Regulatory Impact Statement: Detailed policy for a Digital Identity Trust Framework

Coversheet

Purpose	
Decision Sought:	Analysis produced for the purpose of informing final Cabinet decisions on the detailed policy for a Digital Identity Trust Framework
Advising Agencies:	Department of Internal Affairs
Proposing Ministers:	Minister for the Digital Economy and Communications
Date:	10 February 2021

Problem Definition

Trusted digital identity is a critical enabler of citizen and business participation in the digital economy and access to government services. It is a foundation for the economy and increasingly recognised as a global issue with increased connectivity emphasising the importance of privacy and security when sharing identity related information.

New Zealand lacks consistently applied standards and processes for sharing, storing and using personal and organisational information in a digital environment. As a result:

- people have limited control over their personal information and how it is used;
- the digital identity ecosystem is characterised by incoherence, ad-hoc regulation and lack of interoperability; and
- the way identity related information is shared is inefficient.

These core challenges create risks around the privacy and security of information and ultimately undermining trust and confidence in digital identity and the willingness of services and individuals to develop and use digital identity services. Consequently, the significant potential economic and social benefits of digital identity (estimated to be worth between 0.5% and 3% of GDP – at least $1.5 billion in NZ) are not being fully realised.

Cabinet has agreed to the establishment in legislation of a Trust Framework that will bring coherence to the standards and processes used by digital identity services across government and for any third parties wishing to engage with government on digital identity services. Detailed policy decisions are now required on key elements of that Trust Framework.

Executive Summary

Background

A Digital Identity Trust Framework (Trust Framework) is a policy and regulatory framework that sets and applies standards for security, privacy, identification

management and interoperability; and enforces the standards through accreditation of participants and governance of the rules.

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:

- people - for example, 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;
- businesses and organisations - for example, 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;
- Government – for example, 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; and
- society – for example, 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.

In July 2020, Cabinet agreed to address this problem via the implementation of a regulatory Trust Framework in order to ensure minimum standards are consistently applied across the digital identity ecosystem [CAB-20-MIN-0324 refers]. Cabinet agreed to:

- the establishment of a team, within the Department of Internal Affairs, responsible for developing the Trust Framework rules, and a transitionary governance group (consisting of representatives from public service agencies, the Office of the Privacy Commissioner and Māori) to approve the rules;
- the development of a Bill to establish the Trust Framework in legislation;
- the establishment of a representative Governance Board appointed by a Minister; and
- the establishment of a department-based team to undertake accreditation of potential Trust Framework participants.

Cabinet invited the Minister for Government Digital Services (now the Minister for the Digital Economy and Communications) to report back to the appropriate Cabinet Committee with a detailed policy paper to form the basis for drafting instructions for a Trust Framework Bill. Cabinet also noted that a cost recovery model will be developed as part of the policy and legislative programme for the statutory Trust Framework, and that advice on cost-recovery would be provided in the report back on the detailed policy.

As part of the detailed policy Cabinet paper, policy decisions are required on several Trust Framework components:

- the structure of the board responsible for governing the Trust Framework
- whether accreditation to the Trust Framework is optional or mandatory
- enforcement mechanisms
- disputes resolution; and
- cost recovery.

Governance Board structure

As the establishment of a Governance Board within a public service department in the Bill was already agreed (see previous RIS), the Department considered two main options:

- **Option 1**: A statutory officer – the Bill would establish a statutory officer (appointed by the Chief Executive) with the authority to update the rules of the Trust Framework and appoint advisors to assist their decision making.
- **Option 2**: A public service board (preferred option) – a board of 4-6 public service representatives (appointed by the Chief Executive) who would collectively decide on maintaining and updating the rules of the Trust Framework.

A public service board is the preferred option as it provides individuals with a wider range of skills and experience with decision-making rights. The creation of a Governance Board may increase costs for ecosystem participants (especially in the near term) but will provide an open and transparent mechanism for ensuring the Trust Framework that requires consultation on changes and amendments.

Optional or mandatory accreditation

While Cabinet has agreed to the establishment of a Trust Framework, it has not yet been explicitly asked to decide on whether joining the Trust Framework will be optional or whether it will be required for some or all participants. Options we considered include:

- **Option 1**: Optional (status quo and preferred option) - No requirement to seek accreditation to the Trust Framework for any participants.
- **Option 2**: Minister has authority to delegate sectors for whom compliance is compulsory – the Minister will have the authority to specify classes of information that may only be shared by accredited participants and organisations who may hold and share certain classes of information.
- **Option 3**: Mandatory – the Bill will specify which organisations must comply with the Trust Framework.

We consider that both the status quo and Option 2 are viable approaches. The status quo risks reduced uptake of Trust Framework privacy and security standards in the near term but is the most feasible approach and still provides the Government certain avenues for accelerating uptake (e.g. by requiring public service departments to become accredited) and offers the most flexibility to Trust Framework participants.

Enforcement mechanisms

Enforcement mechanisms will be used to remediate non-compliance with the Trust Framework's rules by an *accredited* party and discourage similar behaviour by other *accredited* parties. Options considered include low-impact mechanisms such as warnings and additional reporting requirements, as well as:

- **Option 1** – Suspension or revocation of a participant's Trust Framework accreditation.
- **Option 2** – the power to issue pecuniary fines of up to $10,000 for non-compliance with the Trust Framework.

These options are not mutually exclusive. Suspensions and revocations present practical issues as they will disrupt user's ability to access services and entitlements, however are still considered an important enforcement mechanism where people's privacy and security have been seriously compromised. Pecuniary fines are unlikely to offer a significant financial disincentive (especially for larger entities such as financial institutions) but will still offer a powerful reputational incentive. For these reasons the adoption of both options (in combination with the establishment with a dispute resolution regime and appropriate criminal penalties for defrauding the Accreditation Authority) is preferred.

Disputes resolution

For the Trust Framework to achieve its objectives, disputes will need to be resolved efficiently and effectively and in a timely manner. Options considered for dispute resolution include:

- **Option 1:** do nothing - no formal dispute resolution process
- **Option 2:** a formalised voluntary scheme
- **Option 3:** a requirement for ADR established in legislation
- **Option 4:** a dedicated Disputes Tribunal established in legislation.

Option Three offers quick and cost-effective opportunities for dispute resolution, will allow for flexible solutions, and ensure a level playing field for all participants.

Cost recovery

In July 2020, Cabinet noted that a cost recovery model will be developed as part of the policy and legislative programme for the statutory Trust Framework [CAB-20-MIN-0324 refers]. s9(2)(f)(iv) The Trust Framework rules and accreditation processes will need to be finalised before we can determine what kind of cost recovery model should be established. A draft version of the rules is anticipated to be developed by August 2021. Potential options for cost recovery include:

- **Option 1**: a fixed charges regime – all applicants are charged a flat rate for the costs of accreditation, governance and enforcement.

- **Option 2** (preferred option): a variable charges regime (based on hours and resources required for accreditation).
- **Option 3**: a levy on participants to fund the Trust Framework.

- The costs of accreditation are likely to vary considerably depending on the systems and processes of each applicant. Therefore, a fixed charges regime is likely to result in significant cross-subsidisation and is not preferred. A levy regime could best reflect the ability of participants to pay and the wider public and club good aspects of the Trust Framework – however, difficulties and costs around ensuring compliance make it unfeasible. A variable charges regime will effectively ensure that costs reflect the complexity of the accreditation process.

Limitations or Constraints on Analysis

A key constraint on this analysis is the July 2020 Cabinet decision to establish a Trust Framework in legislation that includes governance, accreditation and enforcement mechanisms (see above).

While officials have undertaken targeted engagement with sector stakeholders and research bodies to gather a robust body of evidence, the Department has not publicly consulted on the detailed policy proposals considered in this paper.

To mitigate the risks around the lack of public consultation, the Department intends to seek Cabinet authority to release an exposure draft of the Bill. The release of the exposure draft will not seek feedback on whether the policy proposals considered in this RIS should be reviewed or changed. Rather, it will provide the public with the opportunity to comment on whether the Bill gives appropriate effect to these policy proposals (e.g. whether the Authority's enforcement powers regime achieves the objective of ensuring compliance with the Trust Framework). The exposure draft will also include explanatory material setting out how non-compliance may be addressed through existing laws and rules in the wider legislative framework around information sharing.

s9(2)(f)(iv) [redacted] This timeframe was developed in response to several drivers that mean establishing a Trust Framework is a high priority (to ensure appropriate regulation as the ecosystem is developed and avoid any adverse consequences): to enable digital transformation across the public sector and improve access to essential services and entitlements during the ongoing COVID-19 pandemic.

The Bill and the Trust Framework's rules are in the process of being developed concurrently (as part of the Department of Internal Affairs' Rules Development Programme). The Rules and the accreditation process have yet to be tested with potential participants.

Consequently, there is limited evidence on some of the policy proposals discussed in this paper, including the likely cost of accreditation and the potential demand for dispute

resolution services. In the near term, the Department has identified 18 potential Trust Framework participants who are working with the Rules Development Programme.

Demand for accreditation in the medium term remains uncertain, though targeted engagement with public and private sector participants (including representatives from ANZ, ASB, Auckland University, MATTR, Payments NZ, Planit, Sphere Identity, SSS IT Experts, Two Black Labs, Westpac and Xero) indicated strong support for the establishment of a Trust Framework. Until the costs of accreditation are better understood and tested with potential applicants, the likely longer-term take-up of accreditation will remain uncertain.

As the interim Trust Framework is being developed simultaneously, we also have limited understanding of likely take-up. Where possible the Department has relied on evidence from similar regimes and in foreign jurisdictions (including the cost of accreditation to Australia's Trusted Digital Identity Framework).

Responsible Manager(s) (completed by relevant manager)
Sela Finau *Policy Manager* *Policy Regulation and Communities* *Department of Internal Affairs*

Quality Assurance (completed by QA panel)	
Reviewing Agency/Agencies:	Department of Internal Affairs Quality Assurance Panel
Panel Assessment & Comment:	The panel considers that the information and analysis summarised in the RIA partially meets the quality assurance criteria. There is uncertainty about the costs and benefits of the proposal and gaps in the evidence, including the likely uptake of the Trust Framework, some of which results from the lack of full consultation on the specific proposals. However, the analysis shows a good understanding of these limitations, makes appropriate use of available evidence and includes suitable measures to rectify the issues. The RIS provides a balanced view of the advantages and disadvantages of the options and is a sound basis for further work to develop the detailed framework.

Section 1: Outlining the problem

Context/Background Information

What is digital identity?

Digital identity is the user-consented sharing of personal and organisational information online to access services and complete transactions. This sharing of information allows people to assert their personal attributes, such as their income, qualifications, date of birth, or proof of eligibility, online, in order to access services and entitlements. Digital identity services rely on relationships between individuals and service providers, as part of a 'digital identity ecosystem' that includes:

- **users** who are subject to and initiate their own transactions within the ecosystem;
- **information providers** who supply personal and organisational information they hold (e.g. government, banks, utilities, individuals etc.);
- **infrastructure providers** who enable people to disclose their information and consent to share it using a digital platform (e.g. RealMe); and
- **relying parties** who use the trusted personal and organisational information supplied by infrastructure providers to provide services (e.g. banks, government, telecommunications, health providers, and providers of age restricted services such as liquor stores).

