Hon Dr David Clark, Minister for the Digital Economy and Communications

Proactive release of Cabinet material about Detailed Policy for a Digital Identity Trust Framework Bill
14 May 2021

These documents have been proactively released:

17 February 2021, Cabinet Committee Minute of Decision: Digital Identity Trust Framework Bill: Detailed Policy Proposals;

19 February 2021, CAB-21-MIN-0022;

19 February 2021 Cabinet paper: Detailed Policy for a Digital Identity Trust Framework Bill; and

19 February 2021 Regulatory Impact Statement: D tailed policy for a Digital Identity Trust Framework

Some parts of this information release wou d not be appropriate to release and, if requested, would be withheld under the Official Informati n Act 1982 (the Act). Where this is the case, the relevant sections of the Act that would apply have been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Where information has b en withheld for other reasons consistent with advice, it has been annotated with an asterisk. This information may in some cases be accessible under the Official Information Act 1982.

Key to Redact on Codes:

- ***Sec ion 6(b)(i) - to prejudice the entrusting of information to the Government of New Zealand on a ba is of confidence by the Government of any other country or any agency of such a Government***

- **Section 9(2)(f)(iv) - maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials**

DEV-21-MIN-0006

Cabinet Economic Development Committee

Minute of Decision

Digital Identity Trust Framework Bill: Detailed Policy Proposals

Portfolio **Digital Economy and Communications**

On 17 February 2021, the Cabinet Economic Development Committee:

Background

1 **noted** that establishing a Digital Identity Trust Framework in legi lation is considered critical digital infrastructure for the digital economy, with ignificant benefits for individuals, the economy and society;

2 **agreed** that the purpose of the Trust Framework Bill be to:

2.1 promote the provision of secure and tr sted digital identity services that meet essential minimum requirements for security, privacy, identification management and interoperability;

2.2 support community resi ience and realise the wider benefits of digital identity;

Principles

3 **agreed** that the following principles (described in further detail in Appendix A to the paper under DEV-21-SUB-0006) will guide the activities and decision-making of the governance and accreditatio fun tions, and be included in the Trust Framework legislation:

3.1 pe ple centred: the rights and needs of people are paramount, though not to the exclusion of the needs of other entities in the digital identity ecosystem;

3.2 inclusive: everyone has the right to participate in the digital identity ecosystem;

3.3 secure: everyone has the right to expect that personal and organisational information will be stored, shared, and used in a secure manner within the digital identity ecosystem;

3.4 privacy-enabling: privacy is a critical enabler of trust in the digital identity ecosystem and everyone's privacy must be respected;

3.5 enabling of Te Ao Māori approaches to identity: the digital identity ecosystem is inclusive of Māori perspectives on identity and enables the needs and aspirations of Māori to be achieved;

3.6 sustainable: the digital identity ecosystem must be designed and maintained in a manner that supports its technical, social, and economic viability in the long-term;

3.7 interoperable: personal and organisational information should be able to be re-used across services, sectors and geographies, without security or privacy being undermined;

3.8 open and transparent: the digital identity ecosystem is maintained in an accessible, responsive and accountable manner;

Governance Board

4 **agreed** to establish a Governance Board (the Board) as a public service authority within a public service department, with the department nominated by the Prime Minister, and th Board directly accountable to the Minister for the Digital Economy and Communicat ons;

5 **agreed** that the Board must have appropriate knowledge and expertise in echno ogy, identity management, privacy, security and Te Ao Māori interests and participation;

6 **agreed** that members of the Board be appointed by the Chief Executive of the host department, who will have responsibility for ensuring th t the Board has the appropriate skills and experience;

7 **agreed** that the Board be required to seek the views of Treaty partners and the Office of the Privacy Commissioner, and others as directed by the M nister for the Digital Economy and Communications;

8 **agreed** that the Board have the power to appoint committees in order to advise on matters relating to its functions;

9 **agreed** that the purpose of the Board be to:

9.1 monitor the performance and effectiveness of all aspects of the Trust Framework;

9.2 update and am nd the Trust Framework as required to ensure its fitness for purpose and ongoing lignment with the purpose and principles of the Bill;

10 **agreed** that the functions of the Board be to:

10.1 maintain and update the Trust Framework's rules;

10 2 prov de procedures for the lodging of formal complaints;

0.3 undertake education and the publication of guidance;

10.4 any other responsibilities that may be conferred on it by the Minister for the Digital Economy and Communications;

11 **agreed** that the Board have the power to develop regulations for the approval of the Minister for the Digital Economy and Communications to submit to the Executive Council, regarding:

11.1 the rules and standards that make up the Trust Framework;

11.2 the levels of assurance that are required for different kinds of digital identity services;

11.3 the types of assessment (e.g. self-assessment, assessment by the Authority) that are required for different levels of assurance;

11.4 how often reassessment is required in different circumstances;

11.5 the creation of an infringement offences regime;

11.6 the certification requirements for third party assessors;

12 **agreed** that the Bill specify consultation requirements that must be met and approved by the Minister before any amendments can be made to the Trust Framework rules but that exceptions may be granted for technical or non-controversial amendments, or if the Minister determines that adequate consultation has already been undertaken;

Accreditation Authority

13 **agreed** to establish an accreditation authority (the Authority) within a public service department to assume full responsibility for the accreditation process and monitor compliance;

14 **agreed** that members of the Authority be appointed by the Ch ef Executive of the host department, who will have responsibility for ensuring that he Authority has the appropriate skills and experience;

15 **agreed** that the functions of the Authority be to:

15.1 administer the accreditation regime for Trust Framework participants;

15.2 establish and maintain a regist r of accredited Trust Framework participants;

15.3 investigate and take enforcement action in relation to breaches of the Trust Framework;

16 **agreed** that the powers of the Au hority be to:

16.1 accredit participants under the Trust Framework rules;

16.2 establish the pro edures and tests required for a Trust Framework participant to establish their compliance;

16.3 certify hird party accreditors (once governing regulations are established by the Board);

17 **agreed** that the Authority have the power to request the production of information and documents from Trust Framework participants for inspecting and auditing compliance with the Trust Framework (subordinate to existing statutory secrecy requirements);

18 **agreed** that the Authority have the power to enforce the Trust Framework's rules in the event of non-compliance, including:

18.1 issuing a private warning or reprimand to a Trust Framework participant;

18.2 making an order that a public warning or reprimand be issued to a Trust Framework participant;

18.3 imposing additional or more stringent record-keeping or reporting requirements in connection with Trust Framework standards and rules;

18.4 accreditation suspension or revocation;

18.5 making a compliance order requiring a Trust Framework participant to take any action that is necessary to restore it to a position of compliance;

19 **agreed in principle** that the Authority have the power to issue pecuniary penalties for non-compliance with the Trust Framework's rules, subject the development of the rules and the identification of conduct that will be subject to a penalty;

20 **agreed** that the regulations that allow for the certification of third-party accreditors will set out (amongst other matters) the processes and requirements (including monitoring and recertification requirements) that must be met to become an assessor;

Liability

21 **noted** that the Bill will establish liability provisions that set out how accredited participants will be liable for non-compliance with the Trust Framework rules, where h t non-compliance results in harm;

22 **noted** that during consultation, agencies expressed concerns that liabi ty provisions in the Bill could expose them to indeterminate liabilities and discou age participation in the Trust Framework;

23 **agreed in principle** to the establishment of a liability framework, subject to the development of the rules and an assessment of the potential risks to Trust Framework participants and impact on participation;

24 **noted** that final Cabinet approval will be sought to the establishment of a liability framework when the draft Bill is submitted to the Cabinet Legislative Design Committee in the second half of 2021;

Offences and penalties

25 **agreed** that offences be created r lating to:

25.1 knowingly o recklessly representing themselves as being an accredited participant of the Tru t Framework when they are not (with a maximum penalty of $50,000 for individ als nd $100,000 for organisations);

25.2 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);

25.3 accredited participants not updating information required by accreditation process (e.g. business address) (with a maximum penalty of $10,000 for individuals and $20,000 for organisations);

25.4 accredited participants 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);

25.5 obstructing the Authority, without reasonable excuse, in the exercise of their powers to require the provision of documents and information (with a maximum penalty of $10,000 for individuals and $20,000 for organisations);

Infringement offences regime

26 **agreed** that for infringement notices:

26.1 they be provided for through primary legislation and regulations (made under the provisions of the primary legislation by the Board);

26.2 the Authority will authorise enforcement officers to issue infringement notices;

26.3 standard procedures for challenging and enforcing an infringement notice will be available, by treating the identified offences as infringement offences for the purposes of section 21 of the Summary Proceedings Act 1957;

26.4 the infringement fees received will be paid to the Crown bank account, in order to remove the potential perception of infringement notices being used by the Authority as a funding mechanism;

27 **agreed** to the following maximums for infringement offences:

27.1 $3,000 infringement fee for bodies corporate and $1,000 infringement fee for individuals;

27.2 $9,000 fine for bodies corporate and $3,000 fine for individuals;

Financial implications

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

29 **agreed** to allow the Authority to recover costs through variable charging for accreditation;

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

Disputes resolution

31 **agreed** to establish a disputes resolution process to help:

31.1 ensure that participants can challenge any decisions around rule infringement;

31.2 the application of sanctions and liability issued in the administration of the accreditation regime;

Legislative implications

32 **invited** the Minister for the Digital Economy and Communications to issue drafting instructions to the Parliamentary Counsel Office for a Bill to give effect to the above paragraphs;

33 **authorised** the Minister for the Digital Economy and Communications, in consultation with the Minister of Internal Affairs as necessary, to decide minor policy and technical issues arising during drafting, that align with the overall policy intent, including possible amendments to legislation in the Internal Affairs portfolio;

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

35 **invited** the Minister for the Digital Economy and Communications to report back to the Cabinet Legislation Committee with the draft Bill in the second half of 2021.

