Coversheet: Progressing Digital Identity: Establishing a Trust Framework

Advising agencies	Department of Internal Affairs
Decision sought	Approval to proceed with the preferred option
Proposing Ministers	Minister for Government Digital Services Minister of Internal Affairs

Summary: Problem and Proposed Approach

Problem Definition

What problem or opportunity does this proposal seek to address? Why is Government intervention required?

New Zealand lacks consistently applied standards and processes for sharing, storing and using personal and organisational information in a digital environment. As a result, systems and services have been developed in an unstructured and inconsistent manner that creates inefficiencies, increases security and privacy risks and hinders interoperability. This is undermining consumer trust and confidence in digital identity[1] services at a time when more and more transactions are taking place online, and the ability to share information digitally to assert one's information is becoming increasingly vital to daily life and a key foundation for the economy. A governance and compliance regime is required to ensure that those who are providing digital identity services consistently meet legislation and standards for using, storing and sharing personal and organisational information. This will imbue the ecosystem with consistency and trust, encourage uptake, enable the flow of information, improve user experience, reduce identity theft, and position the digital identity ecosystem to realise the significant social and economic benefits digital identity services can provide.

Summary of Preferred Option or Conclusion (if no preferred option)

How will the agency's preferred approach work to bring about the desired change? Why is this the preferred option? Why is it feasible? Is the preferred approach likely to be reflected in the Cabinet paper?

The preferred government intervention, as outlined in the Cabinet paper, is the implementation of a regulatory framework to ensure minimum standards are consistently applied across the digital identity ecosystem. This intervention would include:

- The establishment of a Digital Identity Trust Framework (Trust Framework) to set the rules (standards, legislation) for those participating in New Zealand's digital identity ecosystem.
- The establishment of a governance board to exercise control over the Trust Framework and to update and maintain its rules as required.

[1] Digital identity is defined as 'user-initiated, digitally-enabled sharing of personal and organisational information'.

- The establishment of an accreditation team to ensure entities are complying with the rules of the Trust Framework.
- The introduction of a new Bill to establish the powers of the Trust Framework, its governance board and accreditation team, as well as introduce amendments to pre-existing legislation to ensure alignment with the Trust Framework.

This would be achieved in two phases.

- **Phase one: the implementation of an interim Trust Framework to allow compliance testing of digital solutions (2020-22).** Under the interim Trust Framework, officials will develop the Trust Framework rules (largely based on existing and developing standards and legislation) and work with a limited number of entities to test their systems against the rules. This will provide participating entities with an opportunity to align their systems with the Trust Framework and ensure they are well positioned to become formally accredited once the Trust Framework is established in legislation (see below). It also provides government with the ability to assess existing and emerging digital identity solutions to ensure they are meeting best practice for identification management, privacy and security while the legislation is under development. This approach aligns well with international models such as Australia's Trusted Digital Identity Framework. In this interim phase, a cross-agency governance group will be established to approve the rules and the compliance testing process. Work will also be initiated to develop a Bill to formally establish the Trust Framework and make amendments to pre-existing legislation necessary to give effect to the Trust Framework. This Bill is likely to be introduced to the House of Representatives in 2021. The anticipated cost of this phase is $3.260 million.

- **Phase two: the formal establishment of the Trust Framework (2022-25).** In this phase, the Trust Framework is established in legislation and becomes legally enforceable. The governance board becomes formalised with its powers and parameters formally established in legislation. The compliance process in phase one transitions into a formal accreditation regime, where systems can be tested against legally enforceable rules, and compliance can be formally recognised. The limitations on the number of entities being assessed against the rules are relaxed and any entity wishing to participate in the trusted digital identity ecosystem can apply to undergo assessment. The Bill will provide the accreditation body with the power to implement a cost-recovery model and charge for accreditation. The anticipated cost of this phase is $3.75 million. The outyear costs of running the Trust Framework will be confirmed once cost recovery policy is confirmed.

The government-led option outlined above is preferred because:

- The intervention outlined above would even out the digital identity playing field, increase people's trust and confidence in digital identity services, and position the ecosystem to realise the significant potential of trusted information sharing via digital means.
- There is a strong imperative to implement an intervention in the near future, especially now that Covid-19 is accelerating demand for digital identity services and solutions. The intervention outlined above could be established in the near term

and scaled in the future, if required, while a larger, more expansive regulatory regime would take considerable time to establish and may not be fit for purpose.

- The private sector is not in a position to implement a regulatory framework itself and has requested government take the lead on this issue.
- A limited government intervention (e.g. the recommendation of best practice guidelines without any associated compliance mechanisms) would do little to remedy the deficiencies within the current ecosystem.

Section B: Summary Impacts: Benefits and costs

Who are the main expected beneficiaries and what is the nature of the expected benefit?

In broad terms, the proposed intervention will bring consistency, trust, structure and efficiency to the digital identity ecosystem. This will produce a wide range of benefits for individuals, businesses, organisations, government and society in general, and these benefits will likely outweigh the costs to government of implementing and administering a new regulatory framework.

Some of the specific benefits of implementing a Trust Framework are outlined below across four categories.

People: Improved access to online services; improved customer experience; greater confidence that personal and organisational information is secure and private; reduced risk and reduced identification fraud; greater control over personal and organisational information; greater transparency around where that information is stored and how it is used.

Examples

- Not having to be physically present to gain access to services e.g. by digitally sharing my prescriptions with a pharmacy.
- Not needing to keep physical documents on your person e.g. you could maintain an electronic version of your driver's licence on your phone.
- Reducing the requirement to reproduce the same documentation every time you want to access different government services, especially when it contains information above and beyond that needed to access the service.
- Reducing incidences of fraud will lower the associated costs of fraud to individuals, currently estimated at $13,627 per event with each victim having to spend on average 12 hours responding to their incident.

Businesses and organisations (both government and non-government): Improved service delivery potentially resulting in an expanding customer base; improved ease of business; improved brand reputation; greater efficiencies (e.g. less duplication, process streamlining); reduced fraud resulting from improved risk assessment; increased confidence to invest in digital solutions; potentially new revenue streams; increased ability to meet regulatory requirements; greater confidence in the validity of personal and organisational information that is being supplied for the purpose of a transaction.

Examples

- The sharing of trusted personal and organisational information within the digital identity ecosystem would make it easier for businesses to comply with Anti-Money Laundering/Countering the Financing of Terrorism obligations.
- Customers could be onboarded more efficiently, reducing the amount of time consumers waste on clunky processes and potentially resulting in greater levels of e-commerce spending.

Government: Improved service delivery; greater efficiencies (e.g. less duplication); improved record keeping increased confidence to invest in digital solutions; increased opportunities to break down information silos between business units and government agencies; improved ability to detect and deter security or privacy breaches of personal and organisational information; improved digital inclusion; greater trans-Tasman alignment; expected reduction in cost of RealMe services.

Examples

- Paper-based systems can be replaced with trusted digital solutions that consume less resources (e.g. employee hours, physical storage space), while offering greater efficiency.
- New Zealand and Australia would be able to align our respective digital identity Trust Frameworks enabling the trans-Tasman business environment.
- Reduced likelihood of serious data breaches, such as those experienced by the Ministry of Culture and Heritage (August 2019) and KiwiSaver provider Generate (February 2020).

Society: Greater interoperability between participants in the trusted digital identity ecosystem; clear and consistent rules for everybody wanting to participate in the trusted digital identity ecosystem, resulting in greater confidence in digital identity services; increased effectiveness in countering certain crimes; greater economic opportunities; improved facilitation of economic transactions, social interactions, and (potentially) political involvement.

Examples

- Enabling trusted digital identity will improve the ability of public and private sector entities to combat identification fraud and the crimes that are perpetuated by it.
- Improved outcomes for Māori resulting from a strong commitment to partner working with Māori in the development of the Trust Framework.
- International studies have suggested that the potential benefit of enabling digital identity services in a mature economy is between 0.5% and 3% of GDP (approximately $1.5 to $9 billion in NZD).[2]

Where do the costs fall?

Government will largely assume the financial cost of implementing and administering the Trust Framework.

[2] Australia Post has separately estimated that digital identity would be worth approximately 0.65% of Australia's GDP – approximately $11 billion. In many of the countries reviewed the benefits were based on a more limited array of attributes than is being considered for digital identity in New Zealand.

Costs to government

- Estimated at $7.1 million to implement and administer the Trust Framework: $3.26 million over phase one (2020-2022), and $3.75 million over phase two (2022-25).
- In phase one (2020-2022), government will assume the one-off cost for the initial compliance testing. The testing body will be authorised to employ a cost recovery model when formally established in phase two – as a result, in this phase, the one-off cost for initial compliance testing will pass to the entity seeking accreditation.
- For those government agencies that intend to become accredited, there is an estimated one-off cost of between $10,000-$250,000 (indicative) for every entity undergoing compliance testing. The exact costs involved in this cannot be determined at this time, but will become clearer during phase one (2020-2022) when officials will have a greater understanding of the rules, who wants to be involved in the Trust Framework and the type of systems they employ. The risk of these costs escalating exponentially beyond initial estimates will be mitigated by engaging with agencies as the rules and compliance processes are developed.

Cost to entities

Those entities undertaking testing so that they can be authorised to participate in the trusted digital identity ecosystem are likely to fall into the following categories with the following categories of costs:

Existing information systems that meet the Trust Framework criteria: no costs incurred.

Existing information systems and/or processes that do not meet the Trust Framework criteria: costs incurred to remediate or update to meet required standard. Huge range depending on the nature and functions of the software.

New information systems built and/or processes developed to meet Trust Framework criteria: costs likely to be integrated into the project itself.

