Regulatory Impact Statement: Digital Identity Services Trust Framework Regulations

Coversheet

Purpose of Document	
Decision sought:	Analysis produced for the purpose of informing final Cabinet decisions on the development of regulations
Advising agencies:	Department of Internal Affairs (the Department)
Proposing Ministers:	Minister for Digitising Government
Date finalised:	15 December 2023

Problem Definition

Regulations are required to give effect to key provisions within the Digital Identity Services Trust Framework Act 2023 (the Act) which is due to come into force on 1 July 2024.

The Government passed the Act to establish a legal framework for the provision of secure and trusted digital identity services for individuals and organisations. Regulations now need to be developed to enable the Trust Framework Authority (TF Authority) to implement the Trust Framework and to accredit and regulate Trust Framework providers (TF providers) in line with the provisions of the primary legislation.

International studies have suggested that the potential benefit of enabling digital identity in a mature economy is between 0.5 per cent and 3 per cent of Gross Domestic Product – approximately $1.5 to 9 billion in NZD. If regulations are not established, the benefits of the regulatory system will not be realised.

This Regulatory Impact Statement aims to determine the best approach to the establishment of the regulations guided by regulatory good practice principles.

Executive Summary

The Requirement

Regulations are required to give effect to key provisions within the Digital Identity Services Trust Framework Act 2023 (the Act).

The Act establishes a Trust Framework that will regulate the provision of digital identity services by Trust Framework providers (TF providers) so that users can securely share digital information about themselves with relying parties to access services. The Trust Framework will give users more control over their own data, including what they choose to share and who they share it with.

To enable the regulatory system to adjust to a rapidly changing business environment, the Act provides for many regulatory requirements to be established in secondary legislation

as either rules or regulations. Both the rules and regulations are required to enable the accreditation of TF providers and TF services and for the general operation of the Trust Framework. This Regulatory Impact Statement focuses on the establishment of the regulations.

Government intervention is designed to provide assurance that digital identity service providers that choose to apply for accreditation and operate within the Trust Framework are meeting appropriate standards. Regulation is required to address information asymmetries and failures in the digital identity services market.[1] The direct benefits are limited to participants that choose to operate within the Trust Framework.

Options

The Department has considered a range of options for delivering the regulations required to give effect to the Act in a manner that reflects good regulatory practice and compared them with the status quo. Those options are:

1. Immediate introduction of light-handed industry enabled regulations;
2. Phased introduction of uniform regulations; and,
3. Immediate introduction of differentiated risk and performance-based regulations.

Option 2 - Phased introduction of uniform requirements – is the Department's preferred approach for the development of regulations. It is expected to deliver a net positive benefit. This option enables the regulations to be developed in a shorter timeframe than the other options and will allow earlier realisation of the regulatory system's benefits. It focuses on the immediate requirements that need to be in place to enable TF provider accreditation, compliance and complaints management in the Trust Framework's implementation phase. Other regulations will be developed and phased in as they are required.

The development of simple, uniform requirements is expected to be relatively easy for digital identity service providers to understand and comply with and presents compliance costs proportionate to the benefits. In comparison to the other options, it also simplifies implementation by the TF Authority, reduces the TF Authority's administrative costs and presents a lower risk profile. Option 2 also recognises that the information required to implement a more sophisticated risk and performance-based model is not sufficiently available in the regulatory system's implementation phase.

Stakeholder views

The Department released a discussion paper in August 2023 that reflected the key elements of option 2. It informed a 4-week targeted stakeholder engagement process on the proposed regulations. The discussion paper was circulated to 40 private sector and non-government organisations, the Data Iwi Leaders Group, and 40 public service organisations and discussed at two online engagement workshops. The Department

[1] Information asymmetries refer to situations where one party in a transaction has more information than the other. In this case, users and relying parties have less information on the digital service being offered than the provider, which will make it more difficult for them to make assessments when choosing service providers and are less able to identify any potential risks with their services. This can lead to the unregulated market delivering sub-optimal outcomes as consumers choose services that present them with less value or greater risks than they might have otherwise chosen to adopt with the benefit of further information. Because the regulation of providers will not be universal, users and relying parties that choose to continue using the services of unregulated digital identity service providers will continue to face the risks inherent in the current market.

received submissions and other feedback from 19 organisations. This included submissions from peak bodies including Digital Identity New Zealand, who represent over 100 organisations and the Data Iwi Leaders Group.

The targeted engagement process confirmed there is broad support for the Trust Framework. There was also support for our preferred approach to developing the enabling regulations, subject to some proposed modifications.

The Department's preferred approach to the development of the regulations has been refined to address stakeholder concerns and suggested improvements where they align with good regulatory practice and the achievement of the Act's objectives. The changes proposed by stakeholders, which we have recommended be adopted, define the intent of the regulations more clearly, reduce compliance costs, better mitigate risks to the Trust Framework's integrity and signal the intent to provide operational guidance to TF providers on how to meet regulatory requirements, including the requirement for the complaints process to have due regard for tikanga Māori.

There were some stakeholder proposals for change in the regulatory approach that we have not adopted.

Some submitters are concerned that leaving the development of cost recovery and renewal arrangements until later in the Trust Framework's implementation phase creates short term uncertainty for potential entrants and could impact adversely on uptake or ongoing participation.

We consider this concern is outweighed by:

- the delay in enabling the establishment of the regulatory system that would be required to develop these additional regulations;
- the higher risks associated with setting fees at this time given the uncertainties around uptake, the operation of the regulatory system and the TF Authority's cost structure; and,
- the incentive available to applicants to obtain accreditation before any fee regime is established.

Some stakeholders have suggested that there is scope to differentiate between applicants for accreditation based on the type of organisation and their risk profile (for example, public service organisations could be exempt from meeting some requirements). Other stakeholders raised concerns with this approach. While we see merit in a regulatory system that takes account of the risks posed by different types of TF provider, it presents significant development and implementation risks in the establishment phase.

We consider standard requirements should apply to all applicants in the regulatory system's establishment phase. The introduction of provisions that enable regulated party experience (performance and risk rating) to be considered or distinctions to be made between different types of provider is something that the TF Board may wish to consider as the regulatory system matures, and the TF Authority develops a better understanding of regulated party behaviour.

The engagement process also highlighted wider implementation issues and risks that go beyond the development of the regulations. Examples include the availability of funding to support uptake by iwi and community information service providers, resourcing of the TF Board and Authority to administer the regulatory system and foster uptake, likelihood of government agency provision of verifiable credentials and related digital identity services, TF provider liability for the actions of users, and communicating the roles of the TF Board and TF Authority. This wider feedback will be taken into account by the Department, the

TF Board and TF Authority and inform the approach adopted for the implementation of the Trust Framework.

Limitations and Constraints on Analysis

This analysis has been framed by the Act and is focussed on the establishment of the regulations provided for under this legislation. Those regulations are limited to establishing the legal and administrative process requirements that either need to be met by regulated parties or establish how the TF Board and TF Authority will manage aspects of the regulatory system. It does not assess the regulatory impact of the rules that are also enabled by the Act and complement the regulations by providing the technical service requirements TF providers will need to meet when designing and delivering accredited services. Nor does it assess the broader regulatory impact of the Trust Framework as a whole. These matters were the subject of earlier regulatory impact assessments considered by Cabinet.[2]

Key assumptions underpinning this analysis include:

- the Act is due to commence on 1 July 2024;
- the enabling rules and regulations should both come into force as soon as possible after the commencement of the Act on 1 July 2024 so the benefits of introducing the Trust Framework can be realised;
- the rules will be subject to a further round of stakeholder consultation in a manner that is consistent with the requirements established in the Act before they are referred to the responsible Minister for approval;
- if a rule is inconsistent with the regulations, the regulations will prevail; and
- Crown funding will cover the cost of administering the Trust Framework for at least its first two years of operation without any cost recovery from regulated parties through fees over this period.

There were some constraints on the Department's analysis.

The Department has not completed an integrated and quantified CBA of the proposed regulations. While taking account of quantifiable data relating to the overall costs and benefits of the Trust Framework where available, our assessment of the regulations is qualitative. It draws on the professional judgement of Departmental legislative and regulatory subject matter experts, feedback from stakeholder engagement, as well as the assessments of costs and benefits of the regulatory system, outlined in previous Regulatory Impact Statements and Cabinet Papers.

As the Act is establishing a new regulatory system in an area where technology, products and services are rapidly evolving in New Zealand and internationally, we have not had a robust evidence base to draw on to assess some regulatory options. Our analysis and

[2] See *Progressing Digital Identity: Establishing a Trust Framework* (Department of Internal Affairs, 23 June 2020) available here: https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/Cabinet-papers-Strategy-for-Digital-Government-Service-2019_redacted.pdf And *Regulatory Impact Statement: Detailed policy for a Digital Identity Trust Framework (10 February 2021)* https://www.dia.govt.nz/diawebsite.nsf/Files/detailed-policy-for-the-digital-identity-trust-framework/$file/detailed-policy-for-the-digital-identity-trust-framework.pdf

approach recognise that the regulatory option that is most effective in the regulatory system's implementation phase should be reviewed and updated as the system matures to take account of participant behaviour and the regulator's experience. Use of and alignment with international standards is a key consideration particularly in the development of the rules which focus on the technical requirements accredited identity services will need to meet.

Timeframe and resource constraints have also been significant considerations during the development and assessment of the options. While we have been able to identify a range of options, our assessment process has recognised the limited implementation time available leading up to 1 July 2024. Early implementation to enable the realisation of benefits is a key imperative. Our assessment has also taken account of the limited resource available to support the development and implementation of the regulatory system given the budget constraints the Digital Identity Services Trust Framework (DISTF) establishment programme has operated under.[3]

The development and assessment of the regulations has involved targeted engagement with key stakeholder groups rather than full public consultation. We consider this more focused engagement process on administrative and technical proposals with representatives of key affected parties was appropriate and has enabled the Department to identify and address key issues of concern to regulated parties and other stakeholders.