Currently the main way people can assert their identity online is through the government provided RealMe service. RealMe is a centralised model of digital identity, which has been Crown funded since its inception. The number of people with a RealMe verified identity has been significantly boosted by initiatives such as Passport co-apply and Studylink. Currently there are over 750,000 verified identities.

Since RealMe was introduced, the digital identity environment has changed significantly. Globally and in New Zealand there has been an emergence of digital identity service providers, which are developing decentralised approaches that allow the customer/citizen to have greater control of their information. Major digital identity infrastructure providers in New Zealand include IBM New Zealand Ltd, Microsoft NZ and InternetNZ, while information providers include a wide range of institutions including ANZ and Auckland Transport.

Cabinet has decided to establish a Digital Identity Trust Framework

Because of this, in July 2020 Cabinet agreed to address this problem via the implementation of a regulatory framework to ensure information and infrastructure providers consistently apply minimum standards across the digital identity ecosystem (at this point it is not considered necessary for relying parties to also be accredited) [CAB-20-MIN-0324 refers]. Cabinet agreed to 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;
- representative governance board appointed by a Minister; and
- department-based team to undertake accreditation of potential Trust Framework participants.

A Trust Framework is a policy and regulatory framework that sets and applies standards for security, privacy, identification management and interoperability; and enforces the standards

through accreditation of participants and governance of the rules. For further details on the Trust Framework, the digital identity ecosystem and its participants, please see the July RIS (*Progressing Digital Identity: Establishing a Trust Framework*).

Cabinet did not explicitly consider the issue of whether the Trust Framework would be mandatory for some or all ecosystem participants.

Cabinet also agreed that the Minister for Government Digital Services (now the Minister for the Digital Economy and Communications) will report back to Cabinet with a detailed policy paper to form the basis for drafting instructions for a Trust Framework Bill. Given the significance of the proposals to be considered, including the creation of new criminal penalties and a cost recovery regime the Treasury's Regulatory Quality Team advised that a new RIS would be required to support the detailed policy paper.

The development of the Trust Framework has linkages with several ongoing government work programmes. These include the GCDO's digital inclusion workstream, the development of new data and statistics legislation by Stats NZ and consideration of establishing a consumer data right.

To ensure the integrity of the Trust Framework, disputes between Trust Framework participants and between Trust Framework participants and users need to be resolved efficiently and effectively and in a timely manner. This is because prolonged disputes are costly, create uncertainty among participants and in the case of potential non-compliance could result in uncertainty and continued consumer harm .

What is the policy problem or opportunity?

Digital identity has historically been impeded by trust, privacy and security issues

New Zealand lacks consistently applied standards and processes for sharing, storing and using 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.

Our understanding of these issues has been informed by significant stakeholder engagement. This included research and surveys undertaken during 2019 and 2020 with a diverse range of private individuals, including Māori, Pacific people, older New Zealanders and people with disabilities. Qualitative research has included interviews and focus groups to gauge public opinion and Māori perspectives on digital identity. Quantitative research has used surveys to reach over 2,000 people and test their understanding of digital identity and associated issues.

Focus group research shows Māori have lower levels of trust than other groups over government holding and sharing information about them. Participants in the focus groups attributed this distrust to the misuse and abuse of Māori data, creating biased assumptions of Māori and a narrative not informed by Māori. "Nothing's ever safe, nothing's ever private" was the consensus among Māori focus group participants concerning the status of their shared information, data, and activities.

In one survey, almost a quarter of those who had used government services stated that they had personal information leaked, hacked or used without permission. The inconsistent application of data, privacy, identification and security standards has been identified as a contributing factor to these breaches. This poses risks to both customers and businesses, undermining trust and confidence in the digital identity ecosystem further and slowing adoption.

Research with sector stakeholders also tells us that trust depends on the perceived motivations of the organisation they're dealing with, and the context. Context factors for building trust includes the type of organisation that is requesting the information, what information is requested and the brand reputation for that company. Commercial enterprises were also seen to focus on their own interests and more likely to contravene rules. Therefore, people would be reluctant to see them have access to personal information held by government without appropriate reassurances and controls in place.

While RealMe seeks to address some of these issues by providing an all-of-government digital identity service that provides a high degree of trust and security, the regulatory requirements of the Electronic Identity Verification Act 2012 (including that all participating entities be approved by Cabinet) has stymied uptake.

However, digital identity has the potential to deliver significant benefits to a wide variety of stakeholders

A Digital Identity Trust Framework (Trust Framework) will bring consistency, trust, structure and efficiency to the digital identity ecosystem. This will produce a wide range of benefits for:

- people – for example, improved access to online services; improved customer experience; greater confidence that personal and organisational information is secure and private; greater control over personal information; reduced risk and reduced identification fraud;
- businesses and organisations – for example, 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;
- Government – for example, 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; and
- society – for example, 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.

By establishing legally enforceable standards for its participants, the Trust Framework will bring coherence to digital identity services across government and for any third parties wishing to engage with government on digital identity services. This will enable multiple parties to participate in a safe and trusted way.

Digital identity can also enable digital trade and other cross-border transactions. The development of the digital identity ecosystem and interoperability will enable New Zealand to advance discussions on digital identity in a variety of different jurisdictions. One example is the New Zealand and Australian Prime Ministers' commitment to mutual recognition of identity services between Australia and New Zealand. There is also potential for ongoing alignment with Canada and the United Kingdom with each of these countries developing their own Trust Frameworks.

A private sector response that would address the 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

Officials have worked with sector stakeholders and research bodies to gather a robust body of evidence to inform, develop and test proposals. This includes regular engagement with over 100 organisations (including public agencies, Crown agents and entities,[1] private digital service providers,[2] financial institutions[3] and academic institutions, such as the University of Auckland and the University of Otago). There is wide support in both the public and private sectors to ensure that digital identity services are trusted, coherent and sustainable.

Detailed policy decisions are required on several issues in order to ensure that the Trust Framework

In order to achieve these benefits and to give effect to Cabinet's decision to establish a regulatory Trust Framework, policy decisions are required on several of its components, including:

- the structure of the **Governance Board**;
- assessing whether accreditation to the Trust Framework should be **optional or mandatory**;
- establishing **enforcement mechanisms** to allow the Accreditation Authority to address non-compliance (including criminal offences);
- establishing a **disputes resolution process** to ensure an efficient and effective process for resolving disputes; and
- establishing **penalties** to protect the integrity of the accreditation regime and to enforce compliance with the Trust Framework.

How to structure the governance of the Trust Framework

As noted above, Cabinet has agreed to the establishment of a representative governance board appointed by the Minister of the host department. However, the Public Service Commission subsequently advised officials that under the Public Service Act 2020, if a Board is established within a public service department it must be appointed by the Chief Executive of that Department. Cabinet approval for a revised proposal whereby the Board is appointed by the Chief Executive will be sought from Cabinet along with the other detailed policy proposals discussed in this RIS. The purpose of the Governance Board will be:

- to monitor the performance and effectiveness of all aspects of the Trust Framework; and
- to update and amend the Trust Framework as required to ensure its fitness for purpose and ongoing alignment with the purpose and principles of the Bill.

---

[1] Including the Ministries of Business, Innovation and Employment, Social Development, Health, and Education, the National Cyber Security Centre, Treasury, Inland Revenue, Stats NZ, the Office of the Privacy Commissioner and ACC.

[2] Including MATTR, SSS online security consultants, Planit software testing, Middleware Solutions, SavvyKiwi, Sphere Identity and Xero.

[3] Including Westpac, ASB, KiwiBank, ANZ, BNZ, Payments NZ and PartPay.

In carrying out this purpose, the Bill will establish that the Board has a variety of functions, including:

- maintaining and updating the Trust Framework's rules;
- providing procedures for the lodging of formal complaints;
- undertaking education and the publication of guidance; and
- any other responsibilities that may be conferred on it by the Minister.

In establishing the Governance Board, it will be important to ensure that it is as representative of the wide variety of stakeholder interests in the digital identity ecosystem as possible. However, it will be important to balance this goal with the fact that the Governance Board will be responsible for establishing rules regarding the use of trusted government information sources. This information relates to core functions of the state (e.g. immigration, passports etc.) and the effective guardianship of this information is essential to retaining public trust.

The issue of representation is especially significant given the concerns expressed by Te Ao Māori in focus groups about the security and use of their information. Given Māori are Treaty partners, there is a pressing need for the Governance Board to establish an enduring relationship with Māori and to work in partnership in the development of the Trust Framework.

Officials are actively building the capability required to enable effective partnership with Māori. To help achieve this in the near term, the interim Governance Board responsible for approving the Trust Framework rules will include Te Pou Matihiko for Digital Public Services to ensure that the rules reflect Te Ao Māori perspectives. To further address issues of inclusion and to ensure that a partnership approach is taken where appropriate, the Bill will also require that the Board be required to seek the views of Treaty partners.

Whether accreditation is optional or mandatory

In 2020, Cabinet agreed that the statutory Trust Framework would include the establishment of a department-based team to undertake accreditation of potential Trust Framework participants (the Accreditation Authority). The purpose of the Accreditation Authority (the Authority) is to assume responsibility for the accreditation process, including ongoing compliance testing. The Bill will allow the Minister to establish the Authority inside a public service department. The Authority will be appointed by the Chief Executive of the nominated department and be accountable to the Minister.

The success of the Trust Framework will be largely dependent on the extent to which the different sectors of the digital identity ecosystem participate in it. The wider the adoption of the Trust Framework's rules and standards, the greater the improvements in user privacy and security and the greater the opportunities for innovation in service delivery. A range of public and private entities have already expressed an interest in participating in the Trust Framework.

However overall demand for participation to the Trust Framework remains uncertain, particularly given the significant costs of becoming accredited (initially estimated at between $10,000 and $250,000 including the costs of obtaining independent pre-accreditation

documents)[4]. This impact statement will therefore review whether accreditation to the Trust Framework should be optional or mandatory for some or all sector participants.

Enforcement mechanisms

Those who are accredited to participate in the Trust Framework will need to comply with Trust Framework rules. Enforcing that *compliance* will be essential to ensuring the *digital identity ecosystem* remains functional, trustworthy and sustainable. Implementing legal enforceability will help instil trust in the framework by ensuring there are mechanisms in place to ensure *accredited* participants follow the rules. Without such mechanisms, it is possible that *accredited* parties would not feel obliged to comply with regulations and standards, leading to a situation where the public's trust and confidence in their products, systems and services would be undermined.

Disputes Resolution

For the Trust Framework to achieve its objectives, disputes will need to be resolved efficiently and effectively and in a timely manner. This is because prolonged disputes are costly, create uncertainty among participants and in the case of potential noncompliance could result in consumer harm continuing and uncertainty.

