The process by which the Ministry ensures that information is managed across its lifecycle, such that it is accurate, relevant, and accessible; and that it is retained and disposed of appropriately in line with its value and its risk profile.
Information Asset Owners	<p>All information assets owners are responsible for ensuring the risks to, and the opportunities for their corresponding information assets are managed and monitored. The information asset owner must be someone who understands the value of the asset to the organisation and any legal or regulatory requirements applicable to the collection, use or storage of the information.</p> <p>At the Ministry, Information Asset Owners will typically be DCE, Regional Commissioners or Group General Managers.</p>
Information Stewards	<p>Information Stewards are responsible for the quality, integrity, and responsible use of information assets, enabling the organisation to gain maximum value from the information. They are also responsible for supporting information asset owners to make informed decisions about the management and use of their assets for the duration of their lifecycle.</p> <p>The Information Steward must keep the Information Asset Owner informed and made aware of any risks or concerns surrounding the integrity or safety of information.</p> <p>At the Ministry, Information Stewards will typically be General Managers, Regional Directors, and Directors.</p>
Information governance committees	Information governance committees are responsible for overseeing and tracking the achievement of the Ministry's strategic objectives relating to information governance.
Enterprise Capabilities	<p>Defines the Ministry's capacity and ability to 'do something' and are conceptual, repeatable patterns defining what needs to be delivered and why it needs to be delivered, making up the core functions of the Ministry.</p> <p>It is an organised collection of specific controls that together function to support the Ministry in delivering its strategy and achieving its outcomes securely and efficiently.</p>

Appendix One - The Framework Expanded

Obligations & Drivers								
Legislation & Regulation		Emerging Environmental Factors / Risks		AOG Directives	Organisational Strategy		Principles: Responsible Data Use	
<ul style="list-style-type: none">Privacy Act 2020Public Records Act 2005Official Information Act 1982		<ul style="list-style-type: none">Exceptional information sharing with other agencies, e.g., in a state of emergency or Health emergencies, such as COVID etc.Artificial IntelligenceBiometrics		<ul style="list-style-type: none">NZ Algorithm Charter 2020Protective Security RequirementsDeclaration on Open and Transparent Government	<ul style="list-style-type: none">Te Pae Tawhiti - Our FutureTe Pae Tata - Māori Strategy and Action PlanTe Pae Tata, Pacific ProsperityInformation, Data & Analytics StrategyTechnology Strategy		<ul style="list-style-type: none">NZ Data and Information Management Principles 2016NZ Privacy, Human Rights and Ethics FrameworkCARE principles for indigenous data governance.Māori Data Sovereignty PrinciplesData Protection and Use Policy (DPUP)NIST Cybersecurity Framework	
Foundations								
Te Ao Māori		Privacy, Ethics and Human Rights		Information Security	Data Quality		Metadata	
<ul style="list-style-type: none">Embedding a Māori world view into this work that will honour our commitment as a Te Tiriti o Waitangi partner and prioritise the needs of whānau.		<ul style="list-style-type: none">Ensuring that the Ministry protects and values people’s privacy, recognise human rights and treats people fairly and takes an ethical approach in everything we do with personal informationEnsuring Tikanga, kawa (protocols), and mātauranga (knowledge) underpin the collection, protection, access, and use of information.		<ul style="list-style-type: none">Information security protects sensitive information from unauthorised access, use, change, or loss. It contributes to compliance with legal and regulatory requirements and supports trust.	<ul style="list-style-type: none">Data Quality forms the foundation upon which reliable and effective data management practices are built. Ensuring that data is accurate, consistent, and relevant is essential for making informed business decisions, complying with our legislative and social obligations, and building trust that we use information responsibly to create better insights, better decisions, and better lives.		<ul style="list-style-type: none">Metadata serves as a foundational element that underpins effective data discoverability, management, governance, and use	
Leadership / Governance								
Governing Bodies		Information Stewardship	Roles & Responsibilities, & Accountabilities	Decision Rights	Information Strategies		Operating Model	
<ul style="list-style-type: none">Responsible for overseeing and tracking the achievement of the Ministry’s strategic objectives relating to information held and used as part of our functions.Approve Guardrails to meet protective security, privacy, and information management requirements.Oversees organisational risk and that it is managed in line with all relevant legislative and regulatory frameworks across all areas of the organisation.Ultimate decision-makers for information related initiatives.		<ul style="list-style-type: none">Information asset owners and stewards to ensure accountability, clarity, and effectiveness in managing information to leverage value from information whilst ensuring it is protected.	<ul style="list-style-type: none">Clearly defines who is accountable for the risk management of the information assets they steward.	<ul style="list-style-type: none">Defining who makes decisions about information and under what circumstances.	<ul style="list-style-type: none">Set expectations for information or data specific strategies required, e.g., data quality strategy		<ul style="list-style-type: none">Represents how the framework will be operationalised to support our outcomesFunctions that facilitate and support Information Governance within the organisation	
Guide								
<ul style="list-style-type: none">Policies	<ul style="list-style-type: none">Standards	<ul style="list-style-type: none">Guides	<ul style="list-style-type: none">Processes	<ul style="list-style-type: none">Patterns	<ul style="list-style-type: none">Advice	<ul style="list-style-type: none">Training	<ul style="list-style-type: none">Awaren	<ul style="list-style-type: none">Change Management
Design								
<ul style="list-style-type: none">Strategies		<ul style="list-style-type: none">Information Lifecycle		<ul style="list-style-type: none">Information Use	<ul style="list-style-type: none">Enterprise Capabilities	<ul style="list-style-type: none">Modelling and Design		<ul style="list-style-type: none">Enabling Services
Assure								
<ul style="list-style-type: none">Compliance	<ul style="list-style-type: none">Risk Management	<ul style="list-style-type: none">Controls	<ul style="list-style-type: none">Monitor	<ul style="list-style-type: none">Feedback	<ul style="list-style-type: none">KPIs	<ul style="list-style-type: none">OKRs	<ul style="list-style-type: none">Ministry Wide Risks	