The Trust Framework Board (TF Board) and the Māori Advisory Group (MAG) have not been engaged in the early stages of the regulation development process as these groups were not established. We anticipate they will be engaged in the implementation of the first tranche of regulations covered by this RIS and in subsequent phases of regulations' development as well as the overall Trust Framework implementation process.

The Department has, however, continued to engage with the Data Iwi Leaders Group (DILG) on the development of the regulations and the rules. DILG advice will also inform TF Board and MAG consideration of how the TF Authority ensures its implementation processes recognise and respond to the Crown's responsibility to give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi.

We anticipate the TF Authority will undertake further engagement with Māori stakeholders on the implementation of the Trust Framework, including the development of operational guidance on the implementation of the regulations that relate to matters of te ao Māori and tikanga Māori. The TF Authority's approach will be informed by advice received by the TF Board, from the MAG and any consultation with iwi and hapu undertaken by the Board and MAG.

On balance, we consider this assessment provides an adequate foundation and evidence base for Ministers to make informed decisions on the proposed regulatory interventions.

[3] A small programme team within the Department's Digital Public Service Branch is supporting the establishment of the TF Board and TF Authority.

Responsible Manager
 Suzanne Doig General Manager Policy 15 December 2023

Quality Assurance (completed by QA panel)	
Reviewing Agency:	Department of Internal Affairs (the Department)
Panel Assessment and Comment:	The Department's Regulatory Impact Analysis (RIA) panel (the panel) has reviewed the Digital Identity Services Trust Framework RIA in accordance with the quality assurance criteria set out in the CabGuide. The panel members for this review were: • Sam Miles, Principal Policy Analyst (Chair) • Tracey Paterson, Senior Policy Analyst (Member) • Hayden Kerr, Principal Policy Analyst (Member) • Tim Fahey, Policy Analyst (Secretariat) • Sam Strickland, Policy Analyst (Secretariat) The panel considers that the information and analysis summarised in the Regulatory Impact Statement **meets** the quality assurance criteria. The Regulatory Impact Statement contains the necessary information to enable decisionmakers to make an informed decision. The assumptions and constraints in the analysis are reasonable and fairly treated. Appropriate consultation has been undertaken to inform the analysis. Although the costs and benefits are uncertain, this is a consequence of establishing a new regulatory system rather than the shortcomings in the analysis. In particular, consultation has indicated that while there is likely to be take up of Trust Framework accreditation, the speed and extent of take up is uncertain before implementation of the regulatory system. Robust monitoring and evaluation will be necessary, and the phased approach provides an opportunity to address any issues identified. The preferred option provides a reasonable balance between addressing uncertainty and establishing a viable framework. Overall, the RIA does a reasonable job of explaining why government intervention is preferable to the status quo. Sam Miles Chair of the Department of Internal Affairs' RIA panel

Section 1: Diagnosing the policy problem

What is the context behind the policy problem and how is the status quo expected to develop?

New Zealand's digital identity system

1. Many government and private sector services are now provided online. In keeping with this digital environment, New Zealanders expect to access services and complete transactions remotely, rapidly, and with minimal paperwork. However, many transactions that require the provision of digital identity information, such as online banking, claiming a social services payment, or opening a utilities account online, need high levels of security to ensure users' personal information is safe and their privacy is protected.
2. While the use of digital identity services is generally seen as being efficient and provides more opportunities than paper-based systems, it also comes with risks. Users can lose control of their personal information when they share it. Unlike written or spoken information, digital information can be more easily accessed, copied and shared from anywhere in the world. Unfortunately, we are now facing increasing fraud and security risks because of the rapid evolution of global digital sharing.
3. In an environment subject to rapid technological change, regulation is required to address information asymmetries between digital identity service providers and the parties that use their services, and associated harms and failures in the market. Users and relying parties are unable to determine the bona fides of a digital identity service provider or the services they offer.
4. For example, it is difficult for a user to readily obtain assurance that that a digital identity service provider's systems and processes will protect their privacy and ensure that the information they do choose to share with a relying party is secure. Equally, a party that requires information cannot be certain that a provider is meeting appropriate standards that ensure the information they require is indeed about the user they are dealing with and is provided to an appropriate level of assurance.
5. The lack of regulation of digital identity service providers exacerbates the risk of privacy breaches and fraud and has a chilling effect on the growth of digitally enabled social and economic transactions that require digital identity information.

The Digital Identity Services Trust Framework Act 2023

Purpose of the Trust Framework

6. Parliament passed the Digital Identity Services Trust Framework Act 2023 to provide New Zealanders with more confidence in using online identity services.
7. The Act, which is due to come in force on 1 July 2024, will establish:
    a. a legal framework for the provision of secure and trusted digital identity services for individuals and organisations; and
    b. transparent governance and accreditation functions that incorporate te ao Māori approaches to identity.

Regulatory governance, management and advice

8. The Act provides for the TF Board and the TF Authority to administer the legislation. The Department is responsible for both bodies. Both bodies are being established within the Department and are accountable to its Chief Executive.

9. The TF Board's functions include:

   a. recommending draft TF rules to the Minister, reviewing the rules and recommending updates;
   b. recommending regulations to the Minister;
   c. undertaking education and publishing guidance for TF providers and the public; and
   d. monitoring the effectiveness of the Trust Framework.

10. The TF Authority is the regulator. Its functions include:

   a. establishing, administering and maintaining an accreditation regime for digital identity service providers and digital identity services;
   b. establishing, administering and maintaining a register of TF providers and accredited services;
   c. monitoring the performance and effectiveness of the accreditation regime;
   d. operating procedures and tests for TF providers to demonstrate their compliance with the TF rules and regulations;
   e. undertaking compliance monitoring of TF providers;
   f. receiving and assessing complaints; and
   g. investigating breaches of the TF rules, regulations, the terms of use of accreditation marks, and the Act.

11. The Act also provides for the Māori Advisory Group appointed by the responsible Minister to provide advice to the TF Board on issues that raise matters of tikanga Māori, and to establish jointly with the TF Board an engagement policy covering how the two groups will work together and consult with iwi and hapū when necessary.

Trust Framework participants

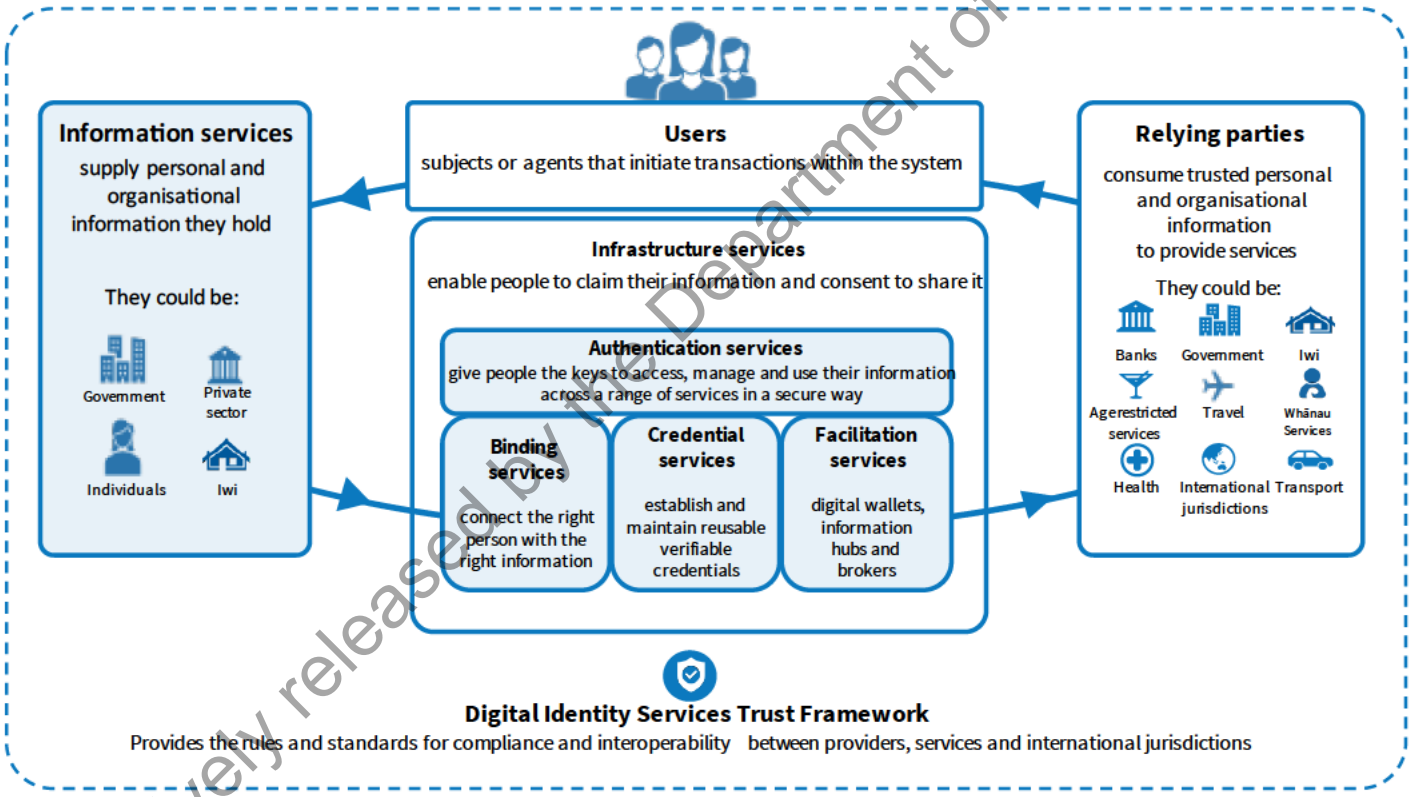
12. The Act, and its enabling rules and regulations, will regulate the provision of digital identity services for transactions between individuals and organisations.