The proposed regulatory regime should include alternative dispute resolution processes to ensure users and participants can resolve disputes about their roles and activities under the Trust Framework expediently and at a low cost. This will ensure that actors under the Trust Framework are not disincentivised from participation by the threat of expensive and time-consuming litigation. This view was supported by public and private stakeholders such as the Ministry of Health, ACC and ANZ Bank when the need for disputes resolution was consulted on during 2019.

Cost-recovery

Currently the accreditation process is still being developed in conjunction with the rules for the Trust Framework. As a result, this RIS is not intended to consider detailed costing options for accreditation. It instead seeks to identity which model for recovering costs is most appropriate for an accreditation regime (e.g. fixed cost recovery, variable cost recovery or a levy regime). The Department will prepare a separate Cost Recovery Impact Statement once the accreditation process has been developed and likely costs have been identified.

Initial estimates have indicated that accreditation to the Trust Framework will require between 70 and 300 work hours, including the costs of assessing privacy, security and administrative approaches and is estimated to cost the Authority between $10,000 and $40,000. Initially there is anticipated to be enough demand to justify an Accreditation

[4] This variance in cost is largely dependent on the complexity of the digital identity solution being proposed, and the corresponding amount of work hours that is required test the adequacy of security, privacy and operational protocols needed to ensure the effective management of information (see discussion of cost-recovery below). These costs are based on the costs of accreditation to Australia's Trusted Digital Identity Framework, and are considered preliminary, as testing of New Zealand's accreditation process is ongoing as part of the Rules Development Programme.

Authority staffed by 5 full time equivalent accreditors. As part of the Rules Development Progamme, officials are already working with a group of 18 digital identity service and information providers who have expressed interest in accreditation. Throughout the rules development programme (including consultation on the rules and the proposed accreditation process) the Department will assess the ongoing demand for accreditation services and the resourcing requirements to meet this demand.

Accreditation to the Trust Framework offers a clear private and commercial benefit to participants (as outlined above). This will potentially include the ability of private sector providers to utilise trusted government information sources for the provision of digital services. It is also easily possible to exclude entities from participation through refusing accreditation if the standards are not met (or revoking accreditation in the case of non-compliance). For the Trust Framework to function effectively, the accreditation regime will require a funding model that equitably attributes costs between participants and incentivise accreditation. It is not intended that any cost-recovery regime for accreditation would apply to public service entities due to the inefficiencies of government charging government.

However, The Trust Framework itself has many aspects that make it like a club good or even a public good. Use of the Trust Framework is non-rivalrous (one entity's use of the Trust Framework's rules does not diminish another's). And while it is possible to exclude entities from accessing the Trust Framework rules, there are strong policy reasons for making them publicly available.

Wider accreditation of digital identity services will result in the more rapid adoption of essential security standards and will provide users with greater control over their personal information. It will also lead to the wider adoption of interoperable standards, helping to improve productivity and consumer choice through the development of innovative and integrated services. Finally, wide-scale accreditation under the Trust Framework will help to support the resilience of New Zealand communities through the removal of current barriers to the access of goods and services digitally.

The World Bank has stated that identification should be treated as a public good, provided to facilitate the rights and inclusion of individuals and to improve administration and service delivery. A Trust Framework is critical infrastructure for the delivery of this public good and will confer benefits to a wide range of system participants.

On this basis, there is an argument that the components of the Bill related to the development, maintenance and enforcement of the Trust Framework itself should be funded through general taxation rather than accreditation fees. s9(2)(f)(iv) [redacted] Any bids for Crown funding to support funding of the Trust Framework will be considered in the context of, and be contingent on, New Zealand's fiscal environment at that time.

What objectives are you seeking in relation to this policy problem or opportunity?

The objectives for the development of the Trust Framework are for:

- people to have easier access to a wider variety of online services (including interoperable services between multiple infrastructure and information providers) and increased confidence that their personal information is protected, leading to reduced risks of harm and greater use of digital services;
- organisations to have the ability to trust that people are who they say they are online and meet requirements to access their services;
- organisations to be able to develop new digital services that easily connect with users' information and that meet compliance requirements;
- digitally enabled mutual recognition to support international trade and interoperability through clear rules and standards;
- people and organisations provided with choice and scale, which fit the way they transact online today and in the future that reflect social and cultural differences; and
- government to be able to deliver improved and efficient public services in tandem with our international partners and be able to better detect and deter security or privacy breaches of personal and organisational information.

Section 2: Option identification and impact analysis

What criteria will be used to evaluate options against the status quo?

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).

When considering which options to support, more weight is assigned to options that effectively ensure trust and can be feasibly implemented.

For the consideration of cost-recovery options, the criteria of Trust is less relevant. It is therefore replaced with the objective of equity. This criterion includes:

1. Equity with respect to the amount each participant pays relative to their contribution to costs;
2. Equity in terms of amount paid relative to the standard of service received; and
3. Equity in terms of ability to pay.

For policy options that will be further developed by way of regulations (e.g. the disputes resolution scheme) other criteria may be applied in future (e.g. the Government Centre for Dispute Resolution's best practice principals for dispute resolution).

There is limited quantitative evidence to support the analysis as work on the costs and demand for accreditation is ongoing as part of the Department's Rules development programme. However, this RIS has been supplemented by evidence provided by stakeholders, what happens in similar regulatory regimes, overseas jurisdiction and how digital identity services are provided now.

What scope are you considering options within?

The July 2020 Cabinet agreement limits the scope of interventions in the digital identity ecosystem to those consistent with a Bill that will establish a Trust Framework and its key components [CAB-20-MIN-0324 refers]. Non-regulatory options were previously considered for the establishment of a Trust Framework (e.g. by publishing best practice standards rather than implementing an enforceable regime – see previous RIS).

Governance Board

Cabinet agreed that the Trust Framework Bill would establish of a representative governance board appointed by the Chief Executive. The previous RIS considered options for establishing a Governance Board outside the public service in a Crown Entity, but this option was discarded as it would place control of trusted government data sources outside of the public service and would be more expensive and take longer to establish. This option is not revisited in the current RIS.[5]

Opt-in or mandatory accreditation

Cabinet agreement has not been explicitly sought on the issue of whether compliance with the Trust Framework will be opt-in or mandatory. In Australia, under an opt-in Trust Framework (the Trusted Digital Identity Framework – the TDIF) demand for accreditation has increased significantly along with awareness of the potential benefits. In the past week, the Digital Transformation Agency has approved applications for accreditation and is working with several organisations helping them to undergo self-assessment against the TDIF's rules. Additionally, most state governments are also mapping their digital identity policies to the TDIF and are looking at accreditation pathways.

Enforcement

Cabinet has not made decisions on what enforcement mechanisms will be available under the Trust Framework Bill. The development of the options for enforcement have been informed by the review of a variety of sources, including existing statutory licensing regimes (such as the Immigration Advisers Licensing Act 2012 and the Lawyers and Conveyancers Act 2011). Officials have also reviewed the approaches taken to the establishment of digital identity frameworks (both government lead and private) in other jurisdictions including Australia, the UK and Canada.

We are seeking Cabinet agreement to allow for the Board to submit regulations regarding an offences and penalties regime (along with an infringement offences regime), to be enforced via the Accreditation Authority, and to the maximum fees for those offences. The Department is also seeking Cabinet agreement to the establishment of enforcement mechanisms for non-compliance with the Trust Framework (including potential warnings, additional reporting requirements and potential to power to issue pecuniary fines for non-compliance and suspend or revoke accreditation).

---

[5] See sections 4 and 5 of the *Progressing Digital Identity: Establishing a Trust Framework* RIS.

Disputes resolution

Decisions have not yet been made by Cabinet on the implementation of a disputes resolution scheme. The purpose of dispute resolution processes under the Trust Framework will be to enable the resolution of disputes between accredited participants and between users and participants.

We are seeking Cabinet agreement to establish a disputes resolution process to help resolve disputes between Trust Framework participants efficiently and effectively. As this is a new area of regulation there is no data on the possible number of and nature of disputes among participants – however, disputes are inevitable and stakeholders with insights into the digital identity trust ecosystem were highly supportive of the Trust Framework including a process to effectively manage disputes.

We anticipate disputes could relate to:

- dishonesty or misleading behaviour/information
- negligence
- service outage/failure.

There are existing avenues that can be used for complaints concerning privacy or criminality (fraud) - for example, through the Privacy Commissioner or the Courts. Dispute resolution under the Trust Framework Bill will not duplicate these avenues.

With regards to disputes between participants we anticipate that the likely parties will be medium to large organisations, including:

- information providers (supply info they hold);
- infrastructure providers (Info sharing tools, credential providers, attribute management;
- Authenticator and Authentication providers; and
- Other service providers (that need to have record management and authentication management).

Demand for disputes resolution is likely to be small (at least until participation in the Trust Framework grows). It is unlikely, assuming the accreditation process is effective, that there will be many large-scale disputes between participants, or between participants and users. A key design consideration going forward will be to ensure accessibility for all participants and users.

The establishment of a tribunal for consideration of Trust Framework disputes was considered. This option was discounted because the costs are likely to outweigh the benefits and the demand for dispute services is likely to be relatively low in the short to medium term.

Cost recovery

Cabinet has not made formal decisions on the establishment of a cost-recovery regime but has noted that a cost-recovery model will be developed as part of the policy and legislative programme for the statutory Trust Framework. The consideration of options for cost recovery has been informed by guidance issued by the Treasury and the Office of the Auditor General.

s9(2)(f)(iv) [redacted]

Describe and analyse the options

The purpose of the Bill is to address the challenges with the status quo by introducing a set of minimum requirements for participation in the digital identity ecosystem that can be monitored and legally enforced.

To help achieve this, we are proposing to seek Cabinet agreement to issue drafting instructions for the Bill to enact a series of detailed policy proposals, including:

- the structure of the **Governance Board**;
- assessing whether accreditation to the Trust Framework should be **opt-in or mandatory**;
- establishing **enforcement mechanisms** that allow the Accreditation Authority to protect the integrity of the Trust Framework and to address non-compliance with its rules;
- establishing a **dispute resolution** regime; and
- establishing **penalties** to protect the integrity of the accreditation regime and to enforce compliance with the Trust Framework.

Time constraints have meant that a full consultation process has not been carried out on the following policy proposals. However, options for governance, enforcement mechanisms, a dispute resolution mechanism and a cost-recovery regime have been discussed as part of extensive targeted stakeholder engagement.

Establishment of a Governance Board

The technologies and standards underpinning digital identity will continue to evolve in the future and the rules of the Trust Framework will need to evolve with them. In this context, the purpose of the Board will be:

- to monitor the performance and effectiveness of all aspects of the Trust Framework; and
- to update and amend the Trust Framework as required to ensure its fitness for purpose and ongoing alignment with the purpose and principles of the Bill.

In carrying out this purpose, the Bill will establish that the Board has a variety of functions, including:

- administering the Trust Framework's rules;
- providing procedures for the lodging of formal complaints;
- undertaking education and the publication of guidance; and
- any other responsibilities that may be conferred on it by the Minister.