The Department currently has no method by which to determine how many entities will be in each category, or if the costs will vary significantly depending on the role a participant plays in the ecosystem (e.g. information provider[3] vs infrastructure provider[4]). All of this will, however, be clarified during phase one (2020-2022) when the policies and processes around compliance testing will be developed.

In phase two, the testing body will be authorised to implement a cost-recovery model. Entities will assume the initial one-off testing costs assumed by government in phase one. The exact costs and the details of the cost-recovery model to be implemented will be determined during phase one (2020-2022).

[3] Information providers supply personal and organisational information that they hold.

[4] Infrastructure providers enable people to disclose their information and consent to share it.

Cost to entities for ongoing compliance obligations

Once approved to operate under the Trust Framework, entities will have ongoing maintenance obligations, likely to cost up to $100,000 (indicative) per annum. Exact obligations have yet to be determined but will possibly include annual reports and occasional reassessments. The cost of these obligations will not be borne by the government, but rather the entities which have successfully undertaken their initial compliance testing/accreditation and are operating under the Trust Framework. Officials have a low confidence in the indicative cost outlined above as the true cost can only be established once the compliance process, the rules that govern it, and the ongoing obligations are finalised.

Analysis

Overall, the monetary and non-monetary benefits of implementing a Trust Framework are likely to exceed the costs. If the Trust Framework enabled even 0.5% of digital identity's $1.5 billion per annum potential, the total cost of the programme at $7.1 million would be substantially less than $7.5 million per annum of benefits generated. Over 5 years this would mean that for every $1 invested into the Trust Framework, approximately $5.36 of value would be generated on average.

What are the likely risks and unintended impacts? how significant are they and how will they be minimised or mitigated?

The main risks are primarily economic in nature. These are outlined below and are matched against their significance and the measures intended to mitigate these risks.

RISK	EXAMPLES	POTENTIAL OUTCOMES	ASSUMPTIONS	MITIGATION MEASURES	ASESSMENT
Costs become excessive for government and/or private sector	The actual costs of compliance testing turns out to be significantly higher than the initial indicative costs. This would affect Government in phase one (2020-22) as government is covering the cost of this testing. In phase two (2022-25) the entity seeking accreditation, whether public or private, will likely assume this cost. The Trust Framework requires more resources than anticipated to set up and/or maintain, increasing overall costs for government. Costs to upgrade systems to meet Trust Framework requirements are significantly higher than originally estimated, adding additional strain to the budget of the private or public sector entity seeking to join the Trust Framework.	Budgets are undermined Costs discourage participation in the Trust Framework	Reasonable costs will encourage participation	Government assumes the risk with regard to the cost of testing. In order to mitigate this risk, government will cover the cost of compliance testing during phase one of the Trust Framework (2020-2022) and work with partners to test and develop compliance processes in such a manner that compliance testing costs remain reasonable and appropriate going forward. The entity undergoing compliance testing assumes the cost of upgrading their systems. In the case of public sector entities, government can mitigate this through budget planning, however, private sector entities remain responsible for their own budgets.	The mitigation measures will ensure this is a low probability risk.
The Trust Framework does not enable Te Ao Māori approaches to identity	Māori do not participate equitably in the digital identity ecosystem. Māori perspectives and approaches to identity are not enabled by the digital identity ecosystem. The digital identity ecosystem is not developed and maintained in partnership with Māori. Māori are not supported in leadership and decision-making roles to ensure Māori perspectives about data are embedded in the trusted digital identity ecosystem.	Undermines the government's commitments to digital inclusion Discourages Māori participation in digital identity and limits the potential benefits of digital identity for Māori communities	It is necessary to encourage Māori participation and better understand the opportunities for Māori in implementing the Trust Framework.	Government assumes the risk. To mitigate this the principles of the Trust Framework, which will be enshrined in the Trust Framework Bill, will include 'inclusion' and 'Enabling Te Ao Māori approaches to identity'. Additionally, there will also be a Te Ao Māori government representative on the governance board of the Trust Framework, with the ability to co-opt non-voting members and appoint an Advisory Board.	The mitigation measures will ensure this is a low probability risk.
Uptake remains low	Entities judge that there is little extra to be gained by becoming part of the Trust Framework and continue to operate independently of it. People decide that it is more convenient to use digital identity services operating outside the Trust Framework, even though they are less secure.	The potential benefits of the Trust Framework remain unrealised for everyone in society Ongoing government funding is committed to a regulatory framework which produces little value	People want a trusted digital identity ecosystem	Both government and private sector assume this risk. The government will mitigate this risk during phase one of the Trust Framework by testing processes and policies to ensure the Trust Framework is implemented in a fashion that meets the requirements and needs of all ecosystem participants.	This risk will remain a realistic possibility because, although government can implement a regulatory regime that accredits digital identity services, it remains dependent on individuals to choose to use those services instead of non-accredited ones.

Social inequalities creep in	The Trust Framework promotes growth in digital identity services, which has the unintended consequence of exacerbating the ‘digital divide’ and creates barriers for disadvantaged groups (e.g. the elderly, refugees).	Discourages participation Undermines the government’s commitments to digital inclusion The potential benefits of the Trust Framework remain unrealised for everyone in society	People from all communities deserve the opportunity to participate in the digital identity ecosystem	Both government and private sector assume this risk. The government will mitigate this risk by ensuring the principle of inclusion (below) will be enshrined in the Trust Framework Bill as one of the guiding principles for the Trust Framework and trusted digital identity ecosystem. ***Inclusive*** *Everyone has the right to participate in the digital identity ecosystem.* *Key measures* • *The digital identity ecosystem can reflect the needs and requirements of a broad range of stakeholders.* • *Barriers to participation in the digital identity ecosystem−whether they be social, financial, or technical−are minimised, without compromising security or privacy.* • *Everyone is able to use digital identity services without risk of discrimination or exclusion.*	This risk will remain a realistic possibility. The Framework will not raise any regulatory barriers to inclusion but while it will set the standards that private sector entities will adhere to, it will be up to private sector entities to develop, invest in and offer digital identity services.

Section C: Evidence certainty and quality assurance

Agency rating of evidence certainty?

The Department's overall evidence of certainty rating is moderate-high.

Option development was informed by extensive stakeholder engagement over the past 18 months.

- This involved not only surveys and focus groups, but also consultation with over 100 organisations, including public agencies, Crown entities, digital service providers, financial institutions, academic institutions and a wide range of international partners.

The Department has high confidence that the evidence base supports the implementation of a trust framework in the near future.

- It was clear from this consultation that stakeholders broadly supported the development of a trusted ecosystem, that this would be important for both the economy and society, and that government should take the lead on this issue.
- Comparable jurisdictions (Canada, Australia, the United Kingdom) have chosen to develop trust frameworks. Australia already has a digital identity trust framework in place and is in the process of formalising this framework in legislation. New Zealand seeks to establish a Trust Framework to help align with these jurisdictions.
- Recent meetings have indicated an increasing interest from public and private sector stakeholders in a near-term government-led intervention to bring trust and consistency to the digital identity ecosystem. This has been prompted by the Covid-19 pandemic, the resulting acceleration in digital transformation in all spheres of life, and the need to support post-Covid economic recovery.

The Department has moderate confidence that the evidence base supports the specific details of the preferred option outlined in this document.

- The Department has moderate confidence in the evidence supporting some aspects of the preferred option because the exact nature of the compliance testing and costs involved will not be determined until phase one of the Trust Framework (2020-2022), and the details of the proposed Trust Framework Bill have yet to be finalised. Similarly, while international partners are also implementing frameworks this is a new development and there is not a significant body of historical evidence regarding what works and what does not.

To be completed by quality assurers:

Quality Assurance Reviewing Agency:
The Department of Internal Affairs, with a representative from Treasury supporting the panel.
Quality Assurance Assessment:
The panel considers that the information and analysis summarised in the RIA *meets* the quality assurance criteria.
Reviewer Comments and Recommendations:
The RIA clearly explains complex concepts using plain English and is concise relative to the nature of the issues being discussed. It convincingly describes the issues and sets out the full range of options. Assumptions, constraints and uncertainties are clearly stated, and it provides balanced analysis. Complete information is provided by setting out likely costs, where they fall, risks and mitigation measures. The RIA also identifies the range of potential impacts from options and links to other work. There has been appropriate consultation.

Impact Statement: A Digital Identity Trust Framework

Section 1: General information

1.1 Purpose

This Regulatory Impact Assessment provides an analysis of options and advice regarding interventions aimed at introducing consistency and trust into the digital identity ecosystem in New Zealand. The analysis and advice have been produced for the purpose of informing final policy decisions to be taken by Cabinet. The Department of Internal Affairs is solely responsible for the analysis and advice set out in this Regulatory Impact Assessment, except as otherwise explicitly indicated.

1.2 Key Limitations or Constraints on Analysis

As the world becomes increasingly digitised, every country around the world is having to come to terms with the emerging issues around the sharing, usage, and storage of information in a digital manner. Given these issues are relatively new, this placed some key limitation and constraints on the Department's analysis. These limitations and constraints are outlined below.

The variety in comparable jurisdictions

The Department consulted with a wide variety of international partners, including comparable jurisdictions such as the United Kingdom, Canada and Australia, to identify and assess intervention options. While there was broad agreement with establishing a Trust Framework, each country has to contend with certain unique features (e.g. federal structure, constitutional constraints). This created minor differences in approaches to the implementation of a Trust Framework which meant that lessons identified, and implementation options, could not always be readily adopted in the Department's options analysis. Sometimes assumptions had to be made regarding options in a New Zealand context, for example, as a unitary state New Zealand has national standards for identification management, whereas federal jurisdictions such as Australia need to align the identification standards and approaches of each state with a federal approach.