13. Figure 1 depicts the relationship between users, information providers, infrastructure providers and relying parties within the Trust Framework. Information providers and infrastructure providers are the parties that can choose to apply for accreditation under the Act and be regulated as 'TF providers.'

- Relying parties: A relying party requires certain information to offer their service (or to receive a product or service). They need to communicate their identity information requirements to the user who needs to give permission for their information to be shared. Relying parties can include banks, government agencies, utility providers, iwi or health providers. Relying parties will not become accredited under the Trust Framework.

- Users: People wanting to access a service (e.g., power from an electricity provider) can present their digital identity information using a digital wallet or other mechanism in which they store this information. People can still use physical copies of their information and apply for services in person or by phone. Users will not become accredited under the Trust Framework.

Figure 1: The digital identity ecosystem



- Information providers: An information provider, such as a government department, a bank, or an education provider, has the user's information and supplies it as a credential. Information providers may be accredited under the Trust Framework.

- Infrastructure providers: One or more infrastructure providers can be involved in the transfer of a user's digital information from an information provider to a relying party. For example, a credential provider can work with other providers to validate that the identity information belongs to the user, and package it safely and securely, through binding and authentication processes, to deliver a reusable package of information called a verified credential.[4] A facilitation provider - such as a provider of a digital wallet - enables the user to store, manage and share their credential with a relying party to access their service or complete a transaction. For example, RealMe is a platform that provides an identity verification service. Infrastructure providers can be public or private sector organisations. Other New Zealand-based private sector identity service providers include MATTR, Centrality and JNCTN.

Benefits of the Trust Framework

14. The Trust Framework aims to:

    a. improve security and increase trust and confidence in the use of digital services within New Zealand;
    b. give users more control and make it easier to securely access and share information about themselves with relying parties through regulated TF providers;[4]
    c. reduce transaction and storage costs for relying parties that need verified identity and other personal information to provide their services;
    d. enable users and relying parties to reduce the time and cost associated with a multitude of online and face-to-face transactions that require verification of identity and other personal information; and
    e. provide greater certainty to TF providers about regulatory requirements, enabling interoperability between providers, promoting service development and increasing the use of their services by users and relying parties.

15. The anticipated benefits of the Trust Framework include:

    a. enabling user-controlled access to, and sharing of, personal information;
    b. minimising identity theft and privacy breaches;
    c. improving information sharing efficiency;
    d. reducing unnecessary sharing of information;
    e. improving access to online and face-to-face services that require the provision of identity and other personal information; and
    f. encouraging the use of digital identity services and transactions.

16. Having more secure and trusted digital identity services will also:

    a. build New Zealand's resilience to unexpected events by enabling secure digital access to essential identity documents and personal information;
    b. support New Zealand's long-term economic growth and development; and

[4] A relying party is an individual or an organisation that relies on personal or organisational information shared with them before being able to provide the products or services they offer.

c. improve digital trade and other cross-border transactions.

17. Enabling the secure sharing of digital identity credentials can streamline and unlock new opportunities for the delivery of services, simplify digital trade and other cross-border transactions and has the potential to deliver significant economic and social benefits in both the public and private sectors. International studies have suggested that the potential benefit for enabling digital identity in a mature economy is between 0.5 percent and 3 percent of Gross Domestic Product (approximately NZD $1.5 to 9 billion).

Secondary Legislation – Regulations and Rules

18. To enable the regulatory system to adjust to a rapidly changing business environment, the Act provides for many regulatory requirements to be established in secondary legislation as either rules or regulations. Both the rules and regulations are required to enable the accreditation of TF providers and TF services and for the general operation of the Trust Framework.

19. Without these rules and regulations, the benefits of the regulatory system cannot be realised. The TF Board and TF Authority will be unable to fully discharge their functions until the secondary legislation is in place. The Board, for example, will be unable to publish guidance for TF providers on accreditation requirements and the TF Authority will be unable to establish, administer and maintain an accreditation regime for digital identity service providers and digital identity services.

20. The regulations will establish broad administrative requirements that either need to be met by regulated parties or clarify how the TF Board and TF Authority manage aspects of the regulatory system. The Act requires that some regulations must be in place to enable the operation of the Trust Framework, while the introduction of other regulations is discretionary. Appendix A outlines the key provisions in the Act relating to the development of the regulations.

21. The Act enables the responsible Minister to make rules that establish the technical service requirements that providers will need to meet when designing and delivering accredited services. They will cover identification management; privacy and confidentiality; security and risk; information and data management; and information sharing and facilitating arrangements.

22. Draft rules have already been the subject of early consultation with key stakeholders and will be the subject of a further final round of consultation in the first half of 2024 before they are referred to the Minister for approval. The regulations must be in place to enable rules to come into force. If a TF rule is inconsistent with the regulations, the regulations will prevail.

Crown funding and cost recovery

23. The original business case for the establishment of the Trust Framework provided for Crown funding to cover the cost of administering the Framework for its first two years of operation without any cost recovery from regulated parties through fees over this period.

24. Funding for the regulatory framework was sought through the Budget 2022 process and again through Budget 2023. Both bids were unsuccessful. 9(2)(g)(i) [redacted]

9(2)(g)(i) [redacted]

25. The annual cost of operating the Trust Framework will be approximately $5 million. The availability of Crown funding is key to the implementation of the Framework and a key consideration in the development of any future cost recovery arrangements. 9(2)(g)(i) [redacted]

Tiriti o Waitangi/Treaty of Waitangi Implications

26. The Act includes provisions to recognise and respect the Crown's responsibility to give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi. The legislation recognises Māori interests in the protection and use of digital identity and provides for te ao Māori approaches to be incorporated into the Trust Framework governance and decision making.

27. These provisions have been considered when developing the options for establishing the regulations and were addressed during the targeted stakeholder engagement process, particularly with the Data Iwi Leaders Group.

28. We anticipate the TF Authority will undertake further engagement with Māori stakeholders on the implementation of the Trust Framework, including the development of operational guidance on the implementation of the regulations that relate to matters of te ao Māori and tikanga Māori. The TF Authority's approach will be informed by advice received by the TF Board, from the MAG and any consultation with iwi and hapū undertaken by the Board and MAG.

Population Implications

29. Research has identified several groups are at higher risk of not being digitally included in New Zealand including seniors, disabled people, people living in rural communities, and families with children living in low socioeconomic communities. Māori are also less likely to be digitally included than the wider population.

30. Several factors impact on digital inclusion rates including motivation, access, skills, and trust. The development of the Trust Framework will help address trust directly by enhancing security and enabling users to have greater control over the way their data is accessed and shared through accredited digital identity services. It is aligned with the Government's Digital Inclusion Blueprint that aims to remove barriers to access for at-risk groups in the population and ensure everyone can access and use online information, products and services.[5]

31. While the Trust Framework will play a role in supporting digital inclusion, there are no significant direct population implications associated with the regulations themselves (apart from enabling the Trust Framework to be implemented).

32. We anticipate, however, that the Trust Framework implementation process will be informed by further engagement with key stakeholder groups. This may include consultation with ethnic community organisations, who can advise on the specific

[5] The Digital Inclusion Blueprint – Te Mahere mō te Whakaurunga Matihiko

accessibility barriers that ethnic communities face and how the digital identity ecosystem could be utilised to address their needs and requirements.

Related strategy, legislation and government initiatives

33. There are three critical components to building a better, more modern digital identity system:

    a. finalising the regulatory framework established under the Act;
    b. modernising the government's existing identity products and services which are marketed under RealMe and include the issuing of Verifiable Credentials; and,
    c. working with other agencies and the private sector to encourage participation in the Trust Framework to produce and issue verifiable identity credentials.

Digital Strategy for Aotearoa

34. The establishment of the Trust Framework will be an enabler of digital transformation across the public sector and the economy. It will be also a key element in the implementation of the Government's Digital Strategy for Aotearoa, aiming to secure New Zealand's place as a world-leading, trusted, thriving digital nation. The passage of the Bill was part of the Strategy's 2022 action plan.

Related Legislation

35. The Trust Framework will align with and complement existing legislation that regulates the use of personal and organisational information in New Zealand. For example, the Privacy Act 2020 controls how agencies collect, use, disclose, store and give access to personal information. Nothing in the DISTF legislation will override the Privacy Act.

36. Nothing in the Act limits or otherwise affects the Electronic Identity Verification Act 2012 which regulates the operation of the Government's identity verification service (RealMe). Likewise, it does not limit or affect the Identity Information Confirmation Act 2012 which provides a consent-based service to allow both public and private sector agencies to check whether identity information presented by customers is the same as that recorded by the Department.

37. Sector specific legislation such as the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 regulates the use of personal and organisational information in New Zealand as well. There are also standards like the Evidence of Identity standard which outlines requirements for consistent identity establishment and confirmation by agencies. The Trust Framework does not supersede this, or any other, legislation.

Related Legislative Developments

38. The Trust Framework and enabling rules and regulations will complement the exposure draft of the Customer and Product Data Bill (Commerce and Consumer Affairs portfolio) which has been the subject of public consultation.