Janine Harvey
Committee Secretary

Present:
Hon Grant Robertson (Chair)
Hon Dr Megan Woods
Hon Carmel Sepuloni
Hon David Parker
Hon Nanaia Mahuta
Hon Poto Williams
Hon Damien O'Connor
Hon Stuart Nash
Hon Kris Faafoi
Hon Willie Jackson
Hon Michael Wood
Hon Dr David Clark
Hon Dr Ayesha Verrall
Hon Meka Whaitiri
Hon Phil Twyford
Rino Tirikatene, MP
Deborah Russell, MP

Officials present from:
Office of the Prime Minister
Officials Committee for DEV

Hard-copy distribution:
Minister for the Digital Economy and Communications

CAB-21-MIN-0022

Cabinet

Minute of Decision

Report of the Cabinet Economic Development Committee: Period Ended 19 February 2021

On 22 February 2021, Cabinet made the following decisions on the work of the Cabinet Economic Development Committee for the period ended 19 February 2021:

[redacted] Out of Scope

[redacted] Out of Scope

[redacted] Out of Scope

[redacted] Out of Scope

[redacted] Out of Scope

DEV-21-MIN-0006 **Digital Identity Trust Framework Bill: Detailed Policy Proposals** CONFIRMED

Portfolio: Digital Economy and Communications

[redacted] Out of Scope

Michael Webster
Secretary of the Cabinet

Office of the Minister for the Digital Economy and Communications

Chair
Economic Development Committee

Detailed policy for a Digital Identity Trust Framework Bill

Proposal

1. A Digital Identity Trust Framework (Trust Framework) is part of critical digital infrastructure for the provision of secure, flexible and interoperable digital identity[1] services that are fit for the future. A Trust Framework sets and applies minimum requirements for security, privacy, identification management and interoperability through the accreditation of service providers.

2. This paper seeks Cabinet approval for the legal purpose, functions and powers of the accreditation and governance bodies for a statutory Trust Framework in New Zealand. It also proposes the establishment of legal mechanisms to deter and respond to non-compliance with the Trust Framework by accredited participants, cr minal offences to protect the integrity of the Trust Framework and provisions to recover the costs of accreditation and governance.

Relation to government priorities

3. Establishing a Trust Framework in New Zealand has wide support from both public and private sector stakeholders. It is essential to realising the social and economic opportunities and benefits associated with moving government and private sector services online. This was emphasis d d ring the COVID-19 pandemic when remote access to important services was essential for many New Zealanders. Modernising our approach to digital identity will prov de resilience to unexpected events and circumstances, by ensuring that peopl can still access essential services online.

4. Digital identity is also a foundational element for enabling the integration of services and digital transformation across government, as identified in Rautaki mō tētahi Rāngai Kāwanatanga Matih ko, the Strategy for a Digital Public Service.

Executive summary

There are regulator and operational gaps in the current digital identity ecosystem

5. Extensi e st keholder engagement[2] and research has highlighted issues with the curr nt dig tal identity ecosystem.[3] These include the inconsistent application of data, privacy identification and security standards as a contributing factor to privacy and security breaches. This has led to a loss of confidence in how government and private sector organisations handle personal information. It also contributes to a lack of trust and interoperability between public and private sector digital identity providers.

[1] Digital identity is the user-consented sharing of personal and organisational information online to access services and complete transactions.

[2] This includes regular engagement with public agencies, Crown agents and entities, private digital service providers, financial institutions and academic institutions.

[3] The digital identity ecosystem consists of the digital identity services that rely on relationships between individuals and service providers.

I propose establishing a Digital Identity Trust Framework to introduce minimum requirements that can be monitored and legally enforced

6. 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. Implementing a Trust Framework will support increased public trust (and uptake) of online services from both public and private sector providers and enable the wider use of trusted government information sources.

7. In July 2020, Cabinet agreed to a two-phased, parallel approach to developing and implementing the Trust Framework [CAB-20-MIN-0324 refers]:

   7.1 Phase 1: a rules development process to allow compliance testing of digital solutions and the development of legislation led by an interim cross-agency governance group; and

   7.2 Phase 2: the formal establishment of the Trust Framework in legislation.

The proposed Bill will establish the governance and accreditation functions n eded to support the Trust Framework

8. Establishing the Trust Framework as part of a statutory gove nance and compliance regime will promote consistency in the application of the rules and standards needed to ensure safe, secure and trusted digital identity services

9. To achieve this, I seek Cabinet agreement to issue drafting instructions for the Bill to enact a series of detailed policy proposals, including:

   9.1 a set of principles to guide the activities and decision-making of the governance and accreditation functions, inc uding: people-centred, inclusive, secure, privacy-enabling, enabling of Te Ao Māori pproaches to identity[4], sustainable, interoperable, and open and tra sparent;

   9.2 establishing a governance board within a public service department to update and maintain the Trust Fr mework;

   9.3 establishing an acc editation authority within a public service department to administer the accreditation regime and enforce compliance;

   9.4 allowing the accreditation authority to recover costs through variable charging for acc ed tation;

   9.5 establishing enforcement mechanisms that allow the accreditation authority to address non-compliance;

   9.6 establishing criminal offences to support the integrity of the Trust Framework;

   9.7 establishing a disputes resolution capability.

10. I am also seeking in-principle agreement to the development of pecuniary penalties and liability framework for non-compliance with the Trust Framework, subject to the development of the Trust Framework's rules and the assessment of potential risks.

[4] This principle was chosen over "Giving effect to Te Tiriti o Waitangi" because the Trust Framework will apply to private sector entities (who are not bound by the Treaty) as well as public sector organisations. For this reason, this principle seeks to ensure that the digital identity ecosystem as a whole is inclusive of Māori perspectives on identity and enables the needs and aspirations of Māori to be achieved. Compliance with the Treaty and the reflection of its values in the Trust Framework represents a key aspect of this principle.

11. As part of the development of the Trust Framework, officials are engaging with Māori as the Crown's Te Tiriti partner to embed Te Ao Māori and Te Tiriti o Waitangi perspectives and requirements into the Trust Framework and address the historic mistrust about the government misuse of Te Ao Māori data. Officials have met with Iwi and Māori representative organisations, post-settlement governance entities and other key Māori partners in order to address issues of inclusion and ensure that a partnership approach is taken. Officials will continue to work with Māori on the development of the rules.

Background

Why is digital identity important?

12. Digital identity is central to the secure, people-centred digital delivery of services such as social protection, health care and finance. Digital identity has the potential to deliver significant economic and societal benefits in both the public and private sectors and through commercial market development. It is an essential foundation fo individual and business participation in the digital economy and acces to government services. International studies have suggested that the potential benefit of enabling digital identity in a mature economy is between 0.5 per cen and 3 per cent of GDP (approximately $1.5 to $9 billion in NZD).[5]

13. Digital identity can also enable digital trade and other cr ss border transactions. Mutual recognition of digital identity services with Austra a has been signalled as a priority for the Single Economic Market agenda by the New Zealand and Australian Prime Ministers (in their annual Leaders' Meetings in 2019 and 2020). Another example involves the recently concluded D gital Economy Partnership Agreement (DEPA) between New Zealand, Chile and Singapore. The development of the Trust Framework Bill and its requirements for interoperability will enable New Zealand to advance discussions on digital identity in the DEPA and other contexts as appropriate.