The limitations around consultation

All stakeholders were consulted on their views regarding the challenges with digital identity services and how they thought these could be addressed, but not all stakeholders were directly consulted on the options that are presented in this assessment. Additionally, engagement with Māori stakeholders remains in its infancy. Iwi have shown a desire to work collaboratively with government to enhance digital iwi registration processes in line with tikanga Māori, however, it takes time to establish enduring relationships. As a result of these challenges, some of the options analysis is based on assumptions that proposals would match to, and deliver on, the feedback received.

The ambiguity of terminology

Digital identity is an ambiguous term. As a result, the comparison of terms such as digital identity framework, digital identity ecosystem or digital identity services can be challenging because definitions are inconsistent and sometimes conflicting. As a result, this made it challenging to compare and analyse data sets and information.

The estimation of costs and benefits

While the benefits of the Trust Framework are highly likely to outweigh the costs, it can be challenging to measure the costs and benefits of digital identity and thus provide accurate figures for analysis. For example, different sectors benefit in different ways - banks may save money by improving inefficient onboarding processes, while government agencies may end up spending more money to provide a better service to the public. Also, a large increase in demand for compliance testing may increase costs to government, but not the benefit. As a result, The Department cannot have high confidence in its assessment of costs and benefits.

The lack of reliable figures to base analysis on

While officials have captured substantial anecdotal evidence regarding digital identity service challenges, it is rare for that information to be accompanied by reliable figures. For example, Non-Governmental Organisations have stated that obtaining Police checks multiple times for volunteers is time consuming and a significant frustration, but they are unable to quantify the full extent of the problem. As a result, the Department has had to base some of its analysis on assumptions and cannot have high confidence in some of its assessment.

The uncertainty regarding the details of compliance testing

Assessment of information systems is required to establish what should be tested for compliance and how it will be tested. This will not take place until phase one of the Trust Framework (2020-2022). As such, the analysis in this document could only be predicated on a basic concept of compliance testing and broad estimates of the costs involved.

The gaps in our evidence regarding value

Evidence demonstrated that business, government, and the public were all aware of the issues around digital identity services and wanted them resolved so that the value of information could be realised. This value, however, is different for each participant in the ecosystem. For example, a builder might value the ability to digitally share their qualifications because that reduces the time spent gaining access to a building site, while the construction company running the site values this process because it is less resource intensive than a process requiring physical documents. As a result, it was difficult to quantify and categorise value for all the participants of the ecosystem. It was also challenging to identify which participants might look to implement solutions based on the Trust Framework first.

1.3 Responsible Manager (signature and date):

Al Bell

Alan Bell, Director, Digital Identity Transition Programme
Department of Internal Affairs

23 June 2020

Section 2: Problem definition and objectives

2.1 What is the current state within which action is proposed?

Digital identity is a critical enabler

With more and more activities taking place online, the ability to digitally share information about oneself to access services and conduct transactions is increasingly becoming a critical enabler of daily life and a foundation for the economy. For example, on any given day, a person might use digital identity services to:

- Open a bank account
- Pay bills
- Shop online
- Work from home
- Undertake education
- Access healthcare
- Access government services

As a result, digital identity services have significance for individuals, businesses, organisations, government agencies, and society in general.

The current state of digital identity in New Zealand

The digital identity ecosystem in New Zealand−that is, the network of users, relying parties, information providers, and infrastructure providers that support the digital sharing of information for a variety of purposes−has emerged in an ad hoc fashion and lacks consistently applied standards and processes for sharing, storing and using personal and organisational information in a digital environment. As a result it is unstructured, and inefficient. Government plays a role, but it is not a comprehensive or overarching role. Instead government applies some rules and provides a RealMe verified identity, which is a government sponsored identity verification service among many private sector solutions. The private sector drives the marketplace, but businesses and organisations vary in how they implement identification, security and privacy, and in how they store, manage and use people's information. All of this undermines consumer trust in digital identity services, impedes the flow of information, and prevents the realisation of the potential benefits on offer.

Intervention will bring consistency and trust

Almost certainly. A government intervention to imbue the digital identity ecosystem with consistency and trust would encourage the use of digital identity services, enable the flow of information, and position the digital identity ecosystem to realise the significant social and economic benefits digital identity services can provide. The implementation of a Trust Framework would be the best option for a government intervention.

RealMe will have a role to play

A product-based solution on its own is unlikely to provide the comprehensive response required for the ecosystem, which relates to a wider sharing of attributes from both the public and private sector. As the government's foremost digital identity service, RealMe will almost certainly have a role to play under the Trust Framework. The exact nature and scope of this involvement has yet to be determined.

Without intervention the situation will not improve

A private sector response that would address the aforementioned issues in a comprehensive fashion is highly unlikely to emerge and the private sector would continue to develop its own rules and standards without government direction. The challenges within the digital identity ecosystem would remain unchanged, but would be increasingly exacerbated by the ongoing digital transformation occurring in all spheres of life – a trend recently accelerated by the Covid-19 pandemic. Trust in digital identity services would remain low, information would remain siloed, and the flow of information impeded. Furthermore, without intervention the digital identity ecosystem in New Zealand would not be positioned to realise the significant opportunities trusted digital identity could offer, the economic benefits of which alone are estimated at approximately NZD $1.5 billion per annum.[5]

2.2 What regulatory system(s) are already in place?

A review of the legislative landscape was undertaken by the Department. The review indicated that there are a variety of rules that govern the use of personal and organisational information in New Zealand. These include:

- **overarching legislation** such as the Privacy Act 1993 which controls how agencies collect, use, disclose, store and give access to personal information.
- **identity-related legislation** such as the Electronic Identity Verification Act 2012, which regulates the operation of the government's RealMe service, and the Identity Information Confirmation Act 2012.
- **sector specific legislation** such as the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 which aims to prevent money laundering and terrorist financing in New Zealand.
- **standards** like the Evidence of Identity standard which outlines requirements for consistent identity establishment and confirmation by agencies (currently being updated).

While this current regulatory environment enables some trust in the digital identity ecosystem, it does so in a restricted fashion, for example:

- The different legal requirements and definitions (e.g. for 'identity') for different sectors can result in a siloed approach to services.
- Some legislation creates barriers to the provision of digital identity services by prohibiting the consented sharing of information held by certain government agencies (e.g. the Births, Deaths, Marriages and Relationships Registration Act 1995), or by having overly prescriptive provisions which have become out of date (e.g. the Public Records Act 2005 being framed around paper-based systems or statutory declaration requirements).

[5] International studies have suggested that the potential benefit of enabling trusted digital identity in a mature economy is between 0.5% and 3% of GDP equivalent. If these figures are applied to New Zealand, the potential value is between $1.48 billion and $8.88 billion NZD (based on 2016 figures). We anticipate that the approximate value of digital identity to the New Zealand economy is up to $1.5 billion NZD of GDP equivalent per annum.

- Some standards (e.g. the Evidence of Identity standard) are just best practice guidelines, as opposed to mandated requirements.
- Some legislation prescribes outdated or onerous requirements (e.g. those organisations wanting to be verified relying parties under the Electronic Identity Verification Act 2012 are required to be listed in a schedule to the Act).

As a result, this collection of regulatory instruments is not fit for purpose in terms of imbuing the digital identity ecosystem with consistency, trust and scale.

New government regulation could provide the overarching structure to support the digital identity ecosystem. Government regulation would be preferable to private arrangements because it would bring consistency to the ecosystem. Private arrangements tend to promote fragmentation and inconsistency since they are usually implemented through bilateral or multilateral contracts between several parties. Furthermore, through consultation, private sector stakeholders have indicated a preference for the establishment of a government-led compliance regime to consistently apply common rules across the digital identity ecosystem.

Any move to advance regulation in the digital identity ecosystem will directly impact:

- **RealMe and its funding.** RealMe is the government’s foremost digital identity service. Uptake for the service has not been as high as originally anticipated and the market has changed significantly since it was introduced. While RealMe is based on a centralised model, globally and in New Zealand there has been an emergence of digital identity service providers who are developing decentralised operating approaches that allow the customer/citizen to have greater control of their information. These new approaches seek to realise the economic benefits while minimising data transfer and enhancing security and privacy. It is anticipated that RealMe (or parts of it) will be brought into the Trust Framework, however, because the scope and nature of its involvement has yet to be determined, the expected impacts on its funding are currently unclear.
- **The Electronic Identity Verification Act 2012**. It is highly likely that legislative amendments to the Act will be required to facilitate the practical use of the Trust Framework for agencies.
- **Potentially, a wider range of legislation.** The Trust Framework Bill would not supersede other legislation, but minor amendments may be required to remove obstacles in other legislation and facilitate opportunities for the Trust Framework and digital solutions. This could include, for example, an amendment to allow the use of digital signatures instead of requiring a physical signature on a paper document. Amendments could be made to any Act dealing with the use of personal information and identity such as the Privacy Act 1993, the Public Records Act 2005, the Identity Information Confirmation Act 2012, Birth, Deaths, Marriages, and Relationships Registration Act 1995, Passports Act 1992, Citizenship Act 1977, Land Transport Act 1998, The Children, Young Persons, and Their Families Act 1989/Oranga Tamariki Act 1989, Family Violence Act 2018, and the Vulnerable Children’s Act 2014.

Other sector specific work in digital identity is likely to complement the Trust Framework, for example:

- The Ministry of Social Development is undertaking work to digitally enable people to apply for support, sharing identity credentials to show evidence of eligibility.
- The Ministry for Primary Industries and the Ministry for Business Innovation and Employment are undertaking work on integrated farm planning that will require standards and processes for sharing of identity related attributes for people and other entities in the food and fibre sector.
- The Ministry of Health is undertaking work to understand their requirements and barriers to implementing effective digital identity in the health sector.
- The Ministry of Education is undertaking early policy work in understanding what is needed to further enhance their digital systems in the future.