39. The proposed Bill intends to give consumers the ability to access and share data that is held about them with trusted third parties in a safe and secure manner. The Bill will also mean businesses have to make information about their products available in a manner that will enable easy product comparison and switching. The Trust Framework

will support this outcome by enabling people to securely access and share their related personal identification information digitally.

40. Officials from the Ministry of Business, Innovation and Employment and the Department will continue to work together to ensure the alignment of both regulatory systems. This will include assessing opportunities to reduce implementation and compliance costs potentially through the accreditation process along with other areas.

Iwi affiliation information

41. Section 21(1)(b) of the Act requires the TF board to consult and invite submissions from tikanga experts who have knowledge of te ao Māori approaches to identity before it can recommend draft TF rules to the Minister. Iwi affiliation information is considered taonga and is a vital element of Māori identity. It reflects connections to place and people and enables whānau and individuals to participate in important aspects of Māori community. Complete and up to date iwi registers enable iwi to offer services, support and opportunities for participation to their members.

42. Iwi affiliation records may provide personal information that could be used as part of a digital identity service under the Trust Framework, if agreed by the user. However, the development of iwi affiliation records is not expected to have any implications for either the regulations or the rules.

Related Government digital identity initiatives

43. The Department has a key role to play in mobilising the digital identity market and is working with public and private sector organisations to stimulate interest and participation.

44. Making government-held personal information available is a key factor in mobilising the market. The development of government identity credentials is, therefore, a critical component in the development of the digital identity eco-system. The legislation will apply to Crown entities and government departments that choose to opt-in and deliver services under the framework alongside iwi, private sector and other non-government organisations.

45. This is expected to include modernising the Department's existing identity products and services marketed under RealMe, including the development of a verifiable identity credential from the authoritative data it holds via its passports, births and marriages registries. My Health Accounts, the digital identity service provided by the Ministry of Health, could also join the Trust Framework in the future. Another government credential that could be of significance to digital identity uptake is a digital driver's licence. Work on this is underway led by Waka Kotahi/New Zealand Transport Agency.

46. Other government departments hold identification information and could issue digital credentials. By way of example only, the Ministry for Business Innovation and Employment holds business and immigration information, Inland Revenue holds IRD numbers, the New Zealand Qualifications Authority holds qualification credentials, and the Ministry of Health holds National Health Index information.

International alignment

47. The Digital Identity Services Trust Framework is intended to align with similar frameworks being developed in Australia, Canada and the United Kingdom. It will underpin the Government's commitment to achieving mutual recognition of digital

identity services with Australia under the Single Economic Market agenda[6], and with the UK under the New Zealand – United Kingdom Free Trade Agreement.

48. The Trust Framework will also provide the opportunity to leverage or activate commitments from New Zealand's participation in the Digital Economy Partnership Agreement (DEPA). This is a partnership between New Zealand, Chile and Singapore which was established in 2020 that aims to help New Zealand exporters and SMEs take advantage of digital trade opportunities.[7]

What is the policy problem or opportunity?

49. Regulations are required to give effect to key provisions within the Act. Without establishing the regulations provided for by the Act, it will not be possible for the TF Authority to accredit TF providers and services and establish an effective regulatory system and achieve the significant benefits outlined in section 1 of this assessment.

50. Consequently, digital identity service providers and their services that would have chosen to seek accreditation may continue to operate without meeting appropriate standards and other requirements. This will be a missed opportunity to mitigate the harm arising from an inadequately regulated market. Moreover, the benefits arising from greater uptake and use of trusted and secure digital identity services outlined in section 1 of this assessment will not be realised.

What objectives are sought in relation to the policy problem?

51. The aim is to establish a suite of regulations that:

    a. addresses anything the Act says must be provided for by regulations;
    b. addresses any of the matters the Act says may be provided for by regulations where there is an immediate need to do so to achieve the Act's purpose;
    c. enables the establishment of a regulatory system that is consistent with the Act's purpose and supports the achievement of its intended outcomes; and,
    d. reflects good regulatory practice principles.[8]

[6] For further information see: https://www.mfat.govt.nz/en/countries-and-regions/australia-and-pacific/australia/new-zealand-high-commission-to-australia/single-economic-market/

[7] For further information see: Overview | New Zealand Ministry of Foreign Affairs and Trade (mfat.govt.nz)

[8] The government's regulatory good practise principles, published by the NZ Treasury, have been used to establish the assessment criteria and informs the design of the options. For further information on the principles see: Government Expectations for Good Regulatory Practice (treasury.govt.nz).

Section 2: Deciding upon an option to address the policy problem

What criteria will be used to compare options to the status quo?

52. Our assessment of the options has been based on the following criteria, which have been weighted as noted below:[9]

Effectiveness (30%)	How effective is the option in achieving the system's regulatory objectives and intended outcomes? In particular, will it: • increase trust and confidence in the use of digital identity services; • protect the privacy of users; • remove the need for relying parties to store large amounts of data; • enable user-controlled access to, and sharing of, personal information; • enhance security, minimise identity theft and privacy breaches; • improve information sharing efficiency; • reduce the over sharing of information; • improve access to online and face to face services that require the provision of identity and other personal information; • build New Zealand's resilience to unexpected events; • support New Zealand's long-term economic growth and development; and • improve digital trade and cross-border transactions and people movements?
Proportionality (15%)	Any regulatory requirements should have benefits that outweigh the cost of their introduction. Are the compliance requirements and costs proportionate to the expected benefits?
Certainty (15%)	Will regulatory requirements, processes and decisions be transparent, predictable and consistent, providing certainty to regulated parties?
Flexibility and durability (15%)	Will regulated parties have the scope to adopt least cost and innovative approaches to meeting their legal obligations? Will the regulations enable the regulatory system to evolve in response to new information and changing circumstances?
Development risk and cost (25%)	Are development and implementation risks, timeframes and costs acceptable? Can the regulations be developed and implemented in the time available? Are the options based on established and proven regulatory features or do they include untested or novel solutions? How certain are the development and implementation timeframes and costs? Are they within acceptable bounds?

[9] We have given greater weight to effectiveness and development risk/cost to reflect the importance of ensuring the regulations deliver the intended outcomes, while taking account of the limited runway and available resourcing for regulations development and implementation.

What scope will options be considered within?

Legislative parameters

53. The development of the options outlined in this Statement are framed by the Act. The Act establishes the purpose of the legislation and makes provision for the regulations that are the subject of this assessment.

54. The legislation is limited to matters relating to the establishment and operation of the Trust Framework and the regulation of TF providers; it does not, for example, enable the regulation of TF users or relying parties. Further, the regulatory system is an opt-in one – the regulatory requirements will only apply to those digital identity service providers that choose to seek, and subsequently receive, accreditation under the Act.

55. The Act binds the Crown. Therefore, the legislation will apply to Crown entities and government departments that choose to opt-in and deliver services under the framework alongside iwi, private sector and other non-government organisations.

56. This assessment addresses the regulatory impact of the proposed regulations. It does not assess the regulatory impact of the Rules which are also being established in accord with the relevant provisions in the Act. The options and their assessment consider the requirement for the Act to come into force on 1 July 2024, if not brought in earlier by Order in Council.

Stakeholder Engagement

57. The options considered and assessed in this statement have been framed by regulatory good practice principles and what is legislatively permissible under the Act. Our development of the options has been informed by input from key stakeholder groups – including users, digital identity service providers and relying parties. Our assessment and refinement of the preferred option has been informed by our consideration of feedback received from targeted stakeholder engagement.

Non-Regulatory Options

58. The options we have developed for assessment are, by definition, regulatory ones. In developing the options, we have taken careful consideration of the discretion the Act provides to determine whether regulations are necessary. In some instances, we have not included regulatory requirements where there is insufficient evidence to suggest they are necessary at this time. For example, we are not proposing to introduce regulations relating to the provisional accreditation application process or the certification of third-party assessors.

International Experience and Good Practice

59. In 2018, the Government committed to a programme led by the Department to develop options for a new approach to digital identity. The programme investigated how the Government could establish the right regulatory settings and environment to take advantage of new technologies, offering a modern approach to meeting the evolving needs and expectations of New Zealanders in the digital identity landscape.

60. Through 2019 and 2020 the Department undertook research and engaged with key stakeholders including equivalent agencies internationally. As already noted, the Trust Framework established under the Act will align with similar trust frameworks being developed in Australia, Canada and the United Kingdom enabling interoperability. Use of, and alignment with, open standards developed by global standards bodies is a key feature of the rules which focus on the technical requirements accredited identity

services will need to meet. The adoption of open standards provides the best opportunity for improved interoperability and utility of credentials.

61. In addition to taking account of, and enabling alignment with, key regulatory systems internationally, the Department's approach to establishing the Trust Framework reflects government expectations for good regulatory practice.[10] Key principles drawn from the 2017 guidelines are reflected in our options assessment criteria and informed the design of the options. The regulatory design also draws on the Department's practical experience establishing other regulatory systems and its consideration of approaches adopted by other government agencies.

What options are being considered?

62. We have considered three regulatory options alongside the status quo.

Status Quo

63. Under the status quo regulations would not be established. In these circumstances, the TF Authority would be unable to accredit and regulate providers that choose to seek accreditation for the services they offer.

64. That means users would not have the option of using accredited TF providers that meet the requirements established by regulations. The risks associated with the continued provision of unregulated providers and services would not be mitigated and the anticipated benefits arising from greater uptake and use of trusted digital identity services would not be realised.