Option One – a non-regulatory Governance board (Counterfactual)

If the Governance Board were not established in the Bill, then a cross-agency governance group would likely be made responsible for maintaining and updating the rules.

Option Two – a statutory officer

A statutory officer could establish a representative panel to advise its decision-making and would be incentivised to consider stakeholder perspectives. However, making the governing body a statutory officer could be perceived as inconsistent with the Trust Framework principles of inclusivity, sustainability and enabling of Te Ao Māori approaches to identity. Consulted agencies (including Te Arawhiti) have already expressed concerns about the representation of Te Ao Māori in the governance of the Trust Framework in particular. For this reason, it is not supported. Despite this, the Public Service Commission recommended that this option be considered, given the simplicity of establishing a statutory officer in legislation and the use of statutory officers in other statutory licensing and registration regimes (e.g. the Valuer-General under the Rating Valuations Act 1998).

Option Three – a public service board

Option Three would allow for collective decision-making rights, whilst establishing the body within a Department. Under this option the generic provisions governing the public service would apply. The chief executive of the department would be responsible for making appointments to the Board (in line with the requirements under section 54 of the Public Service Act 2020) and the host department would be responsible for administering appropriations.

This option requires all voting members of the body to be employees of the public service (likely members of the Board would include representatives from the Government Chief Digital Officer, the Government Chief Information Security Officer and the Government Chief Data Steward). This would leave no place for direct representation from Crown entities (such as the Office of the Privacy Commissioner), Māori representatives or the private sector. It is still possible that the views of these sectors could be supported by appropriate appointments from within the public sector.

Even so, there is a risk that a board comprised of public service representatives may be perceived as being non-inclusive, unable to effectively assess the sustainability of the Trust Framework and unable to support Te Ao Māori approaches to identity. In order to mitigate this risk, the Minister would have the authority to direct the Board to have regard to the views of Treaty partners, the Office of the Privacy Commissioner and others (including private sector interests). The Bill will establish that the Chief Executive must also ensure that the Board has appropriate knowledge and expertise in technology, identity management, privacy, security and Te Ao Māori interests and participation. The Board would also have the power to appoint committees to advise the Board on matters relating to its functions and will be subject to the Trust Framework's principles.

Multi-Criteria Analysis

	Option One – Status Quo / Counterfactual	Option Two – Statutory Officer	Option Three – Public Service Board
Principles	0 Supports an inclusive approach to digital identity that incorporates non-public service representatives in governance and considers Te Ao Māori approaches to digital identity but lacks in openness and transparency. The options for governance have little variance in terms of supporting privacy, security and interoperability.	- Not inclusive as no one person can represent the wide range of stakeholders in the Trust Framework (though may be supported by advisory panels). May negatively affect public perceptions of its ability to enable Te Ao Māori approaches to digital identity and hence may affect the Trust Framework's sustainability over time.	0 Less inclusive but Minister able to direct the board to consider specific interests. The Bill will also ensure the Board is open and transparent in its actions, will include officials (and potentially non-voting members) with a focus on Te Ao Māori approaches to digital identity, supporting greater public trust and the sustainability of the Trust Framework.
Trust	0 No clear mechanisms for appointments, reporting requirements and the establishment of its purpose may negatively affect trust in the rules.	- Likely to enjoy less trust, though will be accountable to the Chief Executive and the Minister for their decision making.	++ Clear mechanisms for appointments, reporting requirements and the establishment of its purpose. Will retain control of the Trust Framework within the legal Crown.
Feasibility	0 Low cost, is already being implemented as part of the rules development programme, but may generate less value for ecosystems participants and users as there is no accreditation regime to ensure compliance or	0 Low cost but will require significant support function from within the Department. The lack of wider representation may disincentivise participation, though this could potentially be mitigated by the appointment of	0 Similar cost to status quo, though legislation will require certain expenses that were optional (but desirable) under the status quo (e.g. consultation on appointments, annual reporting requirements). Wider range of members of different experience and expertise will help

	formal consultation processes to ensure that views of the wider sector are considered in the administration of the rules	advisory sub-committees to support decision making.	to ensure administration of the rules in a way that creates greater value for participants and thereby encourages greater participation.
Flexibility	0 Can be adapted over time in response to the needs of system participants	- Less able to capture changing trends in the needs and requirements of the wide range of sector stakeholders.	- Unable to appoint non-public service members, though the legislation will require the board to have regard to these views.
Overall assessment	0 This option is highly flexible and is already being implemented, however lacks mechanisms to instil openness and transparency in the governance of the Trust Framework.	- While feasible, the appointment of one individual to be responsible for the Trust Framework would not be perceived as compliant with the principles of inclusivity, people-centred and enabling Te Ao Māori approaches, and could negatively impact Trust and be perceived as insufficiently responsive to the needs of participants.	+ Retains control of the Trust Framework within the legal Crown and provides strong mechanisms for ensuring a

Conclusions

The establishment of a Public Service Board, to sit within the Department and appointed by its Chief Executive is the Department's preferred option. This will provide a wider range of experts with responsibility for maintaining and updating the Trust Framework, supporting Trust and best meeting the principles of inclusivity, people-centredness and openness.

Summarise the costs and benefits of your preferred option

Affected groups *(identify)*	**Comment**: nature of cost or benefit (e.g. ongoing, one-off), evidence and assumption (e.g. compliance rates), risks	**Impact** *$m present value where appropriate, for monetised impacts; high, medium or low for non-monetised impacts*
Additional costs of the preferred option compared to taking no action		
Regulated groups	Cost of funding a Governance Board.	s9(2)(f)(iv) [redacted]
Regulators	None directly (government won't be subject to accreditation and other fees as Treasury guidelines recommend generally avoiding this due to the inefficiency of government charging government. However, costs of public service share of the Board's activities will still need to be funded centrally).	Low
Other groups (e.g. wider government, users etc.)	Cost of Governance Board may be passed on to users through higher user fees if funded directly for digital identity services by accredited Trust Framework participants s9(2)(f)(iv) [redacted] May affect uptake, though the relative cost of governance per participant	Uncertain, depends on level of accreditation to the Trust Framework and the size of participating agencies (e.g. large financial institutions will be better able to wear any governance costs).

	will shrink as the number of accredited participants grow.	
Total monetised costs		s9(2)(f)(iv)
Non-monetised costs		*Low*
Additional benefits of the preferred option compared to taking no action		
Regulated groups	Provides official channels between the Governance Board and the Minister that allows the board's decision making to be held to account. The Governance Board will be required to report annually on its decisions, and the Bill will enable the Minister to request that the Board review any issue they consider necessary. This provides participants with a clear and accountable avenue for raising their concerns and seeking changes to the Trust Framework.	Medium
Regulators	Ensures governance of trusted government data sets remains within the legal Crown.	Medium
Other groups (e.g. wider government, users etc.)	An official Governance Board will be required to consult the public on the establishment and amendment of the Trust Framework rules, better ensuring rules that meet the needs of participants and the public.	Medium
Total monetised benefits	The Board's role will be to monitor and ensure the effectiveness of the Trust Framework. An effective Trust Framework is a key foundation of a thriving digital identity ecosystem. This has the potential to deliver significant financial benefits to a wide variety of ecosystem participants, though these are difficult to precisely monetise.	Uncertain. The total benefits of digital identity in a mature economy have been estimated at between 0.5-3 per cent of GDP by a review undertaken by Australia Post. Currently these benefits are being stymied by the lack of coherence in standards in the digital identity ecosystem. The Trust Framework, through the establishment of coherent standards will

		support the realisation of these benefits.
Non-monetised benefits	A Governance Board that achieves its goal of ensuring an effective Trust Framework will generate numerous social and economic benefits, by supporting innovation and integration of services, thereby making it easier for New Zealanders to access services and share their information with confidence and retain greater control over their information.	*Medium*

Whether accreditation to the Trust Framework should be required

In 2020, Cabinet agreed that the statutory Trust Framework would include the establishment of a department-based team to undertake accreditation of potential Trust Framework participants (the Accreditation Authority). The Authority would support the Governance Board, determining who is able to participate in the Trust Framework through assessment of their ability to comply with the Trust Framework rules. This approach is aligned with Australia which has implemented a standards-based Trust Framework with government-led accreditation and governance.

A decision has not yet been explicitly made by Cabinet on whether joining the Trust Framework will be purely optional or whether some or all participants will be required to seek accreditation.

Option One– Status quo - no requirement to seek accreditation to the Trust Framework for any participants

In July, Cabinet did not make any decisions on whether the Trust Framework should be mandatory, though the establishment of an 'opt-in' Trust Framework was implied. Therefore, under the status quo, all Trust Framework participants (including information providers and infrastructure providers) would not be required to become accredited to the Trust Framework.

This option will still create benefits that would not exist in the absence of a regulatory Trust Framework. Accreditation to the Trust Framework will allow participants to signal their compliance with the rules to other ecosystem participants, and to users, providing confidence that information is maintained and shared in a safe and trustworthy manner.

This option allows potential participants to move towards updating their systems and processes to meet Trust Framework requirements at their own pace, lowering transition costs and likely leading to greater compliance by those who choose to become accredited. It also allows the continued development of private sector digital identity ecosystems and Trust Frameworks. s6(b)(i)

However, there is a risk that optional accreditation may lead to low uptake of accreditation if participants do not perceive that the potential benefits outweigh the costs. This could result in lower overall compliance with the Trust Framework across New Zealand's digital identity ecosystem, which in turn could fail to achieve the key goal of improving trust and uptake of digital identity services.

Option Two – Minister has authority to delegate sectors for whom compliance is compulsory

Under this option, the Minister will have the authority to specify:

- classes of information that may only be shared by accredited participants (e.g. trusted government data sources); and
- organisations who may hold and share classes of information.

Before designating any sectors for whom accreditation is mandatory, the Minister would first need to consider a variety of factors, including:

- the likely effect of designation on users and the privacy of their information and relevant markets (e.g. efficiency, competition and innovation);
- the regulatory impact on sector participants; and
- any other matters the Minister considers relevant.

Public consultation would also be required to be undertaken on any proposals to make accreditation to the Trust Framework mandatory for any ecosystem participants. An example for this approach can be found with the Australian Consumer Data Right Act.

This proposal would help to ensure privacy and security and promote trust in critical sectors of the ecosystem, whilst providing flexibility to allow for entities to move towards compliance with the Trust Framework at different speeds, depending on their importance towards meeting the objectives of the Trust Framework, and to recognise the different costs that different organisations face in doing so. The accreditation of key sectors to the Trust Framework could also help to drive the wider ecosystem towards compliance more rapidly as businesses and service providers seek to cooperate with Trust Framework participants.

Option 3 – the Bill will specify which organisations must comply with the Trust Framework

Under this option, the Bill would specify which sectors must be accredited to the Trust Framework before providing specific digital identity services. These would include infrastructure providers and information providers.