2.3 What is the policy problem or opportunity?

New Zealand lacks consistently applied standards and processes for sharing, storing and using personal and organisational information in a digital environment. Legislation and standards exist but they are found in a variety of places, and while some of these requirements are legally binding and some are non-binding guidance or best practice. Consequently, organisations vary in how they manage information, creating inefficiencies and undermining the trust and confidence in the digital identity ecosystem for individuals, the private sector and government agencies. Ultimately, all of this impedes people's ability to access services online, undermines their expectations regarding privacy and security, stifles innovation in service provision, and hinders the realisation of the significant social and economic benefits digital identity services could provide. Government intervention is almost certainly required to address these issues in a comprehensive fashion.

2.4 What do stakeholders think about the problem?

A wide group of stakeholders are affected by the digital identity ecosystem in New Zealand, including individuals, communities, public agencies, Crown entities, digital service providers, financial institutions, academic institutions, and overseas jurisdictions. These stakeholders play various roles within the ecosystem, such as users, information providers, relying parties and infrastructure providers. They are not limited to one role, and their roles vary dependent on context, for example, a bank could be either an information provider or a relying party depending on the transaction being undertaken.

To ascertain the views of these stakeholders, extensive consultation was undertaken both with individuals and over 100 public, private and non-governmental entities. This was achieved through face to face meetings, regular workshops, surveys and focus groups over an 18 month period. The key takeaways from this consultation are outlined below.

Stakeholders broadly agreed on the challenges faced by the digital identity ecosystem in New Zealand.

- People generally felt as if they had lost control of their information, and both individuals and companies were concerned about the security of their information.

- Consumers trust in digital identity services was low. People were wary of providing their information online to private sector companies, out of concern this information could be exploited for commercial gain.
- Non-Governmental Organisations were frustrated that it was not easy to reuse information digitally, primarily because volunteers were having to undergo multiple Police checks.
- Public agencies find it challenging to offer digital services in instances where their customers cannot easily demonstrate who they are or what they are entitled to.
- Industry saw a need for greater consistency, streamlined compliance, and the simplification of processes to make identification services more efficient.

There was also a general preference for a government-led intervention to bring consistency and trust to the digital identity ecosystem.

- People found the prospect of having greater control of their personal information to be appealing.
- Focus group participants preferred the government to take the lead on this issue because government was generally viewed as a reliable actor motivated by public good rather than commercial gain.
- Industry demonstrated enthusiasm to work with government to develop a digital identity trust framework to set the rules of engagement for the digital identity ecosystem.
- Public agencies were keen to work together on approaches that could leverage each other's insights and capabilities for efficient and consistent consented information sharing to address specific issues they each faced in delivering services to the public.

Though there were some concerns about the prospect of a government intervention.

- Users of digital identity services expressed concern about the potential for government to implement an intervention which might provide greater access to personal information for surveillance purposes.
- Māori representatives raised concerns about the establishment of a system that might see government holding more information about them, largely due to historic misuse and abuse of Māori data.
- Some individuals expressed a strong preference for tighter rules specifically for the private sector, based on an assumption that the private sector would be driven by a desire to monetise data, while public sector agencies would be focused on the delivery of public services.

Further consultation

Anecdotal evidence suggests the desire for a government-led intervention had been strengthened in both the public and private sector by the recent Covid-19 pandemic, due to the accelerated digital transformation it has prompted and the need to support post-Covid economic recovery. Despite this development, the Department does not anticipate conducting another round of stakeholder consultation regarding the challenges facing digital identity and possible interventions. A public engagement process will, however, be undertaken as part of the development of a Trust Framework Bill.

2.5 What are the objectives sought in relation to the identified problem?

To develop a trusted, consistent and sustainable digital identity ecosystem in New Zealand which will encourage the use of digital identity services to access services and conduct transactions.

Section 3: Option identification

3.1 What options are available to address the problem?

We have identified four options for achieving the objective of trusted, consistent and sustainable digital identity ecosystem.

Scope

When developing these options, the Department did not consider:

- **The implementation of unique national identifiers**. There was no social licence for such a system and such a development would not align with principle 12 (Unique Identifiers) of The Privacy Act 1993.
- **Non-consented information sharing**. The Department has defined digital identity as 'the user-initiated, digitally-enabled sharing of personal and organisational information' and the promotion of non-consented information sharing would be contrary to this.

Options were, however, based on the assumptions that:

- The current digital identity ecosystem is unstructured, inconsistent and inefficient; and, as a result, it is a low trust environment.
- Establishing and consistently applying rules to the digital identity ecosystem would instil greater trust in digital identity services.

Option 1 – A non-regulatory Trust Framework: establish a team within a government agency to develop a set of best practice rules and standards for digital identity services. A cross-agency governance group would be responsible for maintaining and updating the rules. A team within the Department of Internal Affairs would be responsible for compliance testing against the standards. This testing would have no legal effect, and would instead serve to support trust and promote the development of efficient and interoperable services across the digital identity ecosystem.

Option 2 – Legislative amendments to status quo supported by publication of best practice standards: make amendments to relevant legislation such as the Electronic Identity Verification Act 2012 (the EIV Act) and mandate Identification Management Standards for agencies, to enable a wider range of user-consented information sharing and oversight by government. The Government Chief Digital Officer (GCDO) would publish the standards that make up the proposed Trust Framework as best practice guidance for public, private and non-government sector entities.

Option 3 – Trust Framework: government department-based governance and accreditation (preferred option): Establish a Trust Framework, overseen by a governance board established within a government department. On this board, government representatives would have voting rights on amendments to the Trust Framework, while non-government independent advisors would support their decision making. The board would be supported by an accreditation team, based in a pre-existing government department. A Bill would be introduced to establish the powers of the Trust Framework and its governance board, and to make any consequential amendments required. This option would be implemented in two stages - phase one: interim Trust Framework (2020-22), which will be an informal testing and transition phase, and phase two (2022-25) which will involve the formal implementation of the Trust Framework in legislation.

This option aligns with Australia which has implemented a standards-based Trust Framework with government-led accreditation and governance.

Option 4 – Trust Framework: accreditation scheme run at a distance from primary government: Similar to Option 3 but with an independent governance board established outside of an existing government department. The board would also establish a new entity responsible for accrediting participants in the Trust Framework. This would result in less government control over the governance of the Trust Framework, but would allow for representation of non-government interests on the board. There would be no interim phase under this option, and it would only become operational once the new entity is established and a new Trust Framework Bill was passed.

Options 3 and 4 are not necessarily mutually exclusive. It would be possible to start off with Option 3 and then move to Option 4 in the future if the government determined there would be value in such a move.

The development of these options was informed by extensive stakeholder engagement, involving surveys, focus groups and consultation with over 100 organisations, including public agencies, Crown entities, digital service providers, financial institutions, and academic institutions. It was clear from this consultation that the development of a trusted ecosystem would be important for both the economy and society.

Consultation also took place with a wide range of international partners, all of whom are attempting to implement national-level responses to digital identity issues.

What criteria, in addition to monetary costs and benefits have been used to assess the likely impacts of the options under consideration?

Outlined below are the categories/questions against which the options were assessed.

Principles: This option is consistent with the principles that would underlie a trusted and consistent digital identity ecosystem in New Zealand (e.g. people-centred, inclusive, secure, privacy enabling, sustainable, interoperable, enabling Te Ao Māori approaches, open and transparent).

Trust: This option will instil trust in digital identity. In the event an incident/breach of responsibility undermines trust in the digital identity ecosystem there are (statutory and non-statutory) processes in place to remediate and restore that trust.

Feasibility: This option generates (social, economic, fiscal) value for participants in the ecosystem. This option encourages participation in the ecosystem. The estimated costs (set-up, ongoing) for government and other ecosystem participants are reasonable. This could be implemented within a reasonable timeframe.

Flexibility: This option is responsive to changes in social licence and the needs and requirements of participants. This option is responsive to the emergence of new technologies, new standards and protocols, and new approaches to the digital exchange of information. This option is scalable (i.e. able to grow).

3.3 What other options have been ruled out of scope, or not considered, and why?

A purely commercial model, in which the private sector assumes full responsibility for establishing and administering a framework for digital identity, was not considered because:

- Neither government nor stakeholders expressed an appetite for such an option.
- Such a model would not necessarily improve consumer confidence in digital identity services. The public remains wary of private sector exploitation of their information for commercial gain, but generally views the government as a reliable actor.
- A purely commercial model would probably rely on best practice guidelines (which are currently mandated and non-mandated standards and legislation) and have limited enforcement capabilities. This would not be as effective as a government-led Trust Framework backed by legislation at bringing consistency and structure to the digital identity ecosystem.

Section 4: Impact Analysis

Marginal impact: How does each of the options identified in section 3.1 compare with taking no action under each of the criteria set out in section 3.2?