Regulatory Options

65. We have summarised three regulatory options in **Table 1:**

    a. **Option 1** would enable the immediate introduction of a full suite of 'light-handed' regulations that recognise and leverage industry peak body standards and practises.

    b. **Option 2** would enable the phased introduction of uniform requirements that would apply to all Trust Framework providers. The first tranche of regulations covers the services to be accredited, accreditation requirements, accreditation duration, and TF provider complaints and dispute resolution, recordkeeping and reporting requirements. Regulations to be considered and phased in later where necessary could include cost recovery requirements, accreditation renewal, an alternative dispute resolution scheme, certification of third-party assessors, and other matters required to support the administration of the Trust Framework.

    c. **Option 3** would enable the immediate introduction of comprehensive regulations that differentiate between different types of provider and service using risk and performance-based criteria where appropriate.

66. Option 2 - which has emerged as our preferred option - is outlined more fully in **Appendix B.** The option incorporates several refinements that respond to feedback received from the targeted stakeholder engagement process to the originally preferred option that was outlined in the Department's discussion paper. The changes define the intent of the regulations more clearly, reduce compliance costs, better mitigate risks to

[10] See New Zealand Government, *Government Expectations for Good Regulatory Practice*, April 2017.

the Trust Framework's integrity, and signal the intent to provide operational guidance to TF providers on how to meet regulatory requirements.

67. Further detail on the targeted stakeholder engagement process and the Department's response to the feedback received is outlined in **Appendix C.**

Table 1: DISTF requirements - options outline			
	Option 1: Immediate introduction of light-handed industry-enabled requirements	**Option 2: Phased introduction of uniform requirements**	**Option 3: Immediate introduction of differentiated risk and performance-based requirements**
Accredited Services	The digital identity credential service only would be subject to accreditation (information, binding, authentication and facilitation services would not be specified in the regulations and subject to accreditation).	Specify five digital identity services, including: information, binding, authentication, credential and facilitation services.	Specify 5 digital identity services as per Option 2 with scope to extend and encompass any additional services that may be identified overtime.
Accreditation Requirements	*Accreditation of the credential service* to the requirements established in the TF Rules. *Accreditation of organisations:* Regulations require applicants to be members of an industry body with appropriate professional standards consistent with the Act, that is recognised by the TF Authority. No additional TF provider application requirements beyond those in the Act specified in regulations.	*Accreditation of Services* that meet differentiated standards and processes for each service established in the TF Rules. *Accreditation of TF Organisations:* Regulations establish uniform requirements for TF provider accreditation including: Resident in NZ; organisational capability requirements; receivership/liquidation or bankruptcy notification requirements; personnel integrity requirements related to s 25(1). *Assessment Criteria* require the TF Authority to be satisfied applicants meet requirements in sections 23-25 including those established in regulations. TF Authority to also seek advice from the Privacy Commissioner before making decisions. The TF Authority will also obtain system level advice from the Government Communications Security Bureau and NZ Security Intelligence Service on national security and also advice on cybersecurity risks and protective security considerations.	*Accreditation of Services* that meet *differentiated standards* for each service established in the TF Rules. *Accreditation of Organisations:* Regulations *differentiate TF provider accreditation requirements* for different types of digital identity service provider as provided for in s 28(2) and reflected in s 24(3).
Duration	*5 years for the accredited service* and *indefinitely for accredited providers* subject to their continued membership of an industry body recognised by the TF Authority.	3 years for all TF providers and all accredited services. Recognises the TF Authority can monitor, audit and investigate TF provider compliance. Compliance monitoring will also be informed by reporting requirements specified in regulations.	9(2)(h) [redacted]
Renewal	*Automatic renewal* subject to ongoing membership of a TF Authority recognised industry body and satisfactory compliance with legislative requirements for the delivery of accredited services as assessed by the industry body and the TF Authority.	To be confirmed in phase 2 regulations TF providers will need to demonstrate they continue to meet the accreditation requirements specified in legislation.	*Application process meeting tailored renewal requirements* differentiated by TF provider and service type that *take* account of performance and risk profiles as assessed by the TF Authority through monitoring and auditing. e.g., high performing/lower risk TF providers can complete a tailored renewal process with lower compliance costs).
Accreditation Mark	No regulations required. TF Provider may display *a uniform accreditation mark* issued by the TF Authority that may be applied to the accredited service and the accredited service provider as prescribed by the TF Authority under section 13 of the Act.	No regulations required. TF provider may display an accreditation mark issued by the TF authority which may be applied to each accredited service (not to the TF provider) as prescribed by the TF Authority under section 13.	No regulations required. TF provider may display an accreditation mark issued by the TF Authority - that includes the service level capability where relevant – which may be applied to each accredited service (not to the TF provider) as prescribed by the TF Authority under section 13.
Provisional Accreditation	Provisional accreditation after assessment against legislative requirements to last for 12 months or a longer period agreed by the authority as enabled by section 32(7)(a).	TF Authority to establish the provisional accreditation process in accord with s32. No regulations to be established that specifically apply to provisional accreditation at this time. Provisional accreditation after assessment against legislative requirements to last for 12 months or a longer period agreed by the TF Authority as enabled by s 32(7)(a).	Provisional accreditation after assessment against legislative requirements to last for 12 months or a longer period agreed by the TF Authority as enabled by s 32(7)(a).
Record keeping	Retain records for 12 months from date of last use. Specify minimum essential requirements.	Enables uniform recordkeeping requirements for all providers. Encompasses records about transaction activities, events and actions that occur in the normal course of users' starting, progressing, and completing digital transactions. Records to be retained for a minimum of 12 months from date of last use. For credentials retention is for the period they remain valid plus a further 12 months. Timely access, data security and integrity requirements apply.	Establish *differentiated requirements* specifying the type of records to be retained and the retention period based on TF risk and needs assessment.

	Option 1: Introduction light-handed industry-enabled regulations	Option 2: Phased introduction of uniform requirements	Option 3: Immediate introduction of differentiated risk and performance-based regulations
Reporting	Notification of changes in governance, management or delivery arrangements related to TF provider or service accreditation status. Periodic (quarterly and annual) provision of data to TF Authority on service use, service delivery, complaints breaches and other events impacting on the integrity or availability of accredited services as specified by the regulator. Comply with privacy-breach and other reporting requirements provided in other legislation.	Uniform periodic reporting to the TF Authority on service use, service delivery, complaints and incidents impacting on the integrity or availability of accredited services using templates provided by the TF Authority. *Incident notification:* Notification of cybersecurity and fraud events or any other events that adversely affect privacy, or confidentiality, the integrity or availability of the digital identity service and has caused or presents a risk of causing serious harm to be established under s 28(2). Definition of serious harm and notification expectations and processes to be aligned with those established under the Privacy Act 2020 by the Privacy Commissioner. Examples of serious harm included.	Annual reporting and periodic notification and reporting on actual or potential high-risk incidents. Differentiation in requirements based on provider type and accredited services. Comply with privacy-breach and other reporting requirements provided in other legislation.
Complaints	Adherence to industry association code of conduct and complaints management policies.	Uniform internal complaints process requirements prescribed in regulations apply to all TF providers. TF Authority to provide guidance to TF providers on good practise regarding tikanga Māori following MAG/Māori/Iwi engagement.	*Differentiated internal complaints* process based on size and type of provider and nature of accredited services delivered.
Dispute Resolution	All TF providers to be members of an industry association recognised by the TF Authority that offers a disputes resolution service.	To be confirmed in phase 2 regulations, if required.	TF Authority to provide a *disputes resolution scheme*, or recognise a disputes resolution scheme provider, for use where a TF provider is not a member of an industry body offering disputes resolution service.
Cost Recovery	First 2 years fully funded by the Crown. *Application and renewal fees:* A variable fee that reflects any differences in the actual marginal cost of processing different types of applications as provided for in s 24(4). *Disputes Resolution Scheme:* Charges for accessing industry-based disputes resolution services established by industry bodies with majority of cost met by association members. Modest additional fees paid by parties to the dispute. *Other TF Costs:* Fully funded by the Crown in recognition of TF public good benefits.	First 2 years fully funded by the Crown. Future cost recovery policy and fee schedule to be confirmed in phase 2 regulations if required.	First 2 years fully funded by the Crown. *Application and Renewal Fees:* A *variable fee* that reflects any differences in the marginal cost of processing different types of applications as provided for in s 24(4). *Disputes Resolution Scheme:* Fees for partial cost recovery of established in regulation. *Other TF Costs:* Annual accreditation fees enabling partial recovery (say 50%) of trust framework operating costs with fees differentiated for different types of provider, service and different levels of assurance as provided for in s 28. Remaining costs Crown funded to recognise public good benefits.
Third-party Assessors	TF Authority certifies industry bodies as third-party assessors for the accreditation of TF providers and services.	To be confirmed in phase 2 regulations, if required.	Criteria that enable the TF Authority to certify independent assessors with the capability to assess one or more types of provider and service.
Other Matters	*Compliance Order Forms:* Regulations not required.	*Compliance Order Forms:* To be confirmed in phase 2 regs, if required.	*Compliance Order Forms: Establish forms* to support the TF Authority's compliance management activities.

How do the options compare to the status quo/counterfactual?