While this option would likely improve overall trust in digital identity services, it would involve significant short-term costs for many businesses and service providers. Based on the costs of accreditation to Australia's Trusted Digital Identity Framework, the costs of accreditation to the Trust Framework will likely range from $10,000 to $250,000 depending on the complexity of the service being provided. In addition to this, some organisations may face significant costs in updating their IT services and processes in order to be compliant with the Trust Framework. If digital identity service providers do not see the value of accreditation, this may reduce the availability of digital identity services in the near term, especially for smaller service providers that have fewer resources to draw upon.

The Department has estimated that the cost of undertaking 25 complex accreditations in a year would amount to approximately $1 million.

Multi-Criteria Analysis

	Option One – optional accreditation	Option Two – Minister to designate classes of participants and information that must be accredited	Option Three – Bill to establish what services must be accredited
Principles	0 Improves privacy, security and interoperability where providers choose to become accredited.	+ Improves privacy, security and interoperability for key sectors of the ecosystem which could then drive wider adoption of standards across the sector.	+ Greatly improves privacy, security and interoperability for those able to afford accreditation and compliance, but in the near-term risks reducing inclusivity and the sustainability of the Trust Framework.
Trust	0 Will install greater trust in services which choose to become accredited, though if uptake of accreditation is low, overall trust in the ecosystem may not change much. Current indications are that interest in accreditation is strong, and demand for accreditation could be spurred by the government requiring public service departments to become accredited.	+ Will install greater trust in mandated services which could flow on to the wider ecosystem over time.	+ Will install greater trust in digital identity services.
Feasibility	0 Providers will be able to move towards accreditation as their own business practices and IT strategies suggest. May generate less value in the near term if uptake is lower than expected.	- Some providers may struggle to meet accreditation requirements, though this can be mitigated by consultation requirements and guidelines in the Bill.	- - Many service providers will find accreditation in the near term unfeasible. In a worst-case scenario this could potentially lead to providers withdrawing digital identity services, reducing participation in the ecosystem and its associated benefits.

Flexibility	0 Option is flexible to the requirements and capabilities of participants.	0 Some flexibility to respond to the capability of the sector and emerging trends and business models.	- - No flexibility to respond to changing capability of the ecosystem over time.
Overall assessment	0 This option allows greater flexibility for sector participants to move towards in a way that minimises costs for them. There is a risk that this may led to sub-optimal uptake of accreditation, though initial indications from the public and private sector is there is strong demand for uptake.	0 This option provides some privacy and security improvements over the status quo and leaves some flexibility for Ministers to respond to changing circumstances across the sector. However, classifying specific sectors of participants and information may prove complicated and will potentially present feasibility issues for some participants.	- While this option will achieve greater Trust in digital identity services that are accredited, it is unlikely to be feasible in the near term and would require legislative action to amend should the changes be required.

Conclusions

Both the status quo (optional accreditation to the Trust Framework) and Option 2 present viable approaches. The status quo risks reduced uptake of Trust Framework privacy and security standards in the near term but is the most feasible approach. It offers the most flexibility to Trust Framework participants. Under this option, there is also the potential for the Government to require accreditation to the Trust Framework for public service entities (or trusted government data sets) without relying on legislative instruments. Trusted government datasets are a key source of user attributes (e.g. name, date of birth, qualifications, health records etc.) that are needed by relying parties to assess entitlement to goods and services. This will provide a powerful incentive for private infrastructure providers to join the Trust Framework in order to provide services that involve the sharing of this information. Given the critical role that trusted government data sets will play in the evolving digital identity ecosystem, this represents a means of driving wider accreditation to the Trust Framework's rules, without the introduction of potentially burdensome requirements on service providers. For these reasons the status quo is currently our preferred option.

Summarise the costs and benefits of your preferred option

The preferred option in this case is the status quo (no requirement for any participants to join the Trust Framework). This option presents significant benefits over and above the status quo that existed prior to Cabinet's decision to establish a regulatory Trust Framework. These benefits are summarised below.

Affected groups *(identify)*	**Comment**: nature of cost or benefit (e.g. ongoing, one-off), evidence and assumption (e.g. compliance rates), risks	**Impact** *$m present value where appropriate, for monetised impacts; high, medium or low for non-monetised impacts*
Additional costs of the preferred option compared to taking no action		
Regulated groups	No requirement to take on any additional costs, except potentially for public service entities subject to Government directives.	$10,000 to $250,000 per entity, depending on the complexity of the accreditation and the need to develop pre-accreditation protocols to establish compliance with the rules. This cost will be voluntary, and so will only be undertaken were participants consider the costs are outweighed by the benefits.
Regulators	None directly (government won't be subject to accreditation and other fees as Treasury guidelines recommend generally avoiding this due to the inefficiency of government charging government. However, costs of public service share of the Board's activities will still need to be funded centrally).	Low
Other groups (e.g. wider government, users etc.)	Potentially lower system-wide standards for privacy, security and interoperability, at least in the short term.	Low (medium term)
Total monetised costs	The costs of accreditation will vary significantly depending on a variety of factors including the type of information being shared, the extent to which an applicant has already	$10,000 to $250,000 per applicant, zero for entities that do not wish to join the Trust Framework. Total costs estimated at

	established their compliance with the rules and the role they are seeking accreditation for. These cost estimates are based on costs of accreditation to Australia's Trusted Digital Identity Framework. Costs of accreditation in New Zealand are being tested with partner entities as part of the Rules Development Programme.	approximately $1 million in the near term, subject to demand for accreditation. Further many digital identity providers are already investing significantly in their services. The Trust Framework will provide a guide for ecosystem participants to undertake these investments in a systematic way that maximises cross-sector benefits.
Non-monetised costs	In the near term the main costs will relate to potentially reduced trust in digital identity services if demand for accreditation is low. The risk of this is considered low in the near term as a group of 18 public and private sector providers are already working with the Rules Development Programme. These include services involved with AML compliance (e.g. RealAML), identity providers (e.g. MATTR) and information providers (e.g. Inland Revenue and the Ministry of Health).	*Low*
Additional benefits of the preferred option compared to taking no action		
Regulated groups	Flexibility to move towards accreditation overtime as their own needs and business models allow it.	Medium
Regulators	Ability to test and refine accreditation processes in the near term before they become more widely used.	Medium
Other groups (e.g. wider government, users etc.)	Ability to identify which entities are Trust Framework compliant through the accreditation scheme.	Medium
Total monetised benefits	The benefits from accreditation will depend on the long-term uptake of the scheme. Early engagement as part of the	Uncertain. The total benefits of digital identity in a mature economy have been

	Digital Identity and Rules Development Programme indicates strong demand for accreditation.	estimated at between 0.5-3 per cent of GDP by a review undertaken by Australia Post. Currently these benefits are being stymied by the lack of coherence in standards in the digital identity ecosystem. The Trust Framework, through the establishment of coherent standards will support the realisation of these benefits.
Non-monetised benefits	Accreditation will act as a signal to users and partner entities, supporting greater uptake and the consequent benefits that digital identity brings.	*Medium*

Describe and analyse the options: Enforcement mechanisms

In order to maintain Trust Framework accreditation, participants or potential participants must remain *compliant* with the Trust Framework rules. Enforcement will be the approach taken to situations where a participant has failed (either deliberately or accidentally) to successfully implement the rules of the Trust Framework. Enforcement mechanisms will be used to remediate non-compliance by an *accredited* party and discourage similar behaviour by other *accredited* parties.

The Accreditation Authority will be responsible for monitoring compliance and enforcing the Trust Framework's rules. A variety of low impact options are available to address low-level non-compliance (including working with participants to develop a compliance plan, introducing additional reporting requirements and issuing private and public warnings) and are not assessed as part of this RIS.

The options set out below includes the establishment of a pecuniary penalties regime. It is difficult at this time to determine what specific conduct would potentially be subject to a penalty as the Trust Framework rules are still in development. As a result, an in-principle decision is being sought from Cabinet on the establishment of pecuniary penalties in the Bill. This section will be updated prior to seeking final decisions, subject to the development of the rules and the identification of conduct that will be subject to a penalty.

Offences and penalties

The Bill also proposes the establishment of a set of criminal offences to protect the integrity of the Trust Framework. Similar offences are common in a variety of statutory licensing regimes (e.g. the Immigration Advisors Licensing Act, the Lawyers and Conveyancers Act, the Electricity Industry Act, etc). These offences include:

- knowingly or recklessly representing themselves as being an accredited participant of the Trust Framework when they are not – with a maximum penalty of $50,000 for individuals and $100,000 for organisations
- knowingly or recklessly supplying to the Authority any false or misleading information for the purposes of any application for accreditation to the Trust Framework – with a maximum penalty of $50,000 for individuals and $100,000 for organisations
- not updating information required under the accreditation process (e.g. business address) - with a maximum penalty of $10,000 for individuals and $20,000 for organisations
- not informing the Authority of other significant matters (e.g. prior criminal convictions,)– with a maximum penalty of $10,000 for individuals and $20,000 for organisations
- without reasonable excuse, obstructing the Authority in the exercise of their powers to require the provision of documents and information – with a maximum penalty of $20,000.

The Department has engaged closely with the Ministry of Justice in the development of these offences and the associated penalties. The Ministry is broadly supportive of the inclusion of these offences, though has queried the need for offences for updating information required

under accreditation process and of not informing the Authority of other significant matters. The Department's view is that:

- Not updating information required by the accreditation process and failing to make the Authority aware of significant matters may lead to situations where the Accreditation Authority is unaware of potential risks of non-compliance, or could lead to situations where the use of its powers (e.g. its power to require the provision of information) cannot be acted upon in a timely way;

The remaining options considered below are not mutually exclusive.

Option One – Status quo

Under this option, the Accreditation Authority would be restricted to the use of the low-impact compliance mechanisms (e.g. warnings, reporting requirements) to address non-compliance. Where non-compliance is not addressed, accredited participants would be removed from the Trust Framework when compliance with the Trust Framework is reassessed (which will be required by the Act annually).

This will be appropriate for addressing less serious non-compliance. However, these options are likely to have limited effect in addressing recidivist or serious non-compliance, especially when non-compliance threatens the privacy and security of the users of Trust Framework accredited services.

Under this option, there are also other legal avenues to address non-compliance with the Trust Framework. In particular, the Privacy Act provides a means of filing complaints for non-compliance with relevant codes of conduct and the information privacy principles. If a compliance order issued by the Privacy Commissioner is not followed, then the participant could be charged with a criminal offence and subject to a penalty of up to $10,000.

Option Two – Suspension or revocation of a participant's Trust Framework accreditation

Under this option, the Accreditation Authority would have the authority to suspend or revoke a participant's accreditation in some circumstances.

While the power to revoke or suspend an accreditation or license is common in most statutory licensing regimes, there are practical issues that affect its appropriateness for the Trust Framework. The suspension of a participant's accreditation could in many cases negatively affect the ability of users to access services and entitlements. This risk is exacerbated by the potential for the Trust Framework to foster interconnected and interoperable services between different entities. While switching service providers may be an option in some cases, this will be less viable for significant institutions and agencies such as public service entities and financial institutions. This risk was noted by the Ministry of Health when it was consulted in 2019.