14. Several government agencies also onsider that the development of the Trust Framework will complement and support ongoing policy work programmes, including the development of a 'consumer data right' for consumers to securely share data that is held about them with trusted third parties, with their consent. A well-functioning digital identity system would:

    14.1 reduce t e amount of data collected across government;

    14.2 suppo t public trust in the use of data across the ecosystem;

    14 3 supp rt public trust in the use of data across the ecosystem; and

    14 4 facilitate the use of data as a strategic asset across and beyond government.

[5] See McKinsey Digital's "Digital Identification: A Key to Inclusive Growth" (2019): https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth; World Economic Forum's "Reimagining Digital Identity: A Strategic Imperative" (2020): http://www3.weforum.org/docs/WEF_Digital_Identity_Strategic_Imperative.pdf. Australia Post has separately estimated that digital identity would be worth approximately 0.65 per cent of Australia's GDP – approximately $11 billion. In many of the countries reviewed the benefits were based on a more limited array of attributes than is being considered for digital identity in New Zealand.

Wide stakeholder engagement and research with individuals has been undertaken

15. Officials have worked with sector stakeholders and research bodies to gather a robust body of evidence to inform, develop and test proposals (including public agencies, Crown agents and entities, private digital service providers,[6] financial institutions[7] and academic institutions, such as the University of Auckland and the University of Otago). Engagement has been undertaken with iwi groups (including the Iwi Chairs Forum and the Data Iwi Leaders Group). Advice on Māori representation in the governance of the Trust Framework will be a priority in future engagement with iwi.

16. To support engagement, evidence gathering has also included research and surveys undertaken during 2019 and 2020 with a diverse range of private individuals, including Māori, Pasifika, older New Zealanders and people with disabilities. Qualitative rese rch has included interviews and focus groups to gauge public opinion and Māori perspectives on digital identity.

17. The proposals for the New Zealand Trust Framework follow closely, and lign with, the direction of the trust frameworks in comparable jurisdictions (i.e. Aus ralia, Canada and the UK). s6(b)(i) [redacted]

Regulatory and operational gaps have led to digital identity services developing in an unstructured and inconsistent way

18. The research identifies a number of regulatory and operational gaps in the provision of digital identity services in New Zealand. These include that New Zealand lacks consistently applied standards and processes for sharing personal and organisational information in a digital environment. As a result, systems and services have been developed in an unstructured and inconsisten way that creates inefficiencies, increases security and privacy r sks and hinders interoperability. This is undermining people's trust and confidence in digital identity services at a time when more and more transactions are taking place online, and the ability to share information digitally to assert one's iden ity is becoming increasingly vital to daily life and a key foundation for the economy.

Cabinet confirmed th deve opment of a statutory Trust Framework to address current regulatory and operational gaps

19. In July 2020 Cabinet agreed to the development of a Bill to establish the Trust Framewor in legislation [CAB-20-MIN-0324 refers]. In addition to the rules and s andards other key components of a Trust Framework include: a governance board, an accreditation regime, and mechanisms for enforcing the Trust Framework (including non-criminal enforcement mechanisms, offences and provisions for apportioning liability where damages are incurred).

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

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

The purpose and principles of the Bill

20. The purpose of the Bill is to promote the provision of secure, adaptable and trusted digital identity services that meet essential minimum requirements for security, privacy, identification management and interoperability; and to support community resilience and realise the wider benefits of digital identity.

21. In July 2020, Cabinet agreed that the Bill would include principles to guide the ongoing development and administration of the Trust Framework [CAB-20-MIN-0324 refers]. I recommend that these principles are: people-centred, inclusive, secure, privacy-enabling, enabling of Te Ao Māori approaches to identity, sustainable, interoperable, and open and transparent. A more detailed description of the principles and proposed key measures is provided at **Appendix A**.

Purpose, function, powers and form of the Governance Board

22. The purpose of the Governance Board (the Board) will be to:

    22.1 monitor the performance and effectiveness of all aspects of the Trust Framework; and

    22.2 update and amend the Trust Framework as required to ensure it is fit for purpose and ongoing alignment with its purpose and p nciples.

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

    23.1 maintaining and updating the Trust Framework's rules;

    23.2 providing procedures for the lodging of formal complaints;

    23.3 undertaking education and the publica on of guidance; and

    23.4 any other responsibilities that may be conferred on it by the Minister.

24. In order to perform these functions the Bill will provide the Board with the power to submit regulations to the Executive Council on approval by the Minister for the Digital Economy and Communic tions, including for the establishment of the rules and standards of the Trust Framework. A summary of these powers can be read in **Appendix B.** In arrying out its functions, the Board will be responsible to the Minister.

25. The Bill wil sp cify consultation requirements that must be met and approved by the Minister before any amendments can be made to the Trust Framework rules. Exceptions m y however be granted for technical or non-controversial amendments, or if he M nister determines that adequate consultation has already been undertaken.

I propose establishing the Board as a public service authority inside an existing department to keep responsibility for government information sources within the legal Crown

26. My preferred option for the legal form of the Board is the establishment of a public service authority. The public service authority - a board of public sector representatives - will be located within a public service department. The Prime Minister will nominate that department and the Board will be appointed by the Chief Executive of the nominated department. The Board will be directly accountable to the Minister for the Digital Economy and Communications.

27. I recommend that the Board be situated within the Crown. This is because the Trust Framework will involve the consented sharing of individual's data from trusted government and other information sources, such as from passports and citizenship [8] The relation of this data to core public services and the importance of utilising it in a safe and trusted manner makes the establishment of a public service authori the appropriate approach.

28. However, there is a risk that a Board where only public-sector rep esentatives have decision-making rights regarding the Trust Framework may be perceived as non-inclusive particularly by Treaty partners. Therefore, the Bill will establish that the Chief Executive must also ensure that the Board has appropri te knowledge and expertise in technology, identity and data management (particularly the ethical use of data), privacy, security and Te Ao Māori interests.

The Government Chief Digital Officer and the Department of Internal Affairs will work in partnership with Māori and other stakeholders to addr ss issues of inclusion in the Trust Framework

29. Officials are actively building the capability required to enable effective partnership with Māori. Partnering with Iwi and Mā ri organisations, post-settlement governance entities, other rūnanga and key Māori partners will ensure the Trust Framework is considerate of Te Ao Māori p rsp ctives of identity, will help increase trust and participation levels amongst Māori communities and meet the Crown's Treaty of Waitangi obligations To help achieve this in the near term, the interim governance board responsible for pproving the Trust Framework rules will include Te Pou Matihiko for Dig tal Public Services to ensure that the rules reflect Te Ao Māori perspectives

30. The Governmen 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 r lationship with Māori and to work in partnership in the development of the T ust Framework. The core of the engagement plan with Māori is the development of the Mana Ōrite relationship and agreement with the Data Iwi Leaders group.

[8] Note, the principle of consented-sharing of information under the Trust Framework does not restrict lawful sharing of information as allowed under existing statutes and approved information sharing agreements, and rule-making under the Trust Framework will address exceptions to this principle.

31. Mana Ōrite recognises the equal standing of each of the parties to the agreement and will underpin joint-work to ensure the digital needs and aspirations of Māori throughout Aotearoa New Zealand are more effectively met. Officials expect to formalise the Mana Ōrite agreement in the near future. Advice on Māori representation in the governance of the Trust Framework will be a priority in future engagement. The Bill will also require that Te Ao Māori perspectives and the Crown's Te Tiriti obligations to be incorporated into the design and maintenance of the Trust Framework.

32. To address issues of inclusion and to ensure that a partnership approach is taken where appropriate, I also recommend that the Board be required to seek the views of Treaty partners and the Office of the Privacy Commissioner, and others (including private sector interests) as directed by the Minister for the Digital Economy and Communications. I also recommend that the Board have the power to appoi t committees to advise the Board on matters relating to its functions.

33. As the Trust Framework (and demand for accreditation) grows in the medium term, there is the potential to scale the governance and accreditation r gime nto 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) will be reviewed two ye rs afte the implementation of the Trust Framework.

Purpose, function and powers of the Accreditation Authority

34. The purpose of the Accreditation Authority (the Au hority) is to assume responsibility for the accreditation process, including ongoing compliance testing. The Bill will allow the Prime Minister to establish the Authori y inside a public service department. The Authority will be appointed by the Chief Executive of the nominated department and be accountable to the Minister.

35. The functions of the Authority will include:

    35.1 administering the ccreditation regime for Trust Framework participants;

    35.2 establishing nd maintaining a register of accredited Trust Framework participan s; and

    35.3 inve tiga ing and taking enforcement action in relation to breaches of the Trust Framework and offences under the Bill.