Table 2:	Status Quo	Option 1: Introduction of light-handed industry-enabled regulations:	Option 2: Phased introduction of uniform regulations:	Option 3: Introduction of differentiated risk and performance-based regulations:
Effectiveness	*0*	0/+ Minor improvement on the status quo. Proposed regulations address all regulatory requirements specified in the Act. However, the reliance on industry body recognition and processes, longer accreditation periods and lighter recordkeeping and reporting arrangements means there is scope for greater variation in TF compliance than under options 2 or 3. This level of regulation is likely to be less effective than either option 2 or 3.	++ Potentially a significant improvement on the status quo with earlier benefits realisation than other options. Regulations are focused on those matters that must be in place to enable TF provider accreditation, compliance and complaints management in the start-up phase. The option is aligned with the Act's purpose and is likely to significantly improve outcomes particularly in the establishment phase by specifying robust accreditation application and assessment criteria with renewal after 3 years, establishing recordkeeping and reporting requirements that will support compliance monitoring, and establishing appropriate complaints management requirements.	++ Potentially a significant improvement on the status quo with regulations covering all regulatory requirements specified in the Act. Provides incentives for TF providers to comply with regulatory requirements by taking account of their risk profile and performance which may have a marked impact on the achievement of Trust Framework outcomes in the medium to longer term. The lack of data on TF provider performance makes it challenging to establish evidence-based risk profiles meaning this approach is likely to be more effective in the medium-long term rather than during the establishment phase.
Proportionality	*0*	0/+ Benefits of a light-handed approach outweigh costs. While the establishment and ongoing operating costs may be lower than Options 2 and 3, the option is also likely to deliver benefits at a lower level meaning the cost to benefit ratio is likely to be poorer than that achieved by option 2 and also poorer than option 3 over the medium to longer term.	+ Benefits of the phased introduction of uniform requirements outweigh the compliance costs. Uniform approach reduces implementation costs for the regulator without a negative impact on outcomes. The ratio of costs to anticipated benefits is higher than the status quo and option 1 outright while it if likely to be higher than option 3 in the establishment phase.	0/+ Benefits of a differentiated risk and performance-based approach outweigh costs. Greater establishment and ongoing regulator implementation costs than option 2. While the option better matches costs to compliance risk and performance, the increased costs may not deliver proportionately greater improvements in effectiveness in the establishment phase and over the short to medium term.
Certainty	*0*	0/+ Greater certainty around regulatory requirements as all regulatory features established to support the establishment and operation of the Trust Framework. However, reliance on industry bodies as intermediaries may create less transparency and less predictable outcomes than option 2.	0/+ Greater certainty than the status quo based on simple, well defined establishment phase requirements that are relatively easy for TF providers to understand and for the TF Authority to apply. Delay in establishing cost recovery, renewal and other regulations results in short term uncertainty, however these regulations are less likely to require change after their establishment as they will be more considered and evidence based.	0/+ Greater certainty than the status quo as all regulatory features established to support the establishment and operation of the Trust Framework. Greater complexity in the regulatory requirements arising from the use of risk and performance related features may result in less certainty around TF Authority decision making in the short term but this could be expected to improve over time.
Flexibility and Durability	*0*	+ Option provides scope for providers to adopt least cost approaches to compliance and respond to change in the regulatory environment.	+ Option provides scope for providers to adopt least cost approaches to compliance and respond to change in the regulatory environment.	+ Option provides scope for providers to adopt least cost approaches to compliance and respond to change in the regulatory environment.
Development Risk and Cost	*0*	- While relatively simple light-handed regulation leveraging industry bodies may reduce compliance costs, recognition of those bodies presents development complexity. Timeframe, DIA policy and TF Authority resourcing constraints, and uncertainty in a new regulatory environment also present development and implementation risks.	+ Largely uniform requirements focused on immediate establishment requirements simplify development and implementation. Phased implementation also addresses time and resource constraints and enables phase 2 regulations to be better aligned with early TF Authority experience and understanding of the emerging regulatory environment.	- - Differentiation results in greater development complexity. Limited development timeframe, DIA policy and TF Authority resource constraints, no regulatory performance information, and uncertainty in a new regulatory environment present significant development and implementation risks. The time required to establish comprehensive regulations would delay drafting and gazettal.
Summary Assessment:	*0*	0/+ A marginal improvement on the status quo. The need for the TF Authority to establish arrangements for recognising and monitoring industry bodies presents significant risks and additional costs in the lead up to the Act's commencement given the development challenges, timeframe and resource constraints. Some elements from this option could be considered during the ongoing development and review of the regulations.	++ **Preferred approach** Significant improvement on the Status Quo. Relatively simple but effective regulatory framework within acceptable risk parameters given time and resource constraints and uncertainties in the regulatory system's establishment phase. Enables earlier introduction and realisation of Trust Framework benefits than options 1 and 3.	+ An improvement on the status quo. However, greater development and implementation risks in the short term. The option offers a vision of how the regulations might evolve over time as the regulatory system matures and the TF Authority develops a better understanding of the regulatory system and TF provider behaviour.

Key: *++ significant improvement on the status quo; + improvement on the status quo; 0/+ minor improvement on the status; **0** neutral/no change; 0/- slightly worse than the status quo; - worse than the status quo; - - much worse than the status quo.*

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

Option 2 – Preferred Approach

68. Option 2 – the phased introduction of uniform regulatory requirements – is the Department's preferred option. It is expected to deliver a net positive benefit. The option enables the development of a relatively simple but effective regulatory framework within acceptable risk parameters given time and resource constraints and the uncertainties inherent in the establishment phase of a new regulatory system.

69. Option 2 enables the regulations to be developed and gazetted in a shorter timeframe than the other options. It focuses on those immediate requirements that need to be in place to enable TF provider accreditation, compliance and complaints management in the Trust Framework's establishment phase. Other regulations can be developed and phased in as they are required.

70. Option 2 also simplifies implementation by the TF Authority and reduces its administrative costs. It provides greater certainty to regulated parties and presents a lower risk profile than the other options. This option enables the realisation of the Trust Framework's benefits, which include improving security and increasing consumer trust and confidence in the use of digital identity services, more quickly than the other options. This approach also provides a foundation that can be built upon based on the TF Authority's early regulatory management experience.

Option 3 – Vision for the Future

71. The benefits provided by a differentiated risk and performance-based approach as outlined in option 3 are an improvement on the status quo. While this approach has the potential to be more effective that option 2 in the longer term, it presents greater development and implementation risks in the short term given the uncertainties inherent in the regulatory system's establishment phase and the lack of sufficient evidence to experience or risk rate different types of TF providers. In addition, more time would be required to develop the regulations than option 2, further delaying implementation.

72. Option 3 does, however, offer a vision of how the regulations might evolve over time as the regulatory system matures, the regulator has better information on the performance of TF providers, and the TF Board looks to refine the regulations to reflect lessons learned during the regulatory system's establishment phase.

Option 1 – Elements worthy of consideration in phase 2

73. Option 1 – the immediate introduction of light-handed industry enabled regulations – would deliver an improvement on the status quo although it does not offer as significant improvement as either option 2 or 3. The need to establish arrangements for recognising and monitoring industry bodies as well as establishing robust cost recovery arrangements would also present significant risks and would delay implementation and the realisation of the Trust Framework's benefits. In short, while this option has potentially lower compliance costs for TF providers than the preferred option, it is not as effective, would take longer to implement and result in additional costs to the regulator.

74. There are, however, elements within option 1 that could be considered during the second phase of regulations development – including the proposed approach to renewal, dispute resolution, cost recovery and certification of third-party assessors.

What are the marginal costs and benefits of the option?

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups: - TF Providers	Accreditation is voluntary so there are no costs for providers that do not wish to apply. No TF Authority accreditation fees in first two years of scheme operation, but applicants may incur fees thereafter for accreditation, renewal and wider TF administration costs through future cost recovery regulations. TF providers will incur direct costs associated with meeting accreditation requirements established in the regulations. Cost is expected to vary depending on the nature and size of the TF provider, the range of services offered. 9(2)(f)(iv) [redacted] Low confidence in estimates as the true cost can only be established once the accreditation and compliance process, rules and ongoing obligations are finalised.	Low-Medium	Low
Regulator: - TF Board and Authority	Establishment and ongoing costs associated with administering the regulations. Includes a portion of the up to $5 million estimated annual cost of operating the Trust Framework regulator. Moderate confidence in estimate based on original business case and further work on implementation costs.	Medium	Medium-High
Others: - Users	No direct costs from regulations. Scope for some regulatory compliance costs to be passed on by TF providers in the form of TF provider service charges (although effective markets do not impose significant charges on users – infrastructure providers in particular may, therefore, seek to recoup costs through charges on relying parties rather than users).	Very Low	Low-Medium
- Relying Parties	No direct costs arising from regulations. Scope for some regulatory compliance costs to be passed on to relying parties in the form of service charges (could involve TF provider charges per transaction for verification or subscription charges).	Low	Low-Medium
- Other Govt agencies	Ministry of Justice costs administering criminal conviction checks. GCSB/NZSIS costs providing system level advice on how to assess national security risks, and the provision of information security and protective security advice to the TF Authority.	Low	Medium
Total monetised costs		-	-
Non-monetised costs		Low-Medium	Medium

Additional benefits of the preferred option compared to taking no action			
Regulated groups: - TF providers	Benefits as outlined earlier in this assessment accrue to providers who are accredited including greater use of their services by users and relying parties and easier establishment of interoperability arrangements with other TF providers to deliver integrated services.	Medium-High	Medium
Regulator: - TF Board and Authority	Regulations enable the TF Authority to accredit and regulate TF providers. Regulations enable the TF Board to undertake education and publish guidance required to support uptake of, and participation in, the Trust Framework.	Medium	Medium
Others: - Users	Increased confidence in the security, privacy and integrity of Trust Framework services resulting in greater use of digital identity services and benefits realisation as outlined earlier in this assessment, including reduced transaction costs to access or provide services, and greater control over access to and use of personal or organisational information.	Medium-High	Medium
Others: - Relying Parties	Increased confidence in the security and integrity of Trust Framework services resulting in greater use of digital identity services and benefits realisation as outlined earlier in this assessment including reduced transaction and data storage costs.	Medium - High	Medium
Total monetised benefits		-	-
Non-monetised benefits		*High*	*Medium*

Note: When attributing 'low-medium-high' values to the costs and benefits incurred by the different parties we have taken account of their relative comparative size. 9(2)(f)(iv)

[redacted]

75. The Department's Regulatory Impact Statement produced in February 2021 to inform Cabinet decisions on the detailed policy for the Trust Framework included some quantified cost and benefit ranges.[11] While referencing some of these estimates in this assessment, we have adopted a qualitative non-monetised approach as we have not been able to quantify the direct costs and benefits associated with the introduction of the regulations and distinguish them from the costs and benefits associated with the introduction of the rules and other elements of the overall regulatory system. As an indicative guide only, we have assumed the costs associated with the regulations can be considered as a portion of the estimated costs digital identity service providers will incur as part of the accreditation testing and application process.