Key:

++	much better than doing nothing/the status quo
+	better than doing nothing/the status quo
0	about the same as doing nothing/the status quo
-	worse than doing nothing/the status quo
- -	much worse than doing nothing/the status quo

Option	**Status quo - No change**	**Option 1 – A non-regulatory Trust Framework**	**Option 2 – Legislative amendments to status quo supported by publication of best practice standards**	**Option 3 – Trust Framework with government department-based governance and accreditation (preferred option)**	**Option 4 – Trust Framework with accreditation scheme run at a distance from primary government**
Option description	Maintain the status quo in New Zealand's digital identity ecosystem and continue with existing legislation, standards (both mandated and non-mandated) and no overarching system oversight.	Maintains the legal status quo, but establishes a set of best practice rules and standards, and a team within a government agency to carry out compliance testing against the standards. This compliance testing would not be legally-binding, but would serve to promote trust and interoperability between digital identity services. A cross-agency governance body would be established to maintain and update the non-regulatory Trust Framework.	Largely maintain the status quo but make amendments to relevant legislation such as the Electronic Identity Verification Act and mandate Identification Management Standards for agencies, to enable a wider range of citizen-consented information sharing and oversight by government. The GCDO would also publish the standards that make up the proposed Trust Framework as best practice guidance for public, private and non-government sector entities.	Establish a Trust Framework, with rules that promote trust and enable interoperability, overseen by a statutory board established within a department. On this board, government representatives would have voting rights on amendments to the Trust Framework, while non-government independent advisors would support their decision making. The board would be supported by a compliance team, based in a pre-existing government department. Introduction of a new Bill to establish powers of the Trust Framework and its governance body and amendments to the Electronic Identity Verification Act and other relevant legislation. This option would be implemented in two stages: phase one: interim Trust Framework (2020-22), which will be an informal testing and transition phase, and phase two (2022-25) which will involve the formal implementation of the Trust Framework in legislation.	Similar to Option 3 but with the governance body established outside of a department. The Board would also establish a new entity responsible for accrediting participants in the Trust Framework. This would result in less government control over the management of the Trust Framework, but would allow for wider representation of non-government interests. There would be no interim phase under this option, and it would only become operational once the new entity is established and a new Trust Framework Bill was passed.
Principles Is this option consistent with the principles that would underlie a consistent and trusted digital identity ecosystem in New Zealand (i.e. people-centred, inclusive, secure, privacy enabling, sustainable, enabling Te Ao Māori approaches to identity, interoperable, open and transparent)?	**0** People-centred/Inclusive – Low. Not people-centred, or inclusive as existing regime relates to a limited range of organisations and enables limited individual control over their own information. Secure/Privacy enabling – Low. Limited security and privacy settings, as breaches of the Privacy Act only enforceable when significant harm occurs and no set standards across all organisations. Interoperable – Low. Limited ability to establish interoperability both domestically and internationally, as no agreed way that information sharing occurs across sectors in New Zealand. Sustainable – Low. Continues to produce cost-inefficiencies, while	+ People-centred – Medium. Could help to promote standards that improve the experience for users. Inclusive – Medium. Government supports inclusivity through compliance testing. Secure – Low. Standards around security will be set out, but not legally enforceable. Privacy – Low. Standards around privacy would be set out, but not legally enforceable. Sustainable – High. Few barriers to entry, and cross-agency oversight would help to keep standards current. Interoperability – Medium. Will promote interoperability within	+ People-centred – Low. Minimal improvements to current situation for people. Inclusive – Medium. Will not impede or promote inclusivity. Secure/Privacy-enabling – Low. Limited security and privacy settings, as breaches of the Privacy Act only enforceable when significant harm occurs and no set standards across all organisations. Negligible improvements. Sustainable – High. Low cost, would potentially encourage greater participation in digital identity, would potentially result in a more effective environment.	++ People-centred – High. The mandating of identity management and security standards would better ensure that people's information is being shared in a manner that is consistent with standards and legislation. Inclusive - High. Government intentionally promotes inclusivity. Secure - High. Government oversight will ensure security requirements are being met, which was a key concern for focus group participants. Privacy-enabling - High. The Trust Framework would introduce and consistently apply privacy standards across the digital identity ecosystem. Government oversight will ensure privacy standards are being met, which was a key concern for focus group participants.	++ Similar to 3 though, improved inclusivity given the greater representation on the governance board. Sustainability would be dependent on uptake. In a low uptake environment costs would significantly outweigh benefits, however, in a high uptake environment this option would allow for specialisation and scale.

Option	Status quo - No change	Option 1 – A non-regulatory Trust Framework	Option 2 – Legislative amendments to status quo supported by publication of best practice standards	Option 3 – Trust Framework with government department-based governance and accreditation (preferred option)	Option 4 – Trust Framework with accreditation scheme run at a distance from primary government
	impeding the ability to generate economic and social value. Open and transparent – Low. Little openness and transparency, with feedback revealing people perceive the lack of transparency from businesses and organisations as a key barrier to taking control of their own information.	NZ by setting out interoperability standards. Open and transparent – High. Government is committed to transparency and subject to OIA and public scrutiny. Government will publicly publish the standards providers are expected to comply with and could officially recognise which bodies have undergone compliance testing.	Interoperable – Low. Gains would be minimal. Open and transparent – Low. Government remains accountable to public.	Sustainable – High. Government oversight and consistency of accreditation would encourage participation because government is viewed as a reliable actor that has the resources to ensure that the system endures. The existence of a governance board would help to ensure that the Trust Framework remains fit for purpose and supports needs and requirements. Interoperable - High. Will ensure interoperability within NZ by consistently applying interoperability standards that all accredited parties must adhere to. Government intentionally promotes interoperability with Australia, and other key international partners. Open and transparent - High. Government is committed to transparency and subject to OIA and public scrutiny. Government will publicly publish the standards accredited bodies are expected to comply with and could officially recognise which bodies are accredited.	
Trust This option will instil trust in digital identity. In the event an incident/breach of responsibility undermines trust in the digital identity ecosystem there are (statutory and non-statutory) processes in place to remediate and restore that trust.	**0** Instil trust - Low. Limited ability to create and use verified information across services, as few enforceable rules apply across services. In a 2019 study, only 5% of NZ participants said they currently felt confident about their rights when it came to their digital identity and data storage.[6] Generate challenges – High. Individual's limited control of their digital information will be exacerbated by increasing digitisation of services. Remediate/restore trust – Low. Limited processes to restore trust as limited penalties and remedies in the Privacy Act and existing legislation that governs the RealMe services.	+ Instil trust – Medium. Government is generally viewed as a trusted actor, and having a centrally agreed set of best practice standards and rules will help to promote consistency across the ecosystem. However, without a means of holding participants to account, compliance with the standards would be uncertain, potentially undermining trust. Remediate/restore trust – Low. Without a means to hold providers to account, trust in the best practice standards could decline.	+ Instil trust – Medium. Improved ability to create and use verified information across services, with more enabling use of RealMe services, but still limited. Improved trust in government processes, with identity assurance introduced. Generate challenges – High. Individual's limited control of their digital information will be exacerbated by increasing digitisation of services. Remediate/restore trust – Low. Limited processes to restore trust as limited penalties and remedies in the Privacy Act and existing legislation that governs the RealMe services. .	++ Instil trust - High. Government is generally viewed as a trusted actor and having one point of contact for accreditation will ensure consistency across the ecosystem. Focus group feedback indicated that people felt like they had lost control of their information and the application and enforcement of stronger rules would increase their trust in digital identity services. Stakeholder feedback indicated a preference for government taking the lead in addressing digital identity issues as a private sector response might result in fragmentation and inconsistency across the digital identity ecosystem.	++ Same as Option 3 though focus group feedback specifically indicated a preference for digital identity to be regulated and monitored by an independent agency as it would be more reliable than governments which come and go.

[6] "Providing a Benchmark Understanding of Digital Identity Among New Zealanders", DINZ (April 2019)

Option	Status quo - No change	Option 1 – A non-regulatory Trust Framework	Option 2 – Legislative amendments to status quo supported by publication of best practice standards	Option 3 – Trust Framework with government department-based governance and accreditation (preferred option)	Option 4 – Trust Framework with accreditation scheme run at a distance from primary government
				Generate challenges – Low. Low probability risk that some people may view one authority having control of the entire process as potentially problematic. Low probability risk that despite people asking for more trusted digital identity services they don't use them because its more convenient to continue using riskier services. Low probability risk that the public misperceives this as putting their information at greater risk of exposure and misuse – focus group participants recognised their information had value to some organisations and were wary that advances in digital identity might result in them being targeted by advertising or result in more of their data being sold. Low probability risk that information remains siloed as entities holding information do not choose to become accredited. Low probability risk that trusted systems, products and services do not improve customer experience. Low probability risk that low uptake means that the potential benefits of the Trust Framework remain unrealised. Low probability risk that Māori needs and requirements are not addressed adequately despite Treaty of Waitangi obligations Remediate/restore trust – High. Government would ultimately retain the right to suspend or revoke accreditation.	
Feasibility This option generates (social, economic, fiscal) value for participants in the ecosystem. This option encourages participation in the ecosystem. The estimated costs (set -up, ongoing) for government and other ecosystem participants are reasonable. This could be implemented within a reasonable timeframe.	**0** Value – Low. Limited value continues for those that can interact with RealMe services. Low value for most of the population, as no ability to share information across sectors in a trusted way. Potential value undermined, with duplication of costs and over-investment. Possible lost opportunity cost to the New Zealand economy of up to $1.5b of GDP equivalent per annum, according to international studies. Participation – Low. Little incentive to trust and interact with other participants in the ecosystem as no clear parameters for how this should occur. Costs – Low. Existing costs to run regulatory regime continue, approximately $250,000 per annum	+ Value – Medium. A consistent compliance testing regime that can help to promote better standards for information security and privacy in the ecosystem. Having undergone compliance testing could be a reputational benefit for businesses, however without a means to enforce compliance, this may be limited. Participation – Medium. Moderate incentive to trust and interact with participants in the ecosystem. Costs of compliance testing may also act as a barrier to participation, especially if a lack of enforcement options is perceived to reduce the credibility of compliance testing.	+ Value – Medium. Improved value for those that interact with RealMe services as greater flexibility. Low value for most of the population, as no ability to share information across sectors in a trusted way. Potential value undermined, with duplication of costs and over-investment. Possible lost opportunity cost to the New Zealand economy of up to $1.5 billion of GDP equivalent per annum, according to international studies based on 2016 figures. Participation – Low. Little incentive to trust and interact with other participants in the ecosystem as no clear parameters for how this should occur. Costs – Medium. Approximately $1.3 million per annum over 2 to 3 years.	++ Value – High. A consistent compliance regime that improves information security and privacy for all, with flow on effects into public and private sector service delivery. Holding accreditation would be a reputational benefit for businesses and potentially open up new revenue opportunities. Participation – High. Likely to encourage participation given government is generally viewed as a reliable partner. However, the extent to which it encourages participation will almost certainly be dependent on the accreditation burden (costs, time, resources) imposed. Low probability risk that the Trust Framework requires more resources than anticipated to set up and/or maintain, increasing overall costs and discouraging participation. Low probability scenario: accreditation costs might be too high discouraging entities from becoming part of trusted digital identity ecosystem.	+ Value – High. A consistent compliance regime that improves information security and privacy for all, with flow on effects into public and private sector service delivery. Holding accreditation would be a reputational benefit for businesses and potentially open up new revenue opportunities. Allows for scalability. Economic value may be low though as the cost to establish this would be much higher than option 3 but it is not clear if the benefits such a system would outweigh the costs. Participation – unclear. Allows for high uptake. Ultimately, however, the extent to which this option encourages participation will almost certainly be dependent on the accreditation burden (costs, time, resources) imposed which are currently unknown. Low probability risk that the Trust Framework requires more resources than anticipated to set