36. As part of i s accreditation function, the Authority will have a range of powers neces ary to carry out its functions as outlined in **Appendix B**. These include being able to accredit participants to perform different tasks under the different levels of assurance outlined in the Trust Framework. Accredited participants will be recognised in public registries.

37. Trust Framework participants will be required to undergo regular reassessments to remain accredited. The Authority will have responsibility for establishing the procedures and tests for monitoring compliance. The Bill will also grant the Authority the power to require the provision of information and documents that the Authority may consider relevant to a participant's compliance with the Trust Framework. These powers will not override legal secrecy requirements around information held by public entities (e.g. such as the secrecy provisions in the Tax Administration Act).

The Bill will provide the Authority with the power to issue a range of penalties to Trust Framework participants

38. Enforcing compliance with the Trust Framework will be essential to ensuring the digital identity ecosystem remains functional, trustworthy and sustainable and that its rules and standards are consistently applied. Legal enforcement mechanisms will be used to remediate and/or sanction non-compliance by accredited parties and to discourage similar behaviour by other accredited parties. 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.

39. Therefore, I propose that the Authority will have the power to enforce compliance with the Trust Framework utilising a variety of mechanisms, including one or mo e of the following:

    39.1 issuing a private warning or reprimand to a Trust Framework part ipan ;

    39.2 making an order that a public warning or reprimand be issued to Trust Framework participant;

    39.3 imposing additional or more stringent record-keeping or reporting requirements in connection with Trust Framework standards and rules;

    39.4 suspension or revocation of a participant's ac redita ion; and

    39.5 making a compliance order requiring a par icipant to take any action that is necessary to restore it to a position of compli nce with the rules of the Trust Framework (with the threat of suspension or revocation of their accreditation if not met).

40. In addition to the penalties set out abov I support the establishment of a pecuniary penalties regime for non-compl ance with the Trust Framework's rules. However, as the rules are still in development, it is difficult to precisely determine what specific conduct could potentially be subject to a penalty. I therefore seek an in-principle decision to establish a pecuniary penalties regime, subject to the development of the rules and the identifica ion of conduct that will be subject to a penalty. Final approval of the establishment of a pecuniary penalties regime will be sought in time for when the draft Bill is submitted to the Cabinet Legislation Committee.

The requirements of compliance for participants will vary depending on the services and levels of a surance required by the Trust Framework

41. The application of the Authority's enforcement powers will be subordinate to legislative requirements and principles, both existing and in development, that will make up the Trust Framework. This includes the principles of the Privacy Act, including Principle 8, which states that agencies take reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading during use and disclosure.

42. The Trust Framework rules will set out different assurance requirements for different services. Higher risk transactions require a greater degree of certainty regarding information because of the potentially significant consequences. However, there is little point in setting and enforcing standards that require every transaction to meet a high level of assurance, as this is not needed and would impose unnecessary costs on ecosystem participants.

The Bill will establish a disputes resolution process to settle disputes regarding the Trust Framework

43. Disputes are damaging, expensive and time consuming, which can increase the costs of administering the Trust Framework and disincentivise participation. I therefore propose that the Bill also establish a disputes resolution process.

44. The objective of this process will be to provide a consistent, structured, equitable, cost effective and timely process that all trust framework participants can have confidence in that:

    44.1 helps to maintain the integrity of the rules and the trust framework;

    44.2 provides access to a dispute resolution process to enable the identification a d resolution of differences interpretation of rules between participants and users;

    44.3 resolve disputes between participants and accreditation authority decisions

    44.4 enable participants to implement remediation plans for unintentional noncompliance with the rules;

    44.5 address potential power imbalance between participants;

    44.6 provide advice on the interpretation of the rules; nd

    44.7 resolve issues associated with trust framework participants exiting the scheme.

45. I anticipate disputes could include:

    45.1 user dissatisfaction with service received from an accredited participant; and

    45.2 participant seeking to assign liability to another for a matter that has led to the first participant being penalised under he Trust Framework.

46. Officials will work with the Ministry of Business, Innovation and Employment's Government Centre for Dispute Resolution (GCDR) and the Ministry of Justice to design the disputes resolution regime to ensure it is appropriate for the Trust Framework as its rules and standards are developed. The disputes resolution process will be based on prin iples that will work to ensure natural justice, including the GCDR's best practice principles and standards. Officials will also work with existing regulators, and ompl ints and disputes resolution bodies to ensure that where their responsibilities might overlap there are processes to ensure that cases are referred to the most app opriate body.

47. The Bill wi l allow the Minister for the Digital Economy and Communications to e tablish the different types of process that may be used as a part of the disputes resolution regime (e.g. mediation, arbitration etc.).

The Bill will allow the Authority to certify third party assessors if required

48. As the Trust Framework matures, it is possible that a single department will not have the capacity to meet rising demands for accreditation. Independent third-party assessors would allow for more accreditations to be undertaken. It is proposed that the Bill include regulation-making powers that allow for the certification of third-party accreditors. These regulations will set out (amongst other matters) the processes and requirements (including monitoring and recertification requirements) to becoming an assessor.

Liability provisions

49. Digital service providers have an interest in clearly understanding the risk of legal liability that flows from their participation in the Trust Framework, and how they may mitigate this risk. In particular, members of a digital identity ecosystem are likely to be concerned about fault-based civil liability (i.e. responsibility for a loss suffered by one party that is shifted to another due to their being in some way responsible for the loss). For example, identity providers may worry that if they issue an incorrect credential, and reliance on that incorrect data results in significant damage to a relying party (e.g. a bank issuing a loan), the identity provider may be liable for the damages

50. Currently, the question of whether a duty of care exists between an issuer of a dig tal credential, for example, is difficult to assess and would likely need to be determined by the courts on a case by case basis.

51. My intention is that the Bill will establish the circumstances where a Trust Framework participant is liable for harms resulting from non-compliance with the T ust Framework's rules. However, during consultation agencies including t e Inland Revenue Department and the Ministry of Education expressed concerns about the potential for liability provisions to leave them vulnerable to new and indeterminate liabilities, and the importance of better understand its potential impact on participation in the Trust Framework.

52. To ensure that the desired outcomes of a liability fr mew rk are achieved, I consider it is necessary to finalise the liability regime in conjunction with the development of the rules (including different categories and levels of a creditation) of the Trust Framework. I am therefore seeking an in-principle decision to the establishment of a liability framework for harms resulting from non-compliance with the Trust Framework's rules. Officials will review the potential risks for agencies and wider participation in the Trust Framework and depending on the outcome of this work, seek final approval in time for when the draft Bill is submitted to the Cabinet Legislative Committee.

Offences

53. A range of offences are proposed to be included in the Bill in order to support the integrity of the Trust F amework and to punish bad actors. It is proposed that offences be created rel ting to a person or entity:

    53.1 knowi gly or recklessly representing themselves as being an accredited parti ipant of the Trust Framework when they are not (maximum penalty of $50 000 for individuals and $100,000 for organisations);

    53.2 knowingly or recklessly supplying to the Authority any false or misleading information for the purposes of any application for accreditation to the Trust Framework (maximum penalty of $50,000 for individuals and $100,000 for organisations);

53.3 not updating information required under the accreditation process (e.g. business address) (maximum penalty of $10,000 for individuals and $20,000 for organisations);

53.4 not informing the Authority of other significant matters (e.g. prior criminal convictions) (maximum penalty of $10,000 for individuals and $20,000 for organisations); and

53.5 without reasonable excuse, obstructing the Authority in the exercise of their powers to require the provision of documents and information (maximum penalty of $10,000 for individuals and $20,000 for organisations).

54. It should be noted that the offences outlined above will not apply to participants that are within the legal Crown (in line with the guidance set out in Cabinet Office Circula CO (02) 4). It is generally considered unlikely that agencies will be non-comp ant w th the proposed offences, and in any case it is considered that criminal liability is ot necessary when factors such as accountability to Ministers and Parliam t already provide a strong incentive to comply.

The Bill will include both offences and an infringement offences regime

55. I also propose to create an infringement scheme to help fill he gap between low level interventions (e.g. guidance) and prosecution. The scheme will provide a mechanism for the Authority to address behaviours that are at the lower levels of offending (e.g. unintentional offending such as advertising as b ing rust Framework compliant when unaware that accreditation is required to do so).

56. For infringement notices:

56.1 the Board would have regulati n-making powers to set the fines for each infringement offence;

56.2 the Authority will authorise enfo cement officers to issue infringement notices;

56.3 standard procedures for challenging and enforcing an infringement notice will be available, by reating the identified offences as infringement offences for the purposes of sec ion 21 of the Summary Proceedings Act 1957; and

56.4 the infringemen fees received will be paid to the Crown bank account, in order to remove t e potential perception of infringement notices being used by the Authority s a funding mechanism.