Bibliography

- DAMA International. (2017). DAMA-DMBOK: Data Management Body of Knowledge (2nd Edition). Denville, NJ, USA: Technics Publications, LLC.
- Data Governance Institute. (n.d.). The DGI Data Governance Framework. Retrieved from The DGI Data Governance Framework: <https://datagovernance.com/>
- Oracle. (2011, May). Retrieved from An Oracle white Paper Architecture: Enterprise Information Management: Best Practices in Data Governance: <https://www.oracle.com/assets/oea-best-practices-data-gov-1357848.pdf>
- Petzold, B., Roggendorf, M., Rowshankish, K., & Sporleder, C. (n.d.). Designing data governance that delivers value. Retrieved from McKinsey Digital: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/designing-data-governance-that-delivers-value>
- PWC. (n.d.). Global and industry frameworks for data governance. Retrieved from PWC: <https://www.pwc.in/consulting/technology/data-and-analytics/govern-your-data/insights/global-and-industry-frameworks-for-data-governance.html>
- SAS. (n.d.). <https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/sas-whitepapers/en/sas-data-governance-framework-107325.pdf>. Retrieved from The SAS®Data Governance Framework: A Blueprint for Success: <https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/sas-whitepapers/en/sas-data-governance-framework-107325.pdf>
- Stats NZ Tataurangi Aotearoa. (n.d.). Co-designing Māori data governance. Retrieved from data.govt.nz: <https://www.data.govt.nz/toolkit/data-governance/maori/>
- Stats NZ Tataurangi Aotearoa. (n.d.). Holistic data governance. Retrieved from data.govt.nz: <https://www.data.govt.nz/toolkit/data-governance/holistic/>
- Stats NZ Tataurangi Aotearoa. (n.d.). Operational data governance. Retrieved from Data.govt.nz: <https://www.data.govt.nz/toolkit/data-governance/odgf/#:~:text=Operational%20data%20governance%20is%20designed,steady%20state%20data%20flow%20mapping>
- Te Kāhui Raraunga. (n.d.). Iwi Data Needs. Retrieved from Te Kāhui Raraunga: <https://www.kahuiraraunga.io/iwidataneeds>
- Wells, D. (2019, August 14). The Path to Modern Data Governance. Retrieved from Eckerson Group: <https://www.eckerson.com/articles/modern-data-governance-problems>
- Te Mana Raraunga: <https://www.temanararaunga.maori.nz/> (Māori independent organisation dedicated to Māori data sovereignty)
- Te Kāhui Raraunga: <https://www.kahuiraraunga.io/> (Iwi Leaders independent organisation dedicated to Māori data sovereignty)

- Tawhiti Nuku Roadmap: <https://www.kahuiraraunga.io/maoridatagovernance> (Māori Data Governance Roadmap by Te Kāhui Raraunga)
- New Zealand Privacy Commissioner: <https://www.privacy.org.nz/> (Government agency responsible for privacy and data protection in New Zealand)
- Smith, Linda Tuhiwai. "Kaitiakitanga: Māori concepts of guardianship." In *Decolonizing methodologies: Research and indigenous peoples*, edited by Linda Tuhiwai Smith, 145-170. London: Routledge, 2012.
- Jones, Michael. "Rangatiratanga: Māori authority and leadership." In *Te Ara: The Encyclopaedia of New Zealand*, edited by the Ministry for Culture and Heritage. Wellington, New Zealand: Te Ara, 2008.
- Durie, Mason. "Manaakitanga: The politics of Māori hospitality." *The Journal of the Polynesian Society* 109.4 (2000): 459-474.
- Mead, Aroha, and Tahu Kukutai. "Whanaungatanga: Towards a politics of relationships." *Sites* 1 (2009): 1-19.
- Edwards, Kahu. "Building social license for data governance: A Te Ao Māori approach." *Journal of Indigenous Affairs* 23.2 (2022): 1-18.
- Taylor, Paul, and David Vaile. "Building social license for data governance: A framework for policy and practice." *Australasian Public Affairs Journal* 20.2 (2016): 177-194.
- Hodge, Graeme, and Neil Lawrence. "The social licence to govern: A conceptual framework." *Public Administration* 89.2 (2011): 157-174.
- Brundtland Commission. "Our common future: Report of the World Commission on Environment and Development." United Nations, 1987.
- Te Whanake. "Building trust in data governance: A case study of Te Ao Māori principles." Wellington, New Zealand: Te Whanake, 2022.
- Aotearoa New Zealand Health and Disability System Review. "Waiora: A report on the future of health and disability care in Aotearoa New Zealand." Wellington, New Zealand: Ministry of Health, 2022.
- Lederer, Paul. "Data sovereignty: A case study of Indigenous data governance in Canada." *Journal of Indigenous Affairs* 22.1 (2021): 1-19.
- Te Rourou: Māori Knowledge Commons: <https://kep.org.nz/module-8/1-whakatau%C4%81k%C4%AB> (Māori digital library and knowledge repository)
- Māori Data Leadership Group: <https://data.govt.nz/toolkit/data-governance/maori/> (Government advisory group on Māori data issues)
- He Tangata Waiora: The Māori Health Strategy: <https://www.health.govt.nz/new-zealand-health-system/setting-direction-our-new-health-system/pae-tu-hauora-maori-strategy> (Government strategy for improving Māori health outcomes)