Option	Status quo - No change	Option 1 – A non-regulatory Trust Framework	Option 2 – Legislative amendments to status quo supported by publication of best practice standards	Option 3 – Trust Framework with government department-based governance and accreditation (preferred option)	Option 4 – Trust Framework with accreditation scheme run at a distance from primary government
	which is currently maintained through existing agency baselines. Timeframe - n/a. Regime already in place.	Costs – Medium. Estimated costs – approximately $1 million per annum, which could be recovered from service providers. Timeframe – High. Could be stood up before the end of 2020.	Timeframe – Medium. Could be stood up with transitionary arrangements in the near future but legislative amendments likely to take 1-3 years.	Costs – Medium. Estimated costs - approximately $1 to $2 million per annum. Timeframe – Medium. Could be stood up with transitionary arrangements in the near future but would not be fully stood up until new legislation established (likely 2022).	up and/or maintain, increasing overall costs and discouraging participation. Low probability scenario: accreditation costs might be too high discouraging entities from becoming part of trusted digital identity ecosystem. Costs – High. Estimated costs approximately $2 to $4 million per annum. Timeframe – High. It will take some time to establish an entirely new entity and get it operational and this would be at odds for a requirement to establish a solution in the near future, especially now that the Covid-19 pandemic has accelerated digitalisation in all spheres of life.
Flexibility This option is responsive to changes in social licence and the needs and requirements of participants. This option is responsive to the emergence of new technologies, new standards and protocols, and new approaches to the digital exchange of information. This option is scalable (i.e. able to grow).	**0** Social licence, needs and requirements – Low. Limited ability to adapt to changes in social licence and participant requirements. No clear way to update and change rules on how this operates. Technology, standards, approaches – Low. Limited adaptability to new technology, particularly the application of the EIV Act due to its prescriptive nature. Scalability – Low. Very limited scalability as no levers to influence the wider ecosystem.	+ Social licence, needs and requirements – Medium. Government remains sensitive to public opinion, but generally slow to respond due to bureaucratic inertia. Technology, standards, approaches – High. Governance board will maintain regular review Inclusion of private sector/Te Ao Māori will possibly improve responsiveness. Scalability – Medium. Will depend on government funding.	+ Social licence, needs and requirements – Low. Minor improvements for RealMe customers. Technology, standards, approaches – Low. Responsive to standards as government will mandate, review and update Identity Management standards. Scalability – Low. Limited scalability.	++ Social licence, needs and requirements – Medium. Government remains sensitive to public opinion, but generally slow to respond due to bureaucratic inertia. Technology, standards, approaches – High. Representative governance board will maintain regular review Inclusion of industry/private sector will possibly improve responsiveness. Scalability – High. Scalable, depending on political will and government funding. Will allow for the consideration of other government solutions which may lead to a reduction in the cost of RealMe services because these could be incorporated into the Trust Framework. These solutions are currently restricted by existing legislation.	++ Same as Option 3.
Overall assessment	**0** **Advantages**: No additional costs to government, no need for time-consuming legislative action. **Disadvantages**: People will have little control over their information. The digital identity ecosystem remains unstructured, inconsistent and inefficient and, as a result, it is a low trust environment. The value of digital identity is not realised as there will be ongoing duplication, over-investment and lost opportunities. Constrained ability to improve service delivery, in either the public or private sector. Continues existing alienation of Māori from digital services. The accelerated adoption of digital solutions in all spheres of life resulting of the Covid-	+ **Advantages**: Establishes a best practice standard that could help to promote the wider adoption of practices that would support the development of the digital identity ecosystem and uptake of digital identity services. **Disadvantages**: the absence of any means of enforcing compliance with the standards and rules could quickly undermine public trust in the system, reducing uptake and the relevance of the standards to service providers. Constrained ability to improve service delivery, in either the public or private sector. Continues existing alienation of	+ **Advantages**: Minor improvements to status quo with best practice clear and some enforcement mechanisms. Simple and affordable for government. **Disadvantages**: The limited nature of the improvements on the status quo would ensure the digital identity ecosystem continues to be a low trust environment that does little to realise the potential value of digital identity. Inefficiencies remain. Continues existing alienation of Māori from digital services. It would take time to amend legislation.	++ **Advantages**: Creates a high trust environment that brings consistency and structure into digital identity in New Zealand. Could be established in a reasonable timeframe at reasonable cost, with provision to grow as required. Government maintains full control over accreditation process, ensuring consistency. Enables Māori-centric ontologies and approaches to be recognised and governance representation. Phase one (2020-22) will allow for compliance testing of digital identity systems in the near term but will also provide space for testing of Trust Framework systems and policies. Will allow for the consideration of other	++ **Similar to Option 4 but also…** **Advantages**: Allows for greater autonomy from government, board could be more industry focused, clear lines of accountability, can react quickly to changes in industry standards, can provide a long term solution by handling a high number of accreditations. Greater autonomy for Māori to run their own systems and governance representation, more distinct from government. **Disadvantages**: Expensive, complicated, low uptake would mean it runs inefficiently, cost model would be almost entirely dependent on crown funding in the short/medium term, will take longer to implement than other options, rules and scope under which it

Option	Status quo - No change	Option 1 – A non-regulatory Trust Framework	Option 2 – Legislative amendments to status quo supported by publication of best practice standards	Option 3 – Trust Framework with government department-based governance and accreditation (preferred option)	Option 4 – Trust Framework with accreditation scheme run at a distance from primary government
	19 pandemic causes the underlying issues with digital identity to be exacerbated.	Māori from digital services. The accelerated adoption of digital solutions in all spheres of life resulting of the Covid-19 pandemic causes the underlying issues with digital identity to be exacerbated.		government solutions which may lead to a reduction in the cost of RealMe services. **Disadvantages**: Government assumes all compliance costs in phase one (2020-22). Risks that compliance costs are higher than anticipated, that trusted services do not improve customer experience, or that the public thinks the Trust Framework makes their information less secure – all of which could discourage participation. Other risks: that information remains siloed, that overall costs for the Trust Framework are higher than anticipated, that low uptake means that the potential benefits of the Trust Framework remain unrealised.	operates remains unclear, may not provide value for money compared to other operational models, less ability for the government to intervene should something go wrong. Costs involved for Māori to develop their own interoperable systems.
Summary	**This would not achieve the objective of a consistent and trusted digital identity ecosystem.** In a scenario where there is no government intervention, a private sector response that would address the aforementioned issues in a comprehensive fashion is highly unlikely to emerge and the private sector would continue to develop its own rules and standards without government direction. The challenges within the digital identity ecosystem would remain unchanged, but would be increasingly exacerbated by the ongoing digital transformation occurring in all spheres of life – a trend recently accelerated by the Covid-19 pandemic. Trust in digital identity services would remain low, information would remain siloed, and the flow of information impeded. Furthermore, without intervention the digital identity ecosystem in New Zealand would not be positioned to realise the significant opportunities trusted digital identity could offer.	**This may help to support the achievement of a more consistent and trusted digital identity ecosystem, but there remain many uncertainties about the ability and willingness of service providers to comply.**	**This may help to support the achievement of a more consistent and trusted digital identity ecosystem, but there remain many uncertainties about the ability and willingness of service providers to comply.**	**This would achieve the objective of a consistent and trusted digital identity ecosystem.** A government-led intervention such as this would imbue the ecosystem with consistency and trust, encourage uptake, enable the flow of information, and position the digital identity ecosystem to realise the significant social and economic benefits digital identity services can provide. **This option could be established in the near term.** Phase one of the Trust Framework (2020-22), in which a small number of participants are informally linked to the Trust Framework, will allow for the testing of policies/processes and the mitigation of risks before the Trust Framework is established in legislation, giving it legal enforceability and enabling more participants into the trusted ecosystem. This phasing approach would also allow for the Trust Framework to be scaled and transformed in the future, if required. **This could be established at a reasonable cost.** Estimated costs to government approximately $1-2 million per annum. **As a result of these factors, option 3 is the Department's preferred option.**	**This would achieve the objective of a consistent and trusted digital identity ecosystem**. This option would almost certainly address the underlying deficiencies of the digital identity ecosystem and, unlike Option 3, it would be legally enforceable from the outset. **It would not be established in a timely manner.** It would take years to set up this regime, ensuring that the challenges in the digital identity ecosystem remain unaddressed for some time. **The costs associated with this option would be higher than any of the other options.** Estimated at $2-4 million per annum. **It is possible that the size and costs of this option might be unnecessarily out of proportion with demand, once the regime is finally implemented**. Undertaking such a comprehensive approach from the outset might lead to a situation where the costs of the regime outweigh the benefits. **While it may be suitable to move to a comprehensive regime like this in the future, the Department does not judge this to be the most suitable starting point for the Trust Framework.** The Department notes that option 3 has the potential to scale into a larger, more comprehensive regime like this is the future, if required.