57. Generally, for infringement offences:

5 .1 he infringement fee ($1,000) is set in primary legislation, with the conduct of the infringement offence set in regulations; and

57.2 a corresponding maximum infringement fine is set in primary legislation. This fine is available should the matter go before the court by way of a defended hearing, due to an unpaid infringement fee, or by the prosecution laying a charging document. The maximum fine for each infringement offence will be set in regulations.

58. The proposed maximums below take into account the harm (potential or actual) from the offending, the target group, consistency with other legislation, and proportionality. I propose the following maximums for infringement offences:

    58.1 $3,000 infringement fee for bodies corporate and $1,000 infringement fee for individuals; and

    58.2 $9,000 fine for bodies corporate and $3,000 fine for individuals.

59. The levels of harm, affordability and appropriateness for the target group, and proportionality have also been factored in when considering the proposed maximum fine. For these reasons, I propose different maximums for bodies corporate and individuals.

Outlining operational decisions for supporting digital identity transformation, including system-wide investment options

60. Currently the main way people can assert their identity online is throug the government provided RealMe service. RealMe is a centralised model f 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

61. Under the Trust Framework the Department can continue to operate RealMe services, which comes within the Minister of Internal Affairs' portfo io responsibilities, alongside developing the Bill. Once the Trust Framework is in pla e we will seek to accredit RealMe services. For the RealMe Identity Verification Service (RealMe IVS) component, this may require amending the Electronic Identity Verification Act 2012 that governs this service.

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

Financial implications

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

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

64. These cost estimates assume that the Authority could carry out up to 100 standard accreditations or 25 complex accreditations in a year.[9] The Authority will consist of four to five full time equivalent staff. s6(b)(i) [redacted]

[9] It is assumed that each accreditation will have different requirements. Standard accreditations are expected to move quickly for tested systems such as the RealMe services. Complex accreditations are assumed to be for new technology that is untested and requires significantly more time and expertise to assess. It is unclear at this stage which accreditations are likely to be more prevalent.

65. The costs include the cost of the Board, the team that develops and updates the Trust Framework rules and the Authority. They will be based within an existing government department, supporting and accrediting potential Trust Framework participants, providing governance and developing and supporting operational policies.

The Bill will provide the Authority with the power to set a variable charging scheme to recover costs

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

67. It is therefore proposed that the Bill include regulation-making powers that all w the Authority to recover costs of accreditation services. Three options were onsidered for recovering costs:

    67.1 Option 1: a fixed charge scheme;

    67.2 Option 2: a variable charge scheme (i.e. to charge app icants based on the number of hours spent on an accreditation); or

    67.3 Option 3: a levy.

68. I recommend that the Bill allow for the Authority to cost-recover through the creation of a variable charge scheme. This approach is prefe red over charging a flat fee for accreditation services. A flat fee is more transparent to potential applicants and simpler to administer for the Author ty. However, it is unlikely to be able to equitably account for the differences in the individual ci cumstances of applicants, the roles and levels of assurance that can be ccredited for, and the costs of assessing and testing respective IT systems and capabi ty A variable charging scheme will allow for a more accurate reflection of the costs of delivering the accreditation service to participants.

A Trust Framework has many aspects of a public good and officials will investigate how best to fund those act vities

69. Setting fees equires f nding a balance between recovering costs and ensuring that services a e incl sive, and regulations are not overly burdensome. Setting fees for accreditatio too high may suppress demand and increase exclusion, working against the Trust F amework's principles. Officials will work with a group of service providers over the next year to review the Trust Framework rules and the likely costs of compliance as part of the development of Trust Framework rules.

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

Legislative implications

71. If the recommendations in this paper are accepted, I will direct the Department of Internal Affairs to issue drafting instructions for the Bill to enact the detailed policy proposals outlined in this paper.

72. I seek authority for myself, in consultation with the Minister of Internal Affairs as necessary, to decide policy issues arising during drafting, including possible amendments to legislation in the Internal Affairs portfolio. It is not currently intended that the Trust Framework Bill will replace or supersede the Electronic Identity Verification Act 2012 (the EIV Act), though amendments may be required to ensure that RealMe can operate on an equal footing with other Trust Framework participants (e.g. the EIV Act currently requires that all relying parties for RealMe are approved by Cabinet).

73. The alignment of the EIV Act with the Trust Framework Bill, and the potential need for consequential amendments, is currently being assessed by officials. Officials will also consider potential alignment with other areas of legal reform, such as the development of new data and statistics legislation by Stats NZ.

74. The Board will have the power to submit regulations to the Executive Council, on the approval of the Minister for the Digital Economy and Communications Thi ncludes regulations for Trust Framework rules, which will specify the roles p ocesses and standards for accredited participants to abide by. For governmen agen ies, this will formalise the assessment of recommended and mandated standards and will not impact on existing legislative or regulatory requirements.

75. s9(2)(f)(iv) The Bill will create a standalone Act to provide for the Digital Identity Tr st Framework.

Impact analysis

Regulatory Impact Statement

76. The Regulatory Impact Analysis requirements apply to the proposals in this paper and a Regulatory Impact Statement (RIS) has been prepared and is attached. The Regulatory Impact Analysis qual ty assurance panel at the Department of Internal Affairs has reviewed the RIS. The panel considers that the information and analysis summarised in the RIA pa tially meets the quality assurance criteria.

77. There is uncertainty abou 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 nd inc udes 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.

Climate Implications of Policy Assessment

78. There are no climate implications from this paper. However, I note that supporting the secure and trusted delivery of services online is likely to positively impact the resources required to access and deliver in-person services.

Human Rights

79. There are no immediate impacts on human rights arising from the proposal outlined in this paper as all information sharing requires user consent. I know that as our digital identity ecosystem evolves it will provide a variety of benefits, particularly for New Zealanders who may struggle with proving who they are online and in the real world. However, these may be inequitably realised due to levels of digital inclusion across different population groups in New Zealand.

80. Therefore, it is important that the proposal is implemented in alignment with ongoing work to improve digital inclusion across government and to support Article 21 of the Universal Declaration of Human Rights (everyone has the right of equal access to public service in their country). This means ensuring accessibility for disabled people, refugees and migrants, and that indigenous rights, data sovereignty and the principles of the te Tiriti o Waitangi are consistently upheld. The design of the proposed Trust Framework and surrounding ecosystem will also allow for alternative channels for proofing identity to be available to those who cannot or choose not to participate.

81. There is also the opportunity for disabled people to benefit from the development f the Trust Framework. Accessibility will need to be considered in the development of the Trust Framework as well as considering representatives from the disabled community in advisory groups and governance mechanisms.

Consultation

82. The Department of Internal Affairs consulted with the Accident Compen atio Corporation, New Zealand Customers Service, Department of Correct ns, Ministry of Education, National Cyber Security Centre, Ministry of Health, Inland Revenue Department, Ministry of Justice, Land Information New Zealand Ministry of Business, Innovation and Employment, Ministry of Foreign Affairs and Trade, Ministry for Primary Industries, Ministry of Social Development, New Zealand Transport Agency, Office of the Privacy Commissioner, Oranga Tamari i, Social Wellbeing Agency, Public Service Commission, Stats NZ, Te Arawhiti, Te Puni Kōkiri the Legislative Design Advisory Committee and the Treasury. The Depar ment of Internal Affairs informed the Policy Advisory Group at the Department of the Prime Minister and Cabinet.

83. I am committed to ensuring that the constructive dialogue with stakeholders and agencies remains a key feature of the development of the exposure draft and the Trust Framework's rules and standards. This will include working with agencies to identify legislative implications, co-devel ping implementation plans and sharing findings to avoid potential duplication in efforts (e.g. developing data standards with Stats NZ). This will include the involvement of representatives from the GCDO, the Government Chief Information Security Officer, the Government Chief Data Steward, the Office of the Privacy Commissione and Te Pou Matihiko for Digital Public Services on the rules development pr gramme.

84. Officials have also regularly engaged with the GCDO's digital inclusion workstream to ensure lignment with the Trust Framework. This engagement will continue throughou its development and implementation to ensure that all New Zealanders will be able to access essential goods and services under a Trust Framework.

I recommend the release of an exposure draft of the Bill for public consultation

85. While officials have undertaken extensive targeted stakeholder engagement with both organisations and individuals, the policy proposals for the Bill have not been publicly released for wider consultation. Given the public interest in the security and privacy of digitised personal information, I seek Cabinet authority to release an exposure draft of the Bill.