These risks would be alleviated by requiring that this punishment only be available were an accredited participant has engaged in serious or recidivist non-compliance that threatens the privacy and security of Trust Framework users. This is like the approach taken in the Electricity Industry Act were suspensions and revocation of licenses can only be made where

non-compliance is found to be prejudicial to the operational and financial security of the wholesale electricity market.

Option Three – Pecuniary fines for non-compliance with the Trust Framework

Under this option non-compliant participants could be issued with pecuniary fines of up to $10,000. When considering whether to issue a penalty, factors that would need to be considered would include:

1. the severity of the breach;
2. the impact on other sector participants;
3. the extent to which the breach was intentional or otherwise;
4. past behaviour;
5. whether the matter was disclosed to the Authority;
6. the amount of time before the breach was resolved; and
7. whether the participant benefitted from the breach.

The inclusion of pecuniary penalties would necessitate the establishment of a rulings panel to determine what (if any) penalties are appropriate in the circumstances.

While the penalty itself will have little impact on larger participants in the Trust Framework (e.g. financial institutions), it will still impose significant reputational risks that will incentivise compliance.

Multi-Criteria Analysis

	Option One – Status Quo	Option Two – Suspensions and revocations	Option Three – establishing a pecuniary penalties regime
Principles	0	0 Risk that the use of suspensions and revocations could negatively affect the people-centredness and inclusivity aspects of the Trust Framework by reducing access to entitlements. Can be addressed by restricting use to severe non-compliance that threatens privacy and security.	+ Supports the principles by providing an incentive to comply with privacy and security requirements.
Trust	0	+ Improves the capability of the Authority to respond to cases of serious non-compliance and restore public trust in the effectiveness of the Trust Framework.	+ Provides the Trust Framework with a means of responding to cases of serious non-compliance that strongly incentivise remediation of privacy and security breaches.
Feasibility	0	0 Not a feasible punishment in most cases. Encourages participation by providing a means of removing bad-actors from the Trust Framework.	- Requires the establishment of a rulings panel to adjudicate on the appropriateness of penalties. This may impose additional costs on Trust Framework participants Presence of penalties may discourage participation in the Trust Framework regime. This risk can be mitigated by clearly establishing in the rules what

			behaviour will potentially be subject to penalties and how this can be avoided.
Flexibility	0	+ Provides the authority with a wider variety of tools to address more serious non-compliance.	+ Provides the authority with a wider variety of tools to address more serious non-compliance.
Overall assessment	0	+ While only viable in a limited number of circumstances, the ability to suspend or revoke accreditation is an important tool for restoring public trust in cases of severe breaches that threaten the privacy and security of Trust Framework users.	+ While unlikely to offer a significant financial deterrent, the ability to penalise non-compliance is an important reputational incentive for addressing non-compliance.

Conclusions

The Department supports including providing the Accreditation Authority with the power to suspend and revoke accreditation, and to issue pecuniary penalties in cases of significant non-compliance. This provides the greatest flexibility to address a wide variety of non-compliance and protect the privacy and security of Trust Framework users. The strenuousness of these penalties for service provision and trustworthiness does support the requirement for a decision-making panel to decide on and review the application of these penalties.

Summarise the costs and benefits of your preferred option

Affected groups *(identify)*	**Comment**: nature of cost or benefit (e.g. ongoing, one-off), evidence and assumption (e.g. compliance rates), risks	**Impact** *$m present value where appropriate, for monetised impacts; high, medium or low for non-monetised impacts*
Additional costs of the preferred option compared to taking no action		
Regulated groups	Trust Framework participants: The application of suspensions and revocations may have significant costs for participants, but these will only be able to be applied in the cases of the most severe non-compliance	Low for compliant participants – will be additional costs associated with the development of a rulings panel and complaints process (assuming no Crown funding). The cost of an equivalent rulings panel for the Electricity Authority is approximately $300,000 per annum.
Regulators	Uncertain, will depend on the extent of non-compliance and the need for penalties to be made and reviewed – this is currently being assessed as part of the rules development programme.	Medium
Other groups (e.g. wider government, users etc.)	If the costs of the application of penalties significantly adds to the maintenance of the Trust Framework, this may have flow-on effects in terms of costs to users. Some users may be temporarily unable to access services if suspensions are applied (though this will only be the case in situations where their privacy or security is seriously threatened).	Medium, potentially low in the long term – depends on the number of accredited participants and the regularity of non-compliance. Even in cases where digital-identity services are suspended, non-digital mechanisms for accessing services and entitlements will still be available.
Total monetised costs	Initially at least compliance is anticipated to be high, as early accredited participants to the Trust Framework will have worked in conjunction with the Rules Development	Uncertain, likely low in the near term – comparable rulings panel cost of $300,000 for Electricity Authority.

	Programme to help test the rules and the accreditation process.	
Non-monetised costs	The presence of fines and suspensions may deter some potential participants from becoming accredited. This risk may be mitigated by engagement with potential participants to help them understand the circumstances in which the penalties may be applied, how less strenuous sanctions (e.g. warnings, reporting requirements) will likely be used in most circumstances and how non-compliance can be avoided.	*Low-Medium*
Additional benefits of the preferred option compared to taking no action		
Regulated groups	Compliant Trust Framework participants may have additional confidence that other accredited participants are compliant.	Low
Regulators	Authority will have greater capability to enforce compliance and respond to a wider range of non-compliance.	High
Other groups (e.g. wider government, users etc.)	Users more likely to be protected from behaviour that raises significant privacy risks.	High
Total monetised benefits	Higher compliance with the Trust Framework will lead to greater trust in accredited participants and the realisation of potential long-term benefits.	The total benefits of digital identity in a mature economy have been estimated at between 0.5-3 per cent of GDP by a review undertaken by Australia Post. Currently these benefits are being stymied by the lack of coherence in standards in the digital identity ecosystem. The Trust Framework, through the establishment of coherent standards will support the realisation of these benefits.

Non-monetised benefits	Higher trust in accredited participants leads to greater uptake of accredited services, resulting in easier access to integrated and innovative digital services.	High

Describe and analyse the options: Disputes resolution

The proposed regulatory regime will require processes to ensure participants can exercise their natural justice right to be heard on matters such as complaints about the decisions of the Accreditation Authority or the Governance Board and regarding compliance with the rules.

As this is a new regulatory regime there is no data on the volume and nature of disputes among potential digital Trust Framework participants, so further sector engagement will be required on the type of issues likely to form disputes and this will inform the final design of the regime. In the near term the volume of disputes is anticipated to be low due to the small number of accredited participants and their close involvement in the rules development process providing them with clarity around the rules and standards.

A range of dispute resolution implementation options have been considered:

- Option 1: do nothing - no formal dispute resolution process
- Option 2: a formalised voluntary scheme
- Option 3: a requirement for Alternative Dispute Resolution (ADR) established in legislation
- Option 4: a dedicated Disputes Tribunal established in legislation

Following discussion with the Ministry of Justice, establishing a Disputes Tribunal was discounted due to the cost and uncertain demand for a dedicated Tribunal.

The criteria used to assess options are:

- User focused and accessible: Users of dispute resolution processes are at the centre of all aspects of the dispute resolution system. Dispute resolution is easy for potential users to find, enter and use regardless of their capabilities and resources.
- Independent and fair: Disputes are managed and resolved in accordance with applicable law and natural justice. All dispute resolution functions are, and are seen to be, carried out in an objective and unbiased way.
- Efficient: Dispute resolution provides value for money through appropriate, proportionate and timely responses to issues. It evolves and improves over time and makes good use of information to identify systemic issues.
- Effective: Dispute resolution delivers sustainable results and meets intended objectives. It fulfils its role in the wider government system by helping minimise conflict and supporting a more productive and harmonious New Zealand.
- Accountable: There is public confidence in dispute resolution. Those involved in its design and delivery are held to account for the quality of their performance. Regular monitoring and assessment and public reporting encourages ongoing improvement across the system.

- Alignment to Objectives of the Trust Framework.

Option One – No formal dispute resolution process.

If no provision for dispute resolution is made in the Bill, disputes will be resolved *either* as agreed upon in their complaints processes, contractual arrangements, or through the courts. Disputes between users and participants will be resolved *either* through a complaint to the Accreditation Authority and subsequent decision on compliance with Trust framework rules, through a complaint to another body such as the Privacy Commissioner, or through the courts.

This is a similar approach take to complaints by the Australian Digital Transformation Authority.

Our assessment of this option against our identified criteria for a disputes resolution process is as follows:

- User focused and accessible: There is no guarantee that users will be at the centre of dispute resolution processes.

- Independent and fair: Participants will have different approaches to resolving issues which mean there may not be a consistent and equitable process. The lack of structure will mean all parties will face uncertainty as to the outcome. There is a risk that some participants and users will be disadvantaged by a potential power imbalance.

- Efficient: The efficiency of this approach cannot be predicted due to its uncertain nature. In some cases, disputes may be resolved in a proportionate and timely manner. It will be more difficult to monitor and improve processes over time.

- Effective: There is a risk that cases are unnecessarily referred to courts which may not achieve the objectives of helping to support the operation of the Trust Framework and minimise conflict.

- Accountable: It will be more difficult to hold processes to account and encourage ongoing improvement.

  Alignment to Trust Framework Objectives: this option is not closely aligned to the Trust Framework objectives as it is not predictable, flexible or fast. It is also less likely to be able to consider Te Ao Māori perspectives.

Option Two – Formalised voluntary mediation scheme

A formalised voluntary dispute resolution scheme would involve Trust Framework participants voluntarily agreeing to participate in dispute resolution processes before taking further action to resolve disputes.

Our assessment of this option against our identified criteria for a disputes resolution process is as follows:

- User Focused and accessible: use of a single dispute resolution scheme administered by the Accreditation Authority would provide consistency and predictability as to how disputes will be managed. Voluntary nature of scheme would impact application however.

- Independent and fair: Use of the dispute resolution scheme will enhance equitable treatment between parties however larger organisations with more resources to fight disputes (e.g. in-house counsel) may be less inclined to voluntarily adhere to the scheme so some risk would remain.

- Efficient: use of a dispute resolution scheme is likely to be faster than seeking redress through the courts.

- Effective: dispute resolution processes such as negotiation and mediation enable more flexible awards/remediation of issues than what is generally available through the courts.

- Accountable: It will be more difficult to hold processes to account and encourage ongoing improvement than option 3.

- Alignment to Trust Framework Objectives: this option is partially aligned to the objectives of the Trust Framework as it offers some predictability, flexibility and speed. However, parties may elect not to participate so the impact of this option may be limited. It is also less likely to be able to consider Te Ao Māori perspectives.

Option Three – A requirement in legislation for participants to use dispute resolution processes

This option would require all Trust Framework participants to undertake a dispute resolution process before they could take enforcement action through the Accreditation Authority against other participants on matters that relate to the compliance with the rules and or with consumers. The legislation could require participants to belong to an approved disputes resolution scheme.