Section 5: Conclusions

5.1 What option, or combination of options is likely to best address the problem, meet the policy objectives and deliver the highest net benefits?

We prefer Option 3 for the following reasons:

- It would bring consistency into the digital identity ecosystem in New Zealand, enabling a high trust environment for all participants.
- Unlike Option 4, which would also enable a high trust environment, it can be established in the near term and at a lower cost.
- It is sufficiently flexible and responsive enough to grow and develop into a larger and more complex model, if required.
- Government would maintain control over compliance process, ensuring consistency across the trusted digital identity ecosystem.
- RealMe, or parts of it, could be incorporated into the Trust Framework.
- Māori representation at the governance level will ensure Māori concerns and approaches to personal information (e.g. prioritising iwi affiliation over other attributes) are given appropriate consideration.
- It would meet stakeholder requirements. Evidence gathered through The Department's engagement process indicated stakeholders generally wanted a government-led intervention, that combined rules, compliance testing and legal enforceability, and could be established in a timely manner.

The digital identity ecosystem is not at a level of maturity to allow for Option 4.

Option 4 would involve the establishment of a larger and more complex Trust Framework regime than Option 3. Similar to Option 3, the Trust Framework would be overseen by a governance body and supported by an accreditation regime, and it would bring trust and consistency to the digital identity ecosystem. Additionally, Option 4 would allow for greater autonomy from government. It would still have clear lines of accountability and could react quickly to changes in industry standards.

However, it could not be established in a timely fashion. This option could not be operationalised until a new entity had been created and resourced to support it, and until such time as a new Trust Framework Bill had been introduced, all of which will take years. Furthermore, there is a realistic possibility that it may not be fit for purpose when it does come on line. The size and complexity of this option may be out of proportion with the market and requirements, especially as there will only likely be a small number of participants authorised to operate under the Trust Framework when it first comes online. As such, the cost of establishing a large and complex regime from the outset outweigh the benefits of such a regime. Approving Option 3 does not preclude the possibility to moving to an Option 4 model in the future, if the uptake and size of the ecosystem warrants such an approach. Option 3 is preferred over Option 4 as it enables responsive scalability.

Options 1 and 2 will not achieve the objective of bringing trust and consistency into the digital identity ecosystem in New Zealand.

Under Option 1, the digital identity ecosystem will continue to be afflicted by inefficiency and a lack of consumer control over their information. Legislation such as the Electronic Identity Verification (EIV) Act 2012 was designed to enable the sharing of government-held information to a restricted range of organisations to electronically verify an individual's identity.

Option 2 will make some improvements to the status quo. Amendments would be made to the Electronic Identity Verification (EIV) Act to remove some of the barriers that currently create challenges for individuals and organisations that wish to engage with RealMe. This would likely improve the flexibility and sustainability of RealMe services. The costs of amending the EIV Act are also likely to be relatively modest (indicative cost of $0.900 million over 3 years).

Options 1 and 2 will do relatively little bring consistency and trust to the wider digital identity ecosystem. They will do little to bring coherence to the application of privacy and security standards across both the public and private sectors, and will not address wider issues regarding the collection and use of people's information.

Implications for Māori

Under Options 1 and 2, Māori continue to have little control of their personal information. Options 3 and 4 provide opportunities for Māori to be in control of their data, its uses, its storage and its analysis.

The Department is confident that the evidence supports the policy proposal outlined above. Our option development was informed by extensive research and stakeholder engagement, including consultation with a wide range of international partners, all of whom were attempting to implement national-level responses to digital identity issues.

5.2 Summary table of costs and benefits of the preferred approach

Affected parties *(identify)*	**Comment***: nature of cost or benefit (eg, ongoing, one-off), evidence and assumption (eg, compliance rates), risks*	**Impact** *$m present value where appropriate, for monetised impacts; high, medium or low for non-monetised impacts*	**Evidence certainty** *(High, medium or low)*
Additional costs of proposed approach compared to taking no action			
Regulated parties	One-off cost which would cover application fee, initial compliance testing and, potentially, minor amendments to information systems (Note: this would be covered by government in phase one, but not phase two) Ongoing maintenance of compliance obligations. Entities that want to be accredited to participate in the trusted digital identity ecosystem are likely to fall into the following categories with the following costs: **Existing information systems that meet the Trust Framework criteria** **Existing information systems that do not meet the Trust Framework criteria** **New information systems built to meet Trust Framework criteria**	(Indicative) $10,000-$250,000 (the cost impact – i.e. is it high/medium/low - is subjective and, as such, is difficult to state definitively. It will be determined by factors such as the size of the participant and the maturity of the Trust Framework). (Indicative) between $0-100,000 per annum. (The cost impact – i.e. is it high/medium/low - is subjective and, as such, is difficult to state definitively. It will be determined by factors such as the size of the participant and the maturity of the Trust Framework). Low. No costs incurred. Costs incurred to remediate or update new system to meet the required standard. Low-high depending on the nature and functions of the software. Costs likely to be integrated into the project itself. Low-high depending on the project.	Officials have low confidence in the indicative figures (and their impact) as the true cost can only be established once the compliance process, the rules that govern it, and the ongoing accreditation obligations are finalised. The Department currently has no method by which to determine how many entities will be in each category, or if the costs will vary significantly depending on the nature of the participant (public sector versus private sector), or the role a participant plays in the ecosystem (e.g. information provider vs infrastructure provider). All of this will, however, be clarified during phase one of the Trust Framework (2020-2022).
Regulators	Establishing and maintaining the Trust Framework.	Medium. Current indicative cost of $1-2m per annum.	Low
Wider government	See Regulated Parties section above.	See Regulated Parties section above.	Low
Other parties	Accredited parties may choose to pass some of their costs onto their users.	Unknown.	Low
Total Monetised Cost	Dependent on how may parties choose to become accredited under the framework.	Unclear.	Low
Non-monetised costs	Dependent on how may parties choose to become accredited under the framework.	Unclear.	Low

Expected benefits of proposed approach compared to taking no action			
Regulated parties	Improved service delivery potentially resulting in an expanding customer base; improved ease of business; improved brand reputation; greater efficiencies (e.g. less duplication, process streamlining); reduced fraud resulting from improved risk assessment; increased confidence to invest in digital solutions; potentially new revenue streams; increased ability to meet regulatory requirements; greater confidence in the validity of personal and organisational information that is being supplied for the purpose of a transaction.	High Reducing incidences of fraud will lower the associated costs of fraud currently estimated at $13,627 per event with each victim having to spend on average 12 hours responding to their incident.	Low.
Regulators	Improved service delivery; greater inclusion; greater efficiencies (e.g. less duplication); improved record keeping, increased confidence to invest in digital solutions; increased opportunities to break down information silos between business units and government agencies.	High	Low
Wider government	Improved service delivery; greater inclusion; greater efficiencies (e.g. less duplication); improved record keeping, increased confidence to invest in digital solutions; increased opportunities to break down information silos between business units and government agencies.	High	Low
Other parties	People: Improved access to online services; improved customer experience; greater confidence that personal and organisational information is secure and private; greater control over personal and organisational information; greater transparency around where that information is stored and how it is used. Society: Greater interoperability between participants in the trusted digital identity ecosystem; clear and consistent rules for everybody wanting to participate in the trusted digital identity ecosystem, resulting in greater confidence in digital identity services; increased effectiveness in countering certain crimes; greater economic opportunities; improved facilitation of economic transactions, social interactions, and, potentially, political involvement.	High International studies have suggested that the potential benefit of enabling trusted digital identity in a mature economy is between 0.5% and 3% of GDP equivalent. If these figures are applied to New Zealand, the potential value is between $1.48 billion and $8.88 billion NZD (based on 2016 figures). The Department anticipates that the approximate value of digital identity to the New Zealand economy is up to $1.5 billion NZD of GDP equivalent per annum.	Low
Total Monetised Benefit		Difficult to estimate accurately but likely to be High	Low
Non-monetised benefits		High	Low. Digital identity trust frameworks are relatively new developments so there is not a lot of accurate and detailed international evidence around the benefits in this context to refer to.

5.3 What other risks/impacts is this approach likely to have?

POTENTIAL IMPACTS	EXAMPLES	POTENTIAL OUTCOMES	ASSUMPTIONS	MITIGATION MEASURES	ASESSMENT
Public misconceptions	The possibility that efforts to enable greater information sharing in the digital identity ecosystem result in a public misconception that information is at greater risk of exposure and/or misuse.	Discourages participation	People are especially concerned about the security of their information	Government assumes this risk. Such a scenario would be mitigated through the establishment of new legislation to govern the Trust Framework, a commitment to administer the Framework in an open and transparent fashion, public reports and possibly also through a public awareness campaign in the initial stages of the Trust Framework.	The mitigation measures will ensure this is a low probability risk.
Sharing information digitally remains challenging	Information could remain siloed because businesses and organisations do not choose to participate in the Trust Framework	The flow of information is impeded, and the potential benefits of digital identity are not realised	Business and organisations are enthusiastic for government intervention to address the issue of silos	Public sector and private sector service providers assume this risk. Officials are working closely with businesses and organisations to ensure their needs and requirements are met by the Trust Framework and encourage their participation.	This is considered a moderate risk. Business and organisations have expressed enthusiasm for government led intervention but the full costs, policies and processes of participating in a Framework have yet to be determined
Service delivery does little to improve customer experience	People may not actually use the digital identity services that are more secure and private, simply because others are more convenient.	Uptake remains low	People prioritise service delivery	Public sector and private sector service providers assume this risk. Service delivery remains the responsibility of service providers and not the Trust Framework, though bringing consistency and trust into the digital identity ecosystem will enable service providers to improve their delivery.	Unclear
Costs become excessive for government and/or private sector	The actual costs of compliance testing turns out to be significantly higher than the initial indicative costs. This would affect Government in phase one (2020-22) as government is covering the cost of this testing. In phase two (2022-25) the entity seeking accreditation, whether public or private, will likely assume this cost. The Trust Framework requires more resources than anticipated to set up and/or maintain, increasing overall costs for government.	Budgets are undermined Costs discourage participation in the Trust Framework	Reasonable costs will encourage participation	Government assumes the risk with regard to the cost of testing. In order to mitigate this risk, government will cover the cost of compliance testing during phase one of the Trust Framework (2020-2022) and work with partners to test and developed compliance processes in such a manner that compliance testing costs remain reasonable and appropriate going forward. The entity undergoing compliance testing assumes the cost of upgrading their systems. In the case of public sector entities, government can mitigate this through budget planning, however, private sector entities remain responsible for their own budgets.	The mitigation measures will ensure this is a low probability risk.