76. It is important to note the uncertainties around the accuracy of the qualitative assessment of both costs and benefits related to the regulations. The 'medium' certainty ratings for benefits realisation relates in part to the 'opt-in' voluntary nature of the regulatory system and the uncertainty around uptake and use of the framework.

[11] See https://www.dia.govt.nz/diawebsite.nsf/Files/detailed-policy-for-the-digital-identity-trust-framework/$file/detailed-policy-for-the-digital-identity-trust-framework.pdf

The low-medium rating for user and relying party costs relates in part to uncertainty around what approach TF providers will take to cost recovery. While there is a higher level of confidence in the assessment of TF Board and TF Authority costs based on business case estimates some uncertainty remains around actual costs until these bodies have had the opportunity to pilot and then deliver regulatory services and we have a better understanding around uptake and use of the Trust Framework.

77. In making our qualitative assessment, however, there is no evidence to suggest the proposed regulations would require any change to the conclusion in previous regulatory impact statements on the establishment of the Trust Framework that the overall monetary and non-monetary benefits of implementing the Trust Framework are likely to exceed the costs.

78. As the Regulatory Impact Statement prepared in February 2021 noted international studies have suggested that the potential benefit of enabling digital identity in mature economy is between 0.5 per cent and 3 per cent of GDP (approximately NZD $1.5 to $9 billion), is not being fully realised. The successful implementation of the Trust Framework will contribute to realising that benefit and the regulations are a necessary requirement for the establishment of the Framework.

79. We are of the view that the regulatory costs associated with the development and implementation of the regulations will be outweighed by the significant economic and societal benefits provided to both public and private sectors.

Section 3: Delivering an option

How will the new arrangements be implemented?

Roles and responsibilities

80. The TF Board may recommend draft regulations to the Minister responsible for the administration of the Act. The Minister provides recommendations to the Governor-General to establish the regulations by Order in Council.

81. The Department is responsible for the TF Board and the TF Authority which both have roles to play in the implementation of the regulations. In the Trust Framework's establishment phase, the Department has also led the development of the regulations and provided advice on them to the Minister.

82. In addition to being able to recommend draft regulations to the Minister, the TF Board's functions include educating and publishing guidance for TF providers and the public on the Trust Framework and monitoring its effectiveness. The TF Authority is the regulator. It is responsible for administering and maintaining the Trust Framework

83. The MAG, which is appointed by the Minister, is responsible for advising the TF Board on matters of tikanga Māori or Māori cultural perspectives, including on the implementation of the regulations.

Rules Development and Accreditation

84. The Department has aligned the rules and regulations development timelines, recognising the links and dependencies between them. It is anticipated the rules will be approved by the Minister, gazetted and come into force at the same time as the regulations. Once both the regulations and rules come into force the TF Authority will be able to consider applications for the accreditation of providers and the services they deliver.

Implementation

85. Implementation of the regulations and the overall Trust Framework is dependent on the function being funded for implementation beyond 2023/24. As noted earlier, the overall costs to the Department are estimated to be around $5 million per annum.

86. The Trust Framework establishment team within the Department will be progressing work on the appointment of staff and the establishment of business processes, systems, operational policy, and guidance required to implement the legislation largely in parallel with the development of the regulations and rules. The TF Authority will only be able to finalise its policies, processes and systems after the final regulations are approved by Order in Council.

87. In addition, the Board and Authority will be progressing the rollout of an uptake strategy designed to highlight the benefits the Trust Framework offers and promote participation in, and use of, the Framework.

88. The Trust Framework implementation process will be informed by further engagement with key stakeholder groups. Consultation with Māori and iwi groups will be guided by the engagement policy developed by the TF Board and MAG. This will be particularly important for informing the development of operational guidance on the implementation of the regulations that relates to matters of te ao Māori and tikanga Māori.

Monitoring, evaluation and review

89. The TF Board has oversight of the monitoring, evaluation and review of the regulations. Under the Act the TF Board may recommend regulations to the Minister and is

responsible for monitoring the effectiveness of the Trust Framework. This role encompasses the evaluation and review of the Trust Framework's regulations.

90. The TF Authority will be establishing Trust Framework monitoring and evaluation arrangements that will inform its consideration of the regulations and the performance of the overall Trust Framework. The record keeping and reporting requirements established in the regulations and administered by the TF Authority - combined with wider monitoring and evaluation arrangements - are expected to inform not only TF provider compliance monitoring but the development of the outstanding regulations and the update of the first tranche of regulations recommended for introduction in 2024.

91. The monitoring and evaluation arrangements will be a valuable means of developing the evidence base required to determine the effectiveness of the regulations, the compliance costs incurred by regulated parties, their impact on Trust Framework uptake and participation, and the efficacy of introducing risk and experience related features into future iterations of the regulations.

Issues and Risk Management

92. Table 4 identifies and addresses a number of implementation issues and risks:

Table 4:

Issue/Risk	Mitigation
Issue: Short 'runway' for the TF Authority to prepare for and implement the regulations	TF Authority establishment team will develop business processes, systems, operational policy and guidance required to implement the legislation largely in parallel with the development of the regulations (and the rules). Regulations assessment criteria gave greater weighting to effectiveness and implementation risk.
Issue: Regulations are not in place by 1 July 2024 delaying Trust Framework implementation and benefits realisation	DISTF Programme Plan recognises the introduction of the rules and the Trust Framework is dependent on the regulations coming into force and makes provision for post-1 July start date scenarios. TF Board and TF Authority communications will ensure stakeholders are aware of key Trust Framework implementation target dates.
Issue: Crown funding required to implement the regulations	Advice to Minister for Digitising Government on Departmental funding requirements to implement and administer the Trust Framework (including the regulations). The Department is exploring options, including opportunities for new funding, to meet the Trust Framework's cost in FY24/25 and outyears.
Risk: Phased development of regulations, particularly cost recovery and renewal, creates uncertainty for digital identity service providers that presents a barrier to uptake and ongoing Trust Framework participation.	Full Crown funding for the first two years from the Act's commence date and provides an incentive for early uptake. TF Authority to employ dedicated staff to promote understanding of the Trust Framework, and the benefits of accreditation to mobilise the digital identity market and stimulate interest and participation. Transparent and open stakeholder engagement to support future phased regulations development.
Risk: Digital identity service providers seeking accreditation are not aware of or do not understand how to comply with regulatory requirements.	Engagement with key stakeholder groups during design of regulatory proposals. TF Authority to produce and publish operational guidance for TF providers.TF Authority staff to engage with digital identity service providers to promote understanding and participation.
Issue: Ensuring the regulations are implemented in a manner that recognises and respects the Crown's responsibility to give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi as provided for in the Act.	Early engagement with the Data Iwi Leaders Group in advance of the establishment of the TF Board and MAG. TF Authority to undertake further engagement with Māori stakeholders on the implementation of the Trust Framework, including the development of operational guidance on the implementation of the regulations that relate to matters of te ao Māori and tikanga Māori. TF Authority's approach will be informed by advice received by the TF Board from the MAG and any consultation with iwi and hapū undertaken by the Board and MAG in accord with their engagement policy once established.

Appendix A: Digital Identity Services Trust Framework Act – Provisions relating to regulations development

DIGITAL IDENTITY SERVICES TRUST FRAMEWORK ACT PROVISIONS RELEVANT TO THE DEVELOPMENT OF REGULATIONS
Meaning of Digital Identity Service *s 10(3)* - The regulations must prescribe the types of digital identity services that may be accredited under this Act.
Accreditation: *Contents of Application s 24* - Applications must contain – key information prescribed by regulations. - Other information required by regulations. - Accompanied by the fee prescribed by regulations. - Key information may differ for different applications, providers and services *s 24(3)*. Criteria *s 26* - The application, provider, or service meets any criteria for the assessment of applications set by regulations *s 26(1)(b)*. Duration *s 30* - Accreditation expires at the end of the relevant period set by the regulations. - Regulations may set different periods for different types of providers and services. Renewal *s 31* - Except where the Act or regulations set different requirements for renewal applications s 23 and s 25 apply. Provisional Accreditation *s 32* - Except where the Act or regulations set different requirements for renewal applications s 23 and s 29 apply.
Regulations for accredited providers and services *s 28* - Regulations may prescribe requirements for: o Periodic self-assessment by TF providers. o Periodic reporting by TF providers. o Complaints and dispute resolution processes that must be operated by TF providers. o Other matters related to the operations of TF providers and the accredited services as the TF Board and Minister think fit. o Fees for recovering the costs of operating the Trust Framework. - Different requirements or fees may be set for different types of providers, services and different levels of assurance for different types of accredited service.
Certification of third-party assessors *s 39* - TF Authority may certify an individual or an organisation to carry out functions relating to the accreditation of providers or services if permitted by, and in accordance with, the regulations *s39(1)*. - The regulations may prescribe circumstances under which the authority may suspend or cancel certification of third-party providers *s 39(3)*.
Record keeping and reporting by third-party assessors *s 41* - The regulations may prescribe record keeping and reporting requirements *s 41*.