86. The exposure draft will provide the public with the opportunity to comment on whether the Bill gives appropriate effect to the policy proposals discussed in this paper (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.

87. If Cabinet agrees, the exposure draft will be released prior to returning to the Cabinet Legislation Committee in 2021. Officials will also have the opportunity to consult with the public on the privacy, security and information management rules under the Tr st Framework through the rules development programme.

Communications

88. I intend to make a public announcement on the Digital Identity Trust Framework if Cabinet agrees to the policy proposals in this paper.

89. As per Cabinet Office Circular CO (18) 4: Proactive Release of Cabinet Material – Updated Requirements, this Cabinet paper will be proactively rel ased ubject to any redactions that may be warranted under the Official Information Act 1982.

Recommendations

90. The Minister for the Digital Economy and Communications recommends that the Cabinet Business Committee:

1. **note** that establishing a Digital Identity Trust Framework in legislation is considered critical digital infrastructure for the digital economy with significant benefits for individuals, the economy and society;

2. **agree** that the purpose of the Trust Framework Bill will be to promote the provision of secure and trusted digital identity services that meet essential minimum requirements for security, privacy, identification management and interoperability; and to support community resilience and realise the wider benefits of digital identity;

Principles

3. **agree** that the following principles (described in further detail in **Appe dix A**) will guide the activities and decision-making of the governance and accreditation functions, and be included in the Trust Framework legislation:

3.1 people-centred - the rights and needs of people are pa amount, though not to the exclusion of the needs of other entit e in the digital identity ecosystem;

3.2 inclusive - everyone has the right to pa ticipate in the digital identity ecosystem;

3.3 secure - everyone has the right to expect that personal and organisational information will be stored, shared, and used in a secure manner within the digital identity ecosystem;

3.4 privacy-enabling - privacy s a crit cal enabler of trust in the digital identity ecosystem and eve yone's privacy must be respected;

3.5 enabling of Te Ao Māori approaches to identity - the digital identity ecosystem is inclusive of Māori perspectives on identity and enables the needs nd aspirations of Māori to be achieved;

3.6 sustainable - the digital identity ecosystem must be designed and ma ntained in a manner that supports its technical, social, and economic v abili y in the long-term;

3.7 interoperable - personal and organisational information should be able to be re-used across services, sectors and geographies, without security or privacy being undermined; and

3.8 open and transparent - the digital identity ecosystem is maintained in an accessible, responsive and accountable manner;

Governance Board

4. **agree** to establish the Governance Board (the Board) as a public service authority within a public service department, with the department nominated by the Prime Minister, and the Board directly accountable to the Minister for the Digital Economy and Communications;

5. **agree** that the Board must have appropriate knowledge and expertise in technology, identity management, privacy, security and Te Ao Māori interests and participation;

6. **agree** that members of the Board will be appointed by the Chief Executive of the host department, who will have responsibility for ensuring that the Board has the appropriate skills and experience;

7. **agree** that the Board will be required to seek the views of Treaty partners and the Office of the Privacy Commissioner, and others as directed by the Minister for the Digital Economy and Communications;

8. **agree** that the Board will have the power to appoint committees in order to advise on matters relating to its functions;

9. **agree** that the purpose of the Board will be to:

   9.1 monitor the performance and effectiveness of all aspects of the Trust Framework; and

   9.2 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;

10. **agree** that the functions of the Board will be to:

   10.1 maintain and update the Trust Framework's rules;

   10.2 provide procedures for the lodging of formal complaints;

   10.3 undertake education and the publication of guidance; and

   10.4 any other responsibilities that may be conferred on it by the Minister for the Digital Economy and Communications;

11. **agree** that the Board will have the power to submit regulations to the Executive Council, on the approval of the Minister for the Digital Economy and Communications, regarding:

   11.1 the rules and standards that make up the Trust Framework;

   11.2 the levels of assurance that are required for different kinds of digital identity services;

   11.3 the types of assessment (e.g. self-assessment, assessment by the Authority) that are required for different levels of assurance;

   11.4 how often reassessment is required in different circumstances;

   11.5 the creation of an infringement offences regime; and

   11.6 the certification requirements for third party assessors;

12. **agree** that the Bill specify consultation requirements that must be met and approved by the Minister before any amendments can be made to the Trust Framework rules but that exceptions may be granted for technical or non-controversial amendments, or if the Minister determines that adequate consultation has already been undertaken;

Accreditation Authority

13. **agree** to establish an accreditation authority (the Authority) within a public service department to assume full responsibility for the accreditation process and monitor compliance;

14. **agree** that members of the Authority will be appointed by the Chief Executive of the host department, who will have responsibility for ensuring that the Authority has the appropriate skills and experience;

15. **agree** that the functions of the Authority are to:

15.1 administer the accreditation regime for Trust Framework participants;

15.2 establish and maintain a register of accredited Trust Framework participants; and

15.3 investigate and take enforcement action in relation to breaches of the Trust Framework;

16. **agree** that the powers of the Authority are to:

16.1 accredit participants under the Trust Framework rules;

16.2 establish the procedures and tests required for a Trust Framework participant to establish their compliance;

16.3 certify third party accreditors (once governing regulations are established by the Board);

17. **agree** that the Authority has the power to request the production of inf rmation and documents from Trust Framework participants for inspecting and auditing compliance with the Trust Framework (subordinate to existing tatutory secrecy requirements);

18. **agree** that the authority has the power to enforce the Trust Fr mework's rules in the event of non-compliance, including:

18.1 issuing a private warning or reprimand to a Trust Framework participant;

18.2 making an order that a public warning or rep mand be issued to a Trust Framework participant;

18.3 imposing additional or more stringent ecord-keeping or reporting requirements in connection wi h Trust Framework standards and rules;

18.4 accreditation suspension or revocation; and

18.5 making a complian e order requiring a Trust Framework participant to take any action tha is ne essary to restore it to a position of compliance;

19. **agree in-principle** that the authority has the power to issue pecuniary penalties for non-complianc with the Trust Framework's rules, subject the development of the rules and the identification of conduct that will be subject to a penalty.

20. **agree** that the regulations that allow for the certification of third-party accreditors will et out (amongst other matters) the processes and requirements (including monitoring and recertification requirements) that must be met to b come an assessor;

L ability

21. **note** my intention that the Bill will establish liability provisions that set out how accredited participants will be liable for non-compliance with the Trust Framework rules, where that non-compliance results in harm;

22. **note** that during consultation, agencies expressed concerns that liability provisions in the Bill could expose them to indeterminate liabilities and discourage participation in the Trust Framework;

23. **agree in-principle** to the establishment of a liability framework, subject to the development of the rules and an assessment of the potential risks to Trust Framework participants and impact on participation;

24. **note** I will seek final Cabinet approval on the establishment of a liability framework when the draft Bill is submitted to the Cabinet Legislative Design Committee in the second half of 2021;

Offences and penalties

25. **agree** that offences are created relating to:

    25.1 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);

    25.2 knowingly or recklessly supplying to the Authority any false or misleadin 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);

    25.3 accredited participants not updating information required by accreditation process (e.g. business address) (with a maximum penalty of $10,000 for individuals and $20,000 for organisation);

    25.4 accredited participants 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 organisa ions); and

    25.5 obstructing the authority, without reasonable excuse, in the exercise of their powers to require the provision o documents and information (with a maximum penalty of $10,000 for ndividuals and $20,000 for organisations);

Infringement Offences Regime

26. **agree** that for infringement notices:

    26.1 that they be provided for through primary legislation and regulations (made under the pr visions of the primary legislation by the Board);

    26.2 the Authority will authorise enforcement officers to issue infringement notices;

    26.3 standard procedures for challenging and enforcing an infringement notice wil be available, by treating the identified offences as infringement offences for the purposes of section 21 of the Summary Proceedings Act 1957; and

    26.4 the infringement fees received will be paid to the Crown bank account, in order to remove the potential perception of infringement notices being used by the Authority as a funding mechanism;

27. **Agree** to the following maximums for infringement offences:

    27.1 $3,000 infringement fee for bodies corporate and $1,000 infringement fee for individuals; and

    27.2 $9,000 fine for bodies corporate and $3,000 fine for individuals;

Financial implications

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

29. **agree** to allow the Authority to recover costs through variable charging for accreditation;

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

Disputes resolution

31. **agree** to establish a disputes resolution process to help ensure that participants can challenge any decisions around rule infringement and the application of sanctions and liability issued in the administration of the accreditation regime;

Legislation

32. **invite** the Department of Internal Affairs to issue drafting instructions to the Parliamentary Counsel Office for a Bill that gives effect to the above policy directions;

33. **authorise** the Minister for the Digital Economy and Communications, i consultation with the Minister of Internal Affairs as necessary, to decide minor policy and technical issues arising during drafting, that align with the overall policy intent, including possible amendments to legislation in the Internal Affairs portfolio;

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

35. **invite** the Minister for the Digital Economy and Communications to report back to the Cabinet Legislation Committee with the draft Bill the second half of 2021.