	Costs to upgrade systems to meet Trust Framework requirements are significantly higher than originally estimated, adding additional strain to the budget of the private or public sector entity seeking to join the Trust Framework.				
The Trust Framework does not enable Te Ao Māori approaches to identity	Māori do not participate equitably in the digital identity ecosystem. Māori perspectives and approach to identity are not enabled by the digital identity ecosystem. The digital identity ecosystem is not developed and maintained in partnership with Māori. Māori are not supported in leadership and decision-making roles to ensure Māori perspectives about data are embedded in the trusted digital identity ecosystem.	Undermines the government's commitments to digital inclusion Discourages Māori participation in digital identity and limits the potential benefits of digital identity for Māori communities	It is necessary to encourage Māori participation and better understand the opportunities for Māori in implementing the Trust Framework.	Government assumes the risk. To mitigate this the principles of the Trust Framework, which will be enshrined in the Trust Framework Bill, will include 'inclusion' and 'Enabling Te Ao Māori approaches to identity'. Additionally, there will also be a Te Ao Māori government representative on the governance board of the Trust Framework, with the ability to co-opt non-voting members and appoint an Advisory Board.	The mitigation measures will ensure this is a low probability risk.
Uptake remains low	Entities judge that there is little extra to be gained by becoming part of the Trust Framework and continue to operate independently of it. People decide that it is more convenient to use digital identity services operating outside the Trust Framework, even though they are less secure.	The potential benefits of the Trust Framework remain unrealised for everyone in society Ongoing government funding is committed to a regulatory framework which produces little value	People want a trusted digital identity ecosystem	Both government and private sector assume this risk. The government will mitigate this risk during phase one of the Trust Framework by testing processes and policies to ensure the Trust Framework is implemented in a fashion that meets the requirements and needs of all ecosystem participants.	This risk will remain a realistic possibility because, although government can implement a regulatory regime that accredits digital identity services, it remains dependent on individuals to choose to use those services instead of non-accredited ones.
Social inequalities creep in	The Trust Framework promotes growth in digital identity services, which has the unintended consequence of exacerbating the 'digital divide' and creates barriers for disadvantaged groups	Discourages participation Undermines the government's commitments to digital inclusion The potential benefits of the Trust Framework remain	People from all communities deserve the opportunity to participate in the digital identity ecosystem	Both government and private sector assume this risk. The government will mitigate this risk by ensuring the principle of inclusion (below) will be enshrined in the Trust Framework Bill as one of the guiding principles for the Trust Framework and trusted digital identity ecosystem. ***Inclusive*** *Everyone has the right to participate in the digital identity ecosystem.*	This risk will remain a realistic possibility. The Framework will not raise any regulatory barriers to inclusion but while it will set the standards that private sector entities will adhere to, it will be up to private sector entities to develop, invest in and offer digital identity services.

	(e.g. the elderly, refugees).	unrealised for everyone in society		*Key measures* • *The digital identity ecosystem can reflect the needs and requirements of a broad range of stakeholders.* • *Barriers to participation in the digital identity ecosystem−whether they be social, financial, or technical−are minimised, without compromising security or privacy.* • *Everyone is able to use digital identity services without risk of discrimination or exclusion.*	

Section 6: Implementation and operation

6.1 How will the new arrangements work in practice?

The preferred option would be formally given effect through the implementation of new legislation, which will establish the powers of the Trust Framework and its governance board.

It will take time to develop and pass legislation, yet there is an increasing imperative to implement some form of Trust Framework in the near future, especially as Covid-19 is accelerating digitalisation in all aspects of life.

As a result, The Department is proposing a two phase solution:

- Phase one: the implementation of an interim Trust Framework (2020-22). In this phase there is no legislation in place and the Framework is not legally enforceable.
- Phase two: the formal establishment of the Trust Framework (2022-25). In this phase, the Trust Framework is established in legislation and becomes legally enforceable.

This approach will allow the Department to meet the demand for a near-term solution to bring trust and consistency into the digital identity ecosystem, while also providing the space to develop the Trust Framework legislation, standards and accreditation process.

In phase one (2020-2022) a cross-agency governance board will be appointed by the Department, which will also establish a team to conduct compliance testing on digital identity solutions. The governance group will consist of representatives for the Government Chief Digital Officer, the Government Chief Information Security Officer, the Government Chief Data Steward, the Office of the Privacy Commissioner and a government Te Ao Māori representative. The board would also have the ability to co-opt non-voting members, and to appoint an advisory body comprised of government and non-government experts and stakeholders. Options for closer participation of non-government partners in the governance of the Trust Framework could be considered during the legislative process.

The team responsible for carrying out compliance testing would be established in the Department of Internal Affairs with the Government Chief Digital Officer. Organisations wishing to operate under the Trust Framework in phase one will do so in an informal manner in which they undertake compliance testing that will test their ability to adhere to best guidance recommendations, as there will be no legislation in place. Phase one will also present an opportunity to test operational policies and processes to ensure the Framework is appropriately positioned to bring more participants into the trusted ecosystem in the future in an efficient and effective manner.

While the compliance testing will help to provide the government with assurance in the near term, in the longer term legislation is preferred. Establishing the Trust Framework accreditation and governance bodies in legislation would give them legal enforceability thus engendering greater trust and participation, while also supporting sustainability. Additionally, establishing a new mechanism for both government and non-government agencies to provide digital identity services without new legislation could be viewed as running counter to the original intent of the Electronic Identity Verification (EIV) Act.

While the Department considered whether an independent Crown Entity could carry out the accreditation and governance, the preference was for keeping these functions within a government agency. This was because the rules for accreditation to an identity recognition system should be made and administered by the government, given that responsibility for any breach of security by a government agency would be the responsibility of the government.

6.2 What are the implementation risks?

RISK	EXAMPLES	POTENTIAL OUTCOMES	ASSUMPTIONS	MITIGATION MEASURES	ASSESSMENT
Excessive costs	The actual costs of compliance turn out to be significantly higher than the indicative costs The Trust Framework requires more resources than anticipated, increasing overall costs Costs to upgrade systems to meet Trust Framework requirements are significant	Undermines budgets Discourages participation	Reasonable costs will encourage participation	During phase one of the Trust Framework (2020-2022) the Department will work closely with a limited number of participants to pilot processes and policies, explore the potential risks and develop appropriate mitigation strategies before moving to the formal implementation of the Trust Framework in phase two (2022-25). This testing and transition will allow the Department to ensure costs remain reasonable and appropriate.	The mitigation measures will ensure this is a low probability risk.
It takes longer than initially anticipated to pass new legislation to govern the Trust Framework	Legislation for other industries takes on greater urgency in the post-Covid environment, delaying the Trust Framework Bill by a number of years	The powers and parameters of the Trust Framework are not formalised on schedule	Legislation will be necessary to formalise the Trust Framework and its parameters and powers in the long-term	In phase one of the Trust Framework the small number of entities participating will be doing so in an informal manner. This is not considered a long term solution, as the Trust framework will not be legally enforceable during this phase. This informal model is intended to be employed until such time as the Framework becomes formalised in legislation. It is highly likely that this informal relationship can be sustained for a term longer than originally anticipated if there are delays to the implementation of new legislation.	This risk is considered to be low probability, low impact.

.

Section 7: Monitoring, evaluation and review

7.1 How will the impact of the new arrangements be monitored?

The Minister for Government Digital Services will retain overall responsibility for the Trust Framework. In phase one of the Trust Framework (2020-2022), the Department will establish a cross-agency governance group that could include appropriate representation from the private sector and iwi in a non-voting capacity. Among other duties, that group will be responsible for monitoring the performance and effectiveness of all aspects of the Trust Framework and reporting back to the Minister for Government Digital Services on a six-monthly basis. In phase two (2022-2025), once the Trust Framework has become officially established through legislation, a governance board will be formally appointed through the standard Appointments and Honours process and will assume the aforementioned monitoring and reporting duties.

Reporting requirements will be formalised in the legislation as part of phase two of the Trust Framework (2022-2025), including which organisation will have responsibility for this (note - not necessarily the Department). The type of data that could be reported could include the number of parties accredited to the Trust Framework, the number of compliance assessments undertaken, the number of disputes that have arisen and how many have been resolved, privacy or security-related issues and their resolution, and the number of active participants in the Trust Framework. The Trust Framework legislation would also likely include a requirement that the governance board must review and report on any matter relating to the Trust Framework that is specified by the Minister in a written request.

7.2 When and how will the new arrangements be reviewed?

The Department will undertake a review of the Trust Framework and its governance arrangements at the conclusion of phase two (i.e. 2025) to assess progress against the Trust Framework’s priorities and – if required – recommend reform. The Department will also support the Minister’s office in assessing the governance board’s bi-annual reports, and recommending potential areas for review.