The legislation could prescribe a system that would cover:

- disputes about all aspects of the Trust Framework rules

- requirements for mediation/arbitration to be provided by independent approved mediators/adjudicators (this could involve private sector providers, membership of existing scheme or government scheme)

- procedural requirements mediation/arbitration e.g. to take place within specific time limits

- investigation powers

- recommend remediation action (including compensation)

- exemptions (for instance don't provide services that are likely to result in disputes)

- measures to avoid participants acting in bad faith and gaming the system, i.e.:
    - where a participant fails to comply with a request for mediation or an offer of mediation any enforcement action on matters relating to the application of Trust Framework rules will be void
    - restrictions on how frequently participants could request mediation on matter relating to the same rule issues.

To achieve the purpose/objective of the dispute resolution process it is proposed that the legislation can provide for a range of consensual dispute resolution processes, including facilitative and evaluative processes, so that each dispute can be resolved through the process assessed to be the most appropriate to the dispute, having regard to the nature and circumstances of that dispute.

This provides for the likelihood that the design of the scheme will evolve as the Trust Framework grows. What is required for a small number of participants (and number of disputes) will be different than what is required as the scheme grows.

Further work is required on the detailed design and implementation of the system and this will be subject to further impact analysis and consultation with users of the system. Further work is required to determine whether it will be important for mediators to have a knowledge of the technical working of digital services.

Our assessment of this option against our identified criteria for a disputes resolution process is as follows:

- User focussed and accessible: Users can be placed at the centre of all aspects of the dispute resolution system.
- Independent and fair: use of a single dispute resolution scheme administered by the Accreditation Authority would provide consistency and predictability as to how disputes will be managed. Use of the dispute resolution scheme will enhance equitable treatment between parties.
- Efficient: use of a dispute resolution scheme is likely to be more proportionate and timely than the other options.
- Effective: dispute resolution processes such as negotiation and mediation enable more flexible awards/remediation of issues than what is generally available through the courts.
- Accountable: There is likely to be more public confidence in the dispute resolution system. This option allows for better monitoring and assessment to ensure improvements to the dispute resolution system occur as required.
- Alignment to Trust Framework objectives: this option is aligned to the objectives of the Trust Framework as it offers predictability, flexibility and speed. Te Ao Māori perspectives can also be at the core of the design of the dispute resolution system.

	Option One – No Disputes resolution regime	Option Two – Voluntary regime	Option Three – Required participation in disputes resolution in legislation
Principles	0 This option is not closely aligned to the Trust Framework objectives as it is not predictable, flexible or fast.	+ This option is partially aligned to the objectives of the Trust Framework as it offers some predictability, flexibility and speed. However, parties may elect not to participate so the impact of this option may be limited.	+ This option is aligned to the objectives of the Trust Framework as it offers predictability, flexibility and speed and consider Te Ao Māori principles.
Equity (User focused and accessible, independent and fair)	0 Some participants will be disadvantaged by a potential power imbalance, particularly between large and small organisations and users. Participants will have different approaches to resolving issues which mean there will not be a consistent and equitable process. The lack of structure will mean all parties will face uncertainty as to outcome.	+ Use of disputes resolution scheme will enhance equitable treatment between parties and consistency and predictability as to how disputes will be managed. However larger organisations with more resources to fight disputes (e.g. in-house counsel) may be less inclined to voluntarily adhere to the scheme so some risk would remain.	++ Use of the dispute resolution scheme administered by the Accreditation Authority will enhance equitable and consistent treatment between parties and place users at the centre of all aspects of the system.
Efficient and effective	0 The cost to government will be low for some as participants will be responsible for their own dispute resolution processes if any. In some cases, disputes may be resolved rapidly through application of contractual terms. However, if most cases are referred to the courts, this would not be an expedient or cost-effective option. The settlement of lengthy and public disputes in court	+ Establishing a disputes resolution scheme would require government investment. However, disputes could be resolved more quickly and cheaply than by seeking redress through the courts, encouraging greater participation.	+ Establishing a dedicated disputes resolution scheme would require government investment. However, disputes could be resolved more quickly and cheaply than by seeking redress through the courts, encouraging greater participation.

	could discourage participation in the Trust Framework.		
Accountable	0 This option would enable organisations to adapt their contractual terms to fit their needs. However, there is limited scope to hold those involved in its design to account for the quality of the performance.	+ Dispute resolution processes could include accountability requirements. .	+ Accountably measure could be prescribed in legislation to ensure regular monitoring and reporting and continuous improvements.
Overall assessment	0 Not an appropriate option given the considerable variation in the likely costs of accrediting different providers.	+ As the Trust Framework is voluntary, having industry organisation take the lead could encourage a wider range of organisation to use ADR as part of best practice approaches to resolving disputes.	++ This option achieves the same benefits as option 2, and best ensures a level playing field for all participants.

Conclusions

The Department supports requiring participants to participate in disputes resolution prior to taking enforcement action. This option the quickest and most cost-effective dispute resolution and allow for flexible solutions and best ensures that users are placed at the centre of the dispute resolution process and Te Ao Māori perspectives and approaches to dispute resolution are provided for.

Affected groups *(identify)*	**Comment**: nature of cost or benefit (e.g. ongoing, one-off), evidence and assumption (e.g. compliance rates), risks	**Impact** *$m present value where appropriate, for monetised impacts; high, medium or low for non-monetised impacts*
Additional costs of the preferred option compared to taking no action		
Regulated groups	All Trust Framework participants required to join an approved accreditation scheme.	It is envisaged that the costs would be shared equally between participants, though it will be necessary to consider how to mitigate the impact on users. Based on information on the cost of mediation in other regimes individual mediation are estimated to cost an average of $6000 per dispute ($3000 for each party), based on 20 hours at $300 per hour. This will vary depending on the complexity of the case. It does not include the internal costs for each participant.
Regulators	Low cost for the regulator as no dedicated disputes resolution system needs to be established.	Low
Other groups (e.g. wider government, users etc.)	Generally low costs. Users will still have access to a complaints system as a first port of call for disputes. It will be necessary to consider how to mitigate the impact on accessibility for users/consumers.	As above, though the cost of mediation ($6000 on average) for individual users will be more significant than for participating entities.
Total monetised costs	Overall costs are anticipated to be low at least in the near term, as early participants will work closely with the rules development team in the development of the rules and the accreditation process.	$6,000 on average.
Non-monetised costs	Potential reduced trust in the Trust Framework if – in the absence of a dedicated disputes body like a tribunal – access to mediation is seen to be too expensive.	Low
Additional benefits of the preferred option compared to taking no action		
Regulated groups	Reduces risk of costly and time-consuming legal action in the courts.	High

Regulators	Raises trust in the Trust Framework by avoiding potentially costly and lengthy legal disputes that undermine trust.	High
Other groups (e.g. wider government, users etc.)	Raises trust in the Trust Framework by avoiding potentially costly and lengthy legal disputes that undermine trust.	High
Total monetised benefits	Will depend on overall number of disputes (likely to be low in the near term) but as the Trust Framework scales likely to be significant.	Unquantifiable
Non-monetised benefits	Raises trust in the Trust Framework by avoiding potentially costly and lengthy legal disputes that undermine trust.	High

Cost recovery

In July 2020, Cabinet noted that a cost recovery model will be developed as part of the policy and legislative programme for the statutory Trust Framework [CAB-20-MIN-0324 refers].

Any system of cost recovery will need to consider the respective public and private benefits conferred by the Trust Framework. While some benefits may be financial and private in nature, many are not. The World Bank has stated that identification should be treated as a public good, provided to facilitate the rights and inclusion of individuals and to improve administration and service delivery. Accreditation to the Trust Framework offers a clear private and commercial benefit to participants. This will potentially include the ability of private sector providers to utilise trusted government information sources for the provision of digital services.

There may be policy objectives for partially funding the costs of accreditation from general taxation in some cases. These include the merit-good aspects of the maintenance and enforcement of the Trust Framework, encouraging participation during its initial establishment and recognising that the costs of accreditation may pose a significant barrier to entry for smaller entities (particularly relying parties).

Ongoing work will inform any future potential bids to partially fund the cost of accreditation and administration of the Trust Framework from the Crown. However, in the current fiscal climate there is a significant likelihood that Crown funding will be unavailable to support the Trust Framework.

Because Cabinet has already sought advice on different options for cost-recovery, this RIS restricts itself to the consideration of these options. Because the status-quo (i.e. no formal regulated Trust Framework) has been superseded by Cabinet's decisions, the different options for cost-recovery are being compared against a counterfactual based on the planned rules development programme. The Trust Framework rules and accreditation processes will need to be finalised before we can determine what kind of cost recovery model should be established.

Option One – There is no formal accreditation process to the Trust Framework (counter factual)

Under this option, there would be no formal accreditation process for entrance to the Trust Framework. The Trust Framework would instead act as a set of best-practice guidelines that entities can seek to comply with.

Option Two – Fixed charges regime

Under this option, the Bill will establish the power for the Authority to participants will be make regulations for the setting of fees for accreditation (with appropriate consultation requirements). The total cost of the Trust Framework in the near term (under a model where accreditation to the Trust Framework is opt-in) has been estimated at $1.5 million, with the Accreditation Authority having the capability to undertake up to 100 'simple' accreditations or up to 25 complex accreditations (with the relative cost of simple and complex accreditations estimated at $10,000 and $40,000 respectively).

A variety of factors influence the relative complexity of the accreditation process, including:

- Whether or not applicants have already separately established (e.g. through auditing processes) that they are compliant with Trust Framework standards;
- How large and complex a volume of data is being relied on;

- The number of roles that an applicant is seeking to be accredited for (e.g. some applicants will seek to be accredited as both information and infrastructure providers);
- The level of assurance that is needed for proposed services (e.g. services involving higher risk will require greater levels of assurance around the accuracy and security of data.

A flat fee is more transparent to potential applicants and simpler to administer for the Authority. However, it is unlikely to be able to equitably account for the differences in the individual circumstances of applicants, resulting in significant cross-subsidisation between different applicants. This may drive smaller providers and organisations for whom accreditation involves relatively low cost to avoid accreditation to the Trust Framework, especially in the near term, before the Trust Framework scales and when the potential benefits are less apparent.

Option Three – Variable charges for accreditation to the Trust Framework

Under this option the Authority would have the power to set variable charges for accreditation and the costs of administering the Trust Framework (i.e. to charge applicants based on the number of hours and direct cost of an accreditation).

This option will be more complex to administer. However, it presents a more equitable approach, as it will avoid cross-subsidisation between simple and complex accreditation processes. This in turn will incentivise more potential participants with relatively simple accreditation processes to apply for accreditation, enabling a more rapid scaling of the Trust Framework (and the corresponding benefits that come with it).

Option Four – a levy on participants to fund the Trust Framework

Under this option, the Authority would have the power to impose a levy on all accredited system participants (e.g. information providers and infrastructure providers), rather than charging for the costs of Accreditation upfront.

There are some aspects of the Trust Framework that make a levy an attractive option for cost recovery. The Trust Framework itself has many aspects that make it like a club good or even a public good. Use of the Trust Framework is non-rivalrous (one entity's use of the Trust Framework's rules does not diminish another's). And while it is possible to exclude entities from accessing the Trust Framework rules, there are strong policy reasons for making them publicly available.