Authorised for lodgement

Hon Dr David Clark
Minister for the Digita Economy and Communications

Appendix A: Trust Framework Principles

People-centred

The rights and needs of people are paramount, though not to the exclusion of the needs of other entities in the digital identity ecosystem.

Key measures

- People's participation in the digital identity ecosystem is on a voluntary basis, with the right to opt-out without penalty.
- Digital identity services are convenient and straightforward for people to use.
- People retain control over their information in line with legislative requirements, including the Privacy Act.

Inclusive

Everyone has the right to participate in the digital identity ecosystem.

Key measures

- The digital identity ecosystem can reflect the needs and requirements of a broad range of stakeholders.
- Barriers to participation in the digital identity ecosystem–whether they be social, financial, or technical–are minimised, without compromising security or privacy.
- Everyone is able to use digital identity services without risk of discrimination or exclusion.

Secure

Everyone has the right to expect that personal and organisational information will be stored, shared, and used in a secure manner within the digital identity ecosystem.

Key measures

- Systems and services are designed with the security of information in mind.
- Technology design, operational controls and regulations governing the use of personal and organisational information safeguard it from breaches, corruption or loss.

Privacy-enabling

Privacy is a critical enabler of trust in the digital identity ecosystem and everyone's privacy must be respected.

Key measures

- Approaches to privacy are proactive and preventative, rather than reactive and remedial.
- Privacy is embedded into the design and maintenance of systems and services, by default.
- There are no gaps in either protection or accountability–privacy is continuously protected across the ecosystem.
- Obligations are being met regarding the legislative requirements of the Privacy Act.

Enabling of Te Ao Māori approaches to identity

The digital identity ecosystem is inclusive of Māori perspectives on identity and enables the needs and aspirations of Māori to be achieved.

Key measures

- Māori participate equitably in the digital identity ecosystem.
- Māori perspectives and approaches to identity are enabled by the digital identity ecosystem.
- The digital identity ecosystem is developed and maintained in partnership with Māori.
- Māori are supported in leadership and decision-making roles to ensure Māori perspectives about data and identity are embedded in the trusted digital identity ecosystem.

Sustainable

The digital identity ecosystem must be designed and maintained in a manner that supports its technical, social, and economic viability in the long-term.

Key measures

- The digital identity ecosystem generates value (e.g. social, eco omi , fiscal) for those involved.
- Systems and services are sufficiently flexible to adapt o change (e.g. social licence, government priorities, emerging technologies, reg latory developments) and support innovation.
- Systems and services are scalable (i.e able to be altered in size) in order to enable people-centred outcomes.

Interoperable

Personal and organisational information sh uld be able to be re-used across services, sectors and geographies, without security or privacy being undermined.

Key measures

- Common approaches (e.g. pen standards, frameworks, best practice guidelines) are employed to ensu e con istency and facilitate interoperability, both nationally and internationally.
- Barriers (e g. prop iety technology) to interoperability or the portability of personal and organi ation l information are minimised.
- Co sultati n and collaboration occur between the public sector, private sector, Treaty partners, the wider community, and international partners to identify and address interoperability issues.

Open and transparent

The digital identity ecosystem is maintained in an accessible, responsive and accountable manner.

Key measures

- It is clear how personal and organisational information is being stored, used and shared, and for what purpose.
- The rules and standards governing the digital identity ecosystem are available to all.
- Government is accountable to the public for its role in the digital identity ecosystem.

Appendix B: Summary of the purpose, functions and powers of the Governance Board and the Accreditation Author ty

Governance Board	**Accreditation Authority**
Purpose: • To monitor the performance and effectiveness of all aspects of the Trust Framework. • To ensure the Trust Framework's fitness for purpose, and ongoing alignment with the Trust Framework principles.	Purpose: • To assume full responsibility for th acc ditation process and monitor compliance.
Functions: • Creating and updating the Trust Framework's rules. • Providing procedures for the lodging of complaints. • Undertaking market facilitation measures (e.g. education, publication of guidelines). • Carrying out such other functions and responsibilities that may be conferred on it by the Minister (e.g. investigating a particular issue on the Minister's request).	Functions: • Administering the acc editation regime for Trust Framework participants. • Establishing a d maintaining a register of accredited Trust Framework participants. • Investigati g and tak ng enforcement action in relation to breaches of the Trust Framework
Powers: • Establishing (in regulations made by Order in Council with the approval of the Minister for the Digital Economy and Communications): ○ the rules and standards that make up the Tru t Framework; ○ what levels of assurance are required fo differ nt kinds of digital identity services; ○ what kinds of assessment (e.g. se f-a sessment, assessment by the Authority) ar re ui ed for different levels of assurance; ○ how often reassessmen is required in different circumstances;	P we s: • Accrediting participants to different tasks (e.g. information providers, infrastructure providers). • Establishing the procedures and tests required for a Trust Framework participant to establish their compliance. • Certifying third party accreditors (once governing regulations are established by the Governance Board). • Requiring the provision of information and documents that the Authority may consider relevant to a participant's compliance with the Trust Framework (subject to confidentiality and secrecy provisions in existing statutes) • Powers for enforcing the Trust Framework's rules in the event of non-compliance, including: ○ issuing public warnings; ○ imposing additional record-keeping or reporting requirements;

○ fines for infringement offences; and ○ the certification requirements for third party assessors. • To appoint committees in order to advise the Governance bodies on matters relating to its functions.	○ accreditation suspension or revocat on; ○ making compliance orders to take any act on that is necessary to restore compliance with the Trust Framework; and ○ issuing infringement notices a d offences against the Act. • Power to set variable charges for the co t of accreditation to the Trust Framework.

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) [redacted] 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 r 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 'digit l 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 informat on and consent to share it using a digital platform (e.g. RealMe); and
- **relying parties** who use the trusted personal and organisatio al information supplied by infrastructure providers to provide services (e.g. bank , government, telecommunications, health providers, and providers of age restricted se vices such as liquor stores).

Currently the main way people can assert their identity o line 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 th re 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 Zeal nd 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 regula ory fr mework 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 g vernment work programmes. These include the GCDO's digital inclusion workstream, he 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 rust ramework participants and between Trust Framework participants and users need to be resolved efficiently and effectively and in a timely manner. This is becaus 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 se vices could provide.

Our understanding of these issues has been informed by significant sta eholder 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 inter iew and focus groups to gauge public opinion and Māori perspectives on digital identity Q antitative 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 t ust 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 activi ies

In one survey, almost a quarter of those who had used government services stated that they had personal information l aked 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 c nfidence in the digital identity ecosystem further and slowing adoption.

Research with ect stakeholders also tells us that trust depends on the perceived motivation of th 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 efficien ies (e g. less duplication); improved record keeping increased confidence to inves in digital solutions; increased opportunities to break down information silos between business units and government agencies; improved ability to detect and dete security or privacy breaches of personal and organisational information; imp oved digital inclusion; greater trans-Tasman alignment; and
- society – for example, greater interoperability between p rticipants in the trusted digital identity ecosystem; clear and consistent ules 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 standard for its participants, the Trust Framework will bring coherence to digital identity serv ces across government and for any third parties wishing to engage with government on digita identity services. This will enable multiple parties to participate in a safe and trusted way.

Digital identity can also en ble digital trade and other cross-border transactions. The development of the digital identity ecosystem and interoperability will enable New Zealand to advance discussions n digital identity in a variety of different jurisdictions. One example is the New Zealand a d Australian Prime Ministers' commitment to mutual recognition of identity services between Australia and New Zealand. There is also potential for ongoing alignment with Ca ada 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 Accr ditation 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 o 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 hos department. However, the Public Service Commission subsequently advised of cials 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 R S. The purpose of the Governance Board will be:

- to monitor the p rformance 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 nd 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. im igration, passports etc.) and the effective guardianship of this information is essential to reta ning 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. Gi en Māori are Treaty partners, there is a pressing need for the Governance Board to e tablish an enduring relationship with Māori and to work in partnership in the d velopment 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 p rspect ves. To further address issues of inclusion and to ensure that a partner hip approach is taken where appropriate, the Bill will also require that the Board be requ red o 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-base 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 departm nt. The Authority will be appointed by the Chief Executive of the nominated departmen 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 b 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 po ential 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 abo t their roles and activities under the Trust Framework expediently and at a low cost. his 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 p blic and private stakeholders such as the Ministry of Health, ACC and ANZ Bank when t e ne d 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 accreditati n. 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 Depa tment will prepare a separate Cost Recovery Impact Statement once the accreditation p ocess 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 n n-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 accred tat on would apply to public service entities due to the inefficiencies of government charging go ernment.