On this basis there is an argument that at least some components of the Trust Framework (i.e. governance, enforcement) should be funded through a levy. Levies are often charged where it is easier to establish a direct link between a group of users and their benefit from the consumption of a service than it is for an individual user. Levies are also common in sectors where entities must cover the costs of a regulator or promoter of the industry (e.g. the fire service).

However, a levy should aim to reflect the level of benefit received (or risk created by) each member of the group. It is difficult to identify an accurate and easily collected measure of benefit against which a levy could be applied. One potential measure could be revenues earned from the provision of digital identity services. A 2020 study from Juniper Research has found that global digital identity revenue from mobile network operators alone will rise from $1.3 billion in 2020 to more than $8 billion by 2025.

However, charging a levy on financial revenues from digital identity services would require the creation of a significant auditing function within the Authority to attempt to ensure compliance (further increasing the funds that would need to be raised from participants). Additionally, it would be relatively straightforward for some participants to avoid a levy on financial benefits (e.g. by offering digital identity services for free and recovering benefits through other aspects of their business).

Multi-Criteria Analysis

	Option One – No accreditation and cost recovery	Option Two – Fixed charging	Option Three – Variable charging	Option Four - Levy
Principles	0 Any entity may review the rules, but cannot guarantee any entities compliance and hence security, privacy and interoperability. Inclusive (as it's free) but the effectiveness and the sustainability of the Trust Framework may fall over time if they are not complied with.	+ Likely to be less inclusive as some potential applicants may be discouraged by upfront costs. Costs are highly transparent. However, will be able to ensure the privacy, security and interoperability of accredited participants, thereby improving the sustainability of the Trust Framework.	+ More inclusive, and likely to promote security, privacy and interoperability by leading to high levels of accreditation to the Trust Framework. Costs will be less open and transparent than under option 2.	+ Effectively supports the principles of an inclusive Trust Framework by recognising the wider public benefits and lowering initial cost to entry.
Equity[6]	0 All participants can use the Trust Framework rules free of cost.	- Will lead to cross-subsidisation between different participants.	++ Better reflects the actual costs that different participants create for the Accreditation Authority	- A levy based on revenues from identity services may better reflect ability to pay. However, some cross-subsidisation may still arise between more and less complex accreditation processes. Costs may also be avoided by entities that do not charge for services.
Feasibility	0	+	+	-

[6] As noted above, equity replaces trust for the consideration of cost-recovery options.

	Can be implemented without additional cost. However, this option may generate limited value for participants as they have no way of signalling whether they are compliant to the public and partner entities.	Relatively straightforward to implement. Establishes compliance, thereby supporting trust and associated benefits.	More complicated to administer and provides less certainty for sector participants regarding potential costs. Establishes compliance, thereby supporting trust and associated benefits.	Lower entry costs may encourage greater participation; however, the use of a levy system would necessitate the development of a monitoring function to investigate levy avoidance. Establishes compliance, thereby supporting trust and associated benefits.
Flexibility	0 This option does not respond to the widespread stakeholder support for the establishment of a true Trust Framework.	0 Highly inflexible and less scalable as a wider variety of potential participants seek to join the Trust Framework over time.	++ More responsive to the needs of different applicants and more likely to lead to be scalable to a larger number of participants	0 This option would potentially be less flexible in assigning costs as new business models emerge.
Overall assessment	0 While feasible, this option fails to achieve the Trust Framework's core objectives of realising the value of digital identity and supporting trust in digital identity services.	0 Not an appropriate option given the considerable variation in the likely costs of accrediting different providers.	+ Will more effectively meet the needs of a wider variety of sector participants.	- Lowers entrance costs and potentially reflects ability to pay but would be complex to administer and creates the risk of cost-recovery avoidance.

Conclusions

The likely significant variance in the costs of accreditation means that only variable charging presents a viable option for cost recovery. Fixed charging would lead to dramatic cross-subsidisation between participants and would likely discourage participation. A levy has certain advantages – particularly its ability to reflect the extent to which different organisations benefit from the governance and enforcement aspects of the Trust Framework. However, its potential to be avoided (and the additional cost of building a capability to monitor compliance) reduces its viability as an option.

Summarise the costs and benefits of your preferred option

Affected groups *(identify)*	**Comment**: nature of cost or benefit (e.g. ongoing, one-off), evidence and assumption (e.g. compliance rates), risks	**Impact** *$m present value where appropriate, for monetised impacts; high, medium or low for non-monetised impacts*
Additional costs of the preferred option compared to taking no action		
Regulated groups	Allocation of costs for accreditation	$10,000 to $40,000 depending on flexibility of Trust Framework – plus additional costs for the governance and enforcement aspects of the Trust Framework – these initially may increase costs by over 30% but will decline as participation in the Trust Framework grows.
Regulators	Additional capability required to calculate costs for accreditation.	Uncertain - will depend on the demand for accreditation.
Other groups (e.g. wider government, users etc.)	Costs of accreditation likely to be passed on to users through digital identity services.	Uncertain, will decline as the scale of the Trust Framework increases.
Total monetised costs	Allocation of costs for accreditation.	Total estimated cost of accreditation of approximately $1 million in the near term, potential to grow as Trust Framework scales and demand for accreditation rises.
Non-monetised costs	Trust Framework rules and standards will still be made public, so entities can work to comply with the rules even if they find the costs of accreditation overly burdensome.	Low
Additional benefits of the preferred option compared to taking no action		
Regulated groups	Minimises cross-subsidisation for accreditation. Sends a signal to partner-entities and users that their services are	Will depend on each entity's commercial model.

	reliable and trustworthy. In this way participants will pay a fair price for the commercial and economic benefits of being accredited to the Trust Framework.	
Regulators	May drive increased participation of the Trust Framework.	Medium
Other groups (e.g. wider government, users etc.)	Wider uptake of accreditation to the Trust Framework will improve privacy, security and interoperability standards across the ecosystem.	Medium
Total monetised benefits	Accreditation to the Trust Framework will lead to greater trust in digital identity and the realisation of potential long-term benefits.	The total benefits of digital identity in a mature economy have been estimated at between 0.5-3 per cent of GDP by a review undertaken by Australia Post. Currently these benefits are being stymied by the lack of coherence in standards in the digital identity ecosystem. The Trust Framework, through the establishment of coherent standards will support the realisation of these benefits.
Non-monetised benefits	Higher efficiency in the provision of Trust Framework accreditation services and fair allocation of accreditation costs between participants, leading to levels of participation that reflect the economic and commercial benefits of the Trust Framework.	High

Section 3: Implementing the preferred option

How will it be implemented?

The Accreditation Authority will be responsible for administering and enforcing the Trust Framework. Cabinet agreed in July 2020 that the Accreditation Authority will sit within a public service department (likely to be the Department of Internal Affairs). The Accreditation Authority will be staffed by the Chief Executive of the host department.

Currently it is intended that the Bill will be considered by the house before the end of 2021, and that it will come into effect by mid-2022. The proposal to establish an opt-in Trust Framework will not impose any requirements on ecosystem participants unless they choose to become accredited.

Cabinet's authority is being sought to release an exposure draft of the Bill, prior to returning to the Cabinet Legislation Committee in 2021. This will provide the public with opportunity to comment on whether the Bill gives appropriate effect to policy proposals – and likely contribute to shaping more detailed design of the Trust Framework.

However, oofficials will engage with potential participants on the privacy, security and information management rules under the Trust Framework through the rules development programme and the ongoing engagement requirements in the Bill throughout 2021. These rules of the Trust Framework will be implemented through secondary legislation, along with several other aspects of the Trust Framework, including:

- fines for infringement offences;
- pecuniary penalties;
- certification requirements for third party assessors; and
- setting charges for accreditation.

Cabinet decisions on the content of these regulations will be sought before the introduction of the Bill to the House of Representatives (currently proposed for early August 2021).

The rules development programme will involve representatives from the GCDO, the Government Chief Information Security Officer, the Government Chief Data Steward, the Office of the Privacy Commissioner and Te Ao Māori. As part of this programme, officials will test the accreditation process and its costs with partner entities in order to try to identify and mitigate any potential risks that the accreditation may prove too expensive or difficult for participants to comply with.

Given Māori are Treaty partners, officials are actively building the capability required to enable effective partnership with Māori. Partnering with Iwi and Māori organisations, post-settlement governance entities, other rūnanga and key Māori partners would help increase trust and participation levels amongst Māori communities and meet the Crown's Treaty of Waitangi obligations.

To help achieve this, the Government Chief Digital Officer (GCDO) will continue to engage with iwi groups (including the Iwi Chairs Forum and the Data Iwi Leaders Group) to establish an enduring relationship with Māori and to work in partnership in the development of the Trust Framework. Advice on Māori representation in the governance of the Trust Framework will be a priority in future engagement with iwi. The Bill will also require that the Board have regard to Te Ao Māori perspectives.

Officials will also continue to work with the Government Centre for Disputes Resolution to develop a disputes resolution regime that will support effective and efficient disputes resolution in the sector. As part of this, we also intend to undertake further engagement with the sector on what is required in an effective disputes process (including ensuring that Te Ao Māori perspectives are taken into account).

After the rules development programme has finished developing the rules, the Governance Board will take responsibility for ensuring they are effective at meeting the principles of the Trust Framework. Where necessary, they will have responsibility for identifying potential amendments to the rules that are required to implement the Trust Framework effectively.

The Department is also continuing to work with officials in partner jurisdictions. The Department has developed a road-map for mutual recognition with Australia's Trusted Digital Identity Framework that will provide the basis for Australian companies offering Trust Framework approved services in New Zealand.

Monitoring, Evaluation, and Review

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 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 the Trust Framework and reporting back to Minister for Government Digital Services on a six-monthly basis. In phase two (2022-2025), once the Trust Framework has become officially established through the Bill discussed in this RIS, a Governance Board will be formally appointed through the standard Appointments and Honours process and will assume the monitoring and reporting duties. The dispute resolution process will be regularly assessed against the GCDR best practice framework assessment tool to help identity what is working well, areas for improvement and what to strive for.

In the interim, the Department will undertake surveys with focus groups and sector representatives (such as Digital Identity New Zealand) to assess how the establishment of the Trust Framework is impacting on trust in, and use of, digital identity services, and the development of the infrastructure needed for the ecosystem to effectively function. Potential metrics around the effectiveness of the Trust Framework could include use of digital identity services, and whether the digital infrastructure needed to support the ecosystem is in place. The Department will begin with a baseline survey before the Trust Framework Bill is established and comes into law in 2021 and will review stakeholder views annually thereafter.

Reporting requirements will be developed in regulations during phase two of the Trust Framework (2022-2025), which will focus on its formal establishment in legislation 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.

As the Trust Framework (and demand for accreditation) grows in the medium term, there is the potential to scale the governance and accreditation regime into a more comprehensive and separate organisation. The ongoing effectiveness of the public-service board, and the viability of alternative governance models (e.g. by the establishment of a Crown entity) would be reviewed two years after the implementation of the Trust Framework.