However, The Trust Framework itself has many aspects that make t 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 whil it is possible to exclude entities from accessing the Trust Framework rules, there are s rong policy reasons for making them publicly available.

Wider accreditation of digital identity services will esult 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 nteroperable 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 Z aland communities through the removal of current barriers to the access of goods and services digitally.

The World Bank has stated that dentification should be treated as a public good, provided to facilitate the rights and inclu ion 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 developmen , maintenance and enforcement of the Trust Framework itself should be funded through general taxation rather than accreditation fees. s9(2)(f)(iv) [redacted]

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 on line 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 teroperability 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 cu tural differences; and
- government to be able to deliver improved and efficient public se vices 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 o responsibility undermines trust in the digital identity ecosystem there are (statutory a d non-statutory) processes in place to remediate and restore that trust.

Feasibility: This option generates (social, economic, fiscal) value for par icipan s in the ecosystem. This option encourages participation in the ecosystem The estimated costs (set-up, ongoing) for government and other ecosystem participan s ar 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, m re weight is assigned to options that effectively ensure trust and can be feasibly implemented.

For the consideration of cost-recovery ptions, 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 opti ns hat 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 Re olution'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 governa ce 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 t s 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 opti n 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, unde an opt-in Trust Framework (the Trusted Digital Identity Framework – the DIF) emand for accreditation has increased significantly along with awareness of the po ential 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 lso 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 ariety of sources, including existing statutory licensing regimes (such as the Immigration Advisers Licensing Act 2012 and the Lawyers and Conveyancers Act 2011). Officials have als reviewed the approaches taken to the establishment of digital identity framewo ks (oth government lead and private) in other jurisdictions including Australia, the UK and Canada.

We are se king Cabinet agreement to allow for the Board to submit regulations regarding an offenc s 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 reso ve 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 d gital identity trust ecosystem were highly supportive of the Trust Framework including a proce s 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 complain s con erning 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 participant we anticipate that the likely parties will be medium to large organisations, including:

- information providers (supply i fo they hold);
- infrastructure providers (Info sharing tools, credential providers, attribute management;
- Authenticator and Auth ntication 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)

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 Author y to protect the integrity of the Trust Framework and to address non-comp ianc with its rules;
- establishing a **dispute resolution** regime; and
- establishing **penalties** to protect the integrity of the accreditation r gime 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 reg me ave 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 pu pose, the Bill will establish that the Board has a variety of functions, including:

- dministe ing 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 e tab ishing 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 responsibl for making appointments to the Board (in line with the requirements under sect on 54 of the Public Service Act 2020) and the host department would be responsible or 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 direc 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-inclusi e, 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 approp ate 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) 
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) 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 requir d to seek accreditation.

Option One– Status quo - no requirement to seek accreditation to the Trust F amework 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 Framewo k was implied. Therefore, under the status quo, all Trust Framework participants (including information providers and infrastructure providers) would not be required to become acc edited to the Trust Framework.

This option will still create benefits that would not exist n 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 part cipants, and to users, providing confidence that information is maintained and shared n a s fe 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 developme t of private sector digital identity ecosystems and Trust Frameworks. s6(b)(i)

However, there is a ri k that optional accreditation may lead to low uptake of accreditation if participants do not perc ive 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 n turn could fail to achieve the key goal of improving trust and uptake of digital identity se vices.

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 cost 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 compl ance more rapidly as businesses and service providers seek to cooperate with Trust Framewor pa ticipants.

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

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

While this option would likely improve overall trus 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 f om $10,000 to $250,000 depending on the complexity of the service being provided. In addit on 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 d ital dentity services in the near term, especially for smaller service providers that have fewer resources to draw upon.

The Department has estima ed 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 standa ds w ll 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 resu , an in-principle decision is being sought from Cabinet on the establishment of p cunia y penalties in the Bill. This section will be updated prior to seeking final decisions, subjec 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 f criminal offences to protect the integrity of the Trust Framework. Similar offences a e common in a variety of statutory licensing regimes (e.g. the Immigration Advisors Licensing Ac , the Lawyers and Conveyancers Act, the Electricity Industry Act, etc). Thes of ences include:

- knowingly or recklessly rep esenting themselves as being an accredited participant of the Trust Framework when they are not – with a maximum penalty of $50,000 for individuals and $ 00,000 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 addres) - 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 o the low-impact compliance mechanisms (e.g. warnings, reporting requirements) to address non compliance. Where non-compliance is not addressed, accredited participants would be rem ved from the Trust Framework when compliance with the Trust Framework is reass ssed (which will be required by the Act annually).

This will be appropriate for addressing less serious non-compl ance However, these options are likely to have limited effect in addressing recidivist or serious non-compliance, especially when non-compliance threatens the privacy and secur ty 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 pro des 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 off nce 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 Accredi ation Authority would have the authority to suspend or revoke a participant's accredi ation n some circumstances.

While the powe to e oke 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 exacerb ted 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 establishmen 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 par cipan s 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, es ablishing a Disputes Tribunal was discounted due to the cost and uncertain dem nd fo 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 dispu e 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 applicab e law nd natural justice. All dispute resolution functions are, and are seen to be, carri d out in an objective and unbiased way.
- Effic ent: 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 use s will be at the centre of dispute resolution processes.

- Independent and fair: Participants will have different app oaches to resolving issues which mean there may not be a consistent and equit ble 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 d sadvantaged 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 t monitor and improve processes over time.

- Effective: There is a risk that cases are unnecessarily referred to courts which may not achieve the obje tives 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.

  Ali nmen 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 ava lable through the courts.

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

- Alignment to Trust Framework Objectives: this ption is partially aligned to the objectives of the Trust Framework as it offers s me 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 fo partic pants to use dispute resolution processes

This option would require all Trust F amework participants to undertake a dispute resolution process before they could take enforcement action through the Accreditation Authority against other participants n 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 m diators/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 he 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 consultati n ith u ers 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 f i : use of a single dispute resolution scheme administered by the Accreditation Authority would provide consistency and predictability as to how disputes will b managed. Use of the dispute resolution scheme will enhance equitable treatment between parties.
- Efficient: u e o a dispute resolution scheme is likely to be more proportionate and timely th n the other options.
- Effective: dispute resolution processes such as negotiation and mediation enable m re 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 f om general taxation in some cases. These include the merit-good aspects of the maintenan e and enforcement of the Trust Framework, encouraging participation during its in tial establishment and recognising that the costs of accreditation may pose a sign ficant barrier to entry for smaller entities (particularly relying parties).

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

Because Cabinet has already sought advice on differe t 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 Fr mewo k rules and accreditation processes will need to be finalised before we can determ ne what kind of cost recovery model should be established.

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

Under this option, there wou d 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 r gulations 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 poten al 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 charg s 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, t presents a more equitable approach, as it will avoid cross-subsidisation between simple and complex accreditation processes. This in turn will incentivise more potential par icipants with relatively simple accreditation processes to apply for accreditation enabling a more rapid scaling of the Trust Framework (and the corresponding benef ts th t come with it).

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

Under this option, the Authority would have he power to impose a levy on all accredited system participants (e.g. in ormation 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 Tr st 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 rul s does not diminish another's). And while it is possible to exclude entities from acce sing the Trust Framework rules, there are strong policy reasons for making them pu licly available.

On this basis th re 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 develo ment 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 propos d for early August 2021).

The rules development programme will in olve ep esentatives from the GCDO, the Government Chief Information Security Offic r, 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 i s c sts 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 Resolu ion to develop a disputes resolution regime that will support effective and efficient d sputes 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 en uring 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 mee ing 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-month y 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 assesse 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 e tablishment of the Trust Framework is impacting on trust in, and use of, digital id ntity 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 suppo t the ecosystem is in place. The Department will begin with a baseline survey befo e 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 regulat ons during phase two of the Trust Framework (2022-2025), which will fo us on its formal establishment in legislation including which organisation will have responsib lity fo this (note - not necessarily the Department). The type of data that could be repor ed could include the number of parties accredited to the Trust Framework, the number of compliance assessments undertaken, the number of disputes that have arisen nd 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 egislation would also likely include a requirement that the Governance Board must review nd eport on any matter relating to the Trust Framework that is specified by the Minister in a wr ten 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.