Recordkeeping and reporting by TF Providers *s 42* - Collect, keep and give information periodically or at all reasonable times on request to the TF Authority as required by the regulations.
Functions of the TF board *s 45* - The TF board's functions are to… (b) recommend regulations to the Minister. - When performing its functions, the board must engage with Māori in the manner provided for under section 53(5) to recognize and provide for Māori interests in the operation of the trust framework.
Role of Māori Advisory Group *s 53* - The board and Māori Advisory Group acting jointly must – prepare an engagement policy setting out how they will work together. - The engagement policy must include details of how and when consultation with iwi and hapū will be undertaken by – the board, the board together with the Māori Advisory Group; the Māori Advisory Group to inform its advice to the board.

Regulation making powers *s 102*
- The Governor-General may, on the recommendation of the Minister, by Order in Council, make regulations for one or both of the following purposes:
  o Providing for anything the Act says may or must be provided for by regulations.
  o Providing for anything incidental that is necessary for carrying out, or giving full effect to, the Act.
- The TF board may recommend draft regulations to the Minister.
- Before regulations are made under this section the Minister must consult the Office of the Privacy Commissioner.

Appendix B: Recommended regulations

OVERVIEW

The Digital Identity Services Trust Framework Act 2023 (the Act) comes into force on 1 July 2024. It enables the introduction of a new regulatory system, which will establish rules and regulations for the provision of secure and trusted digital identity services.

The rules will establish the technical service requirements that TF providers will need to meet when designing and delivering accredited services. The draft rules have been the subject of early consultation with key stakeholders and will be the subject of a further final round of consultation, likely in the first quarter of 2024. They cover – identification management; privacy and confidentiality; security and risk; information and data management; and information sharing and facilitating arrangements.

The regulations will establish broader legal and administrative process requirements that either need to be met by regulated parties or clarify how the TF Board and the TF Authority will manage aspects of the regulatory system. If a rule is inconsistent with the regulations, the regulations will prevail.

The regulations will be developed in two or more phases. The first set of regulations, that are required to initially stand up the regulatory system, will cover:

- *Accredited Services:* Definition of the types of services that will be subject to accreditation under the Act.
- *Accreditation Process*: Accreditation requirements, application assessment criteria, and accreditation duration.
- *Complaints and Dispute Resolution:* The internal complaints and dispute resolution process requirements TF providers need to meet.
- *Recordkeeping*: The information to be retained by TF providers and the period they are required to retain that information.
- *Reporting*: The reporting requirements that will apply to TF providers.

Further regulations will be developed and recommended to the Minister for Digitising Government by the TF Board on an as required basis following the commencement of the Act. These regulations may include:

- *Cost Recovery:* The establishment of fees for the partial recovery of the TF Authority's ongoing costs for administering the Trust Framework, including consideration of accreditation applications or renewals (It is anticipated that the TF Authority's initial establishment and first two years of operating costs will be met from Crown funding without a contribution from fees).
- *Dispute Resolution Scheme:* The establishment of any requirements and criteria that the TF Authority must meet should it want to recommend a dispute resolution scheme, together with any proposed fees to recover costs associated with the provision of complaints and dispute resolution services. The establishment of a fee regime will be considered in conjunction with the development of the TF Authority's complaints and dispute resolution operating model, which will consider the role, if any, of an external dispute resolution service provider.
- *Third Party Assessors*: Arrangements for the certification of third-party assessors to carry out functions relating to the accreditation of TF providers, including appointment criteria, recordkeeping, and reporting requirements.

- *Other Operational Matters:* Any other operational matters that the TF Board considers should be established in regulations to provide greater certainty to both the TF Authority and regulated parties on compliance requirements and ensure the cost-effective management of the regulatory system by the TF Authority. The regulations, for example, will cover any changes to accreditation renewal requirements and compliance order forms.

ACCREDITED SERVICES

The Act requires that the regulations prescribe the types of digital identity service that may be accredited. We propose that the regulations specify that the following services can be delivered as accredited services by TF providers under the Act:

- *Digital Identity Information Service:* This service involves assessing the accuracy of personal or organisational information. It helps ensure that the information linked to an individual or organisation is correct, reducing the risk of information errors and false associations.
- *Digital Identity Binding Service:* This service focuses on assuring the connection between personal or organisational information and the individual or organisation. It establishes a secure link between information and the entity it pertains to.
- *Digital Identity Authentication Service:* This service ensures a secure connection between a user and an authenticator. It also facilitates the secure sharing of personal or organisational information between different parties, maintaining the privacy and integrity of the data.
- *Digital Identity Credential Service:* This service combines bound (connected) information with an authenticator to create a reusable credential. This credential can be used to establish and maintain the user's information across various services, minimizing the need to repeatedly share sensitive information.
- *Digital Identity Facilitation Service:* This service provides a facilitation mechanism to assist users in sharing credentials or specific parts of credentials with relying parties. It simplifies sharing digital identity credentials with trusted parties while maintaining security and control. An example of such a service is a digital wallet.

A binding service cannot be provided in isolation and needs to be combined with either an information service or a credentialling service. The regulations will specify the binding service in its own right to provide digital identity service providers with the flexibility to deliver it in combination with either the information service or the credential service.

As noted in the overview, the specific requirements TF providers will need to meet when designing and delivering accredited services will be established in the rules.

ACCREDITATION PROCESS

Any digital identity service provider that wants to deliver one or more of the services prescribed in the regulations as an accredited service will need to apply and demonstrate to the TF Authority that they can meet the accreditation requirements specified in the Act, rules and regulations.

The Act establishes certain requirements that applications for accreditation must meet. These include:

- Being in a form, and made in a manner, approved by the TF Authority;
- Containing information prescribed in regulations; and
- Providing the information required by section 25(1), which includes whether the applicant has:

- been convicted of a criminal offence in New Zealand or overseas;
- been, or is, the subject of a formal Privacy Commission investigation or proceeding;
- previously had an application for accreditation for themselves or a service they provided declined;
- had their accreditation as a TF provider or of a service they provided suspended or cancelled; or
- not complied with additional record-keeping or reporting requirements or a compliance order imposed or issued under section 83 of the Act.

Accreditation Requirements

In addition to meeting the requirements specified in section 25(1) of the Act, we propose that the regulations incorporate the following requirements that TF providers would need to meet when applying for accreditation of a service or services.

Resident in New Zealand:

Individuals or entities that wish to provide accredited services will need to meet New Zealand residency requirements along similar lines to those established in the Financial Service Providers (Registration) Regulations 2020.

An individual applying for accreditation will need to demonstrate they: have a permanent place of residence in New Zealand, even if they also have a permanent place of residence elsewhere; and are a New Zealand citizen or hold a residence class visa granted under the Immigration Act 2009, or hold a visa granted under that Act that allows them to work or study in New Zealand.

An entity applying for accreditation will need to demonstrate that it is formed or incorporated in New Zealand and carries on business in New Zealand.

This will mean an international company that wants to apply for accreditation will need to have a New Zealand subsidiary which must hold any accreditation granted by the TF Authority. This approach also recognises New Zealand central and local government organisations can apply for accreditation.

Organisational Capability:

Applicants will need to provide information or declarations specified by the TF Authority to demonstrate that the organisation seeking accreditation:

- Has the organisational capability including the people, policies, processes and systems required to deliver TF accredited services;
- Is not in receivership, liquidation, bankrupt of subject to a No Asset Procedure that would result in it being unable to deliver accredited services;
- Can meet the standards and processes prescribed in rules to deliver the service or services; and
- Has arrangements in place to provide a complaints and dispute resolution process that meets the requirements specified in the regulations.

Section 25(1) Verification:

Applicants will be required to provide information to the TF Authority specified in s25(1). This will include provision of:

- Criminal record checks relating to the applicant from the Ministry of Justice, and from overseas agencies where the TF Authority deems this necessary; and,

- A declaration that the applicant has not been or is currently the subject of a Privacy Commission investigation or proceeding, or - where they are or have been the subject of an investigation or proceeding – details on the status or outcome of it.

The applicant will also need to provide information demonstrating that they have appropriate policies and procedures for ensuring its staff recruitment and service contracting practices meet accreditation standards and do not present a risk to the integrity of the Trust Framework. This is expected to include arrangements for:

- Checking whether staff or contractors engaged by it that are involved in the governance, management, design or delivery of accredited services have:
  - been convicted of a criminal offence in New Zealand or overseas;
  - been, or are, the subject of a Privacy Commission investigation or proceeding; and,
- Taking reasonable steps to ensure any staff it wishes to employ or service providers it wishes to contract can meet accreditation standards; will maintain the security, privacy, confidentiality and safety of information relating to any Trust Framework participant; and will not compromise the security or integrity of accredited services or the integrity or reputation of the Trust Framework.[12]

Assessment criteria

The Act enables the TF Authority to accredit a provider if it is satisfied that they meet the requirements in sections 23 to 25 of the Act, any criteria for the assessment of applications, and any other requirements set by regulations.

We propose that that the regulations provide for the TF Authority to use the following criteria to assess applications for accreditation: The TF Authority is satisfied that the applicant:

- Meets the New Zealand residency requirements specified in regulations;
- Does not present a national security risk or conflict with New Zealand's national interests if accredited to deliver a Trust Framework service;
- Intends to deliver one or more of the digital identity services specified in regulations established under the Act;
- Has the capability to meet the service standards and processes specified in the rules;
- Has demonstrated it will provide an internal complaints and dispute resolution process that meets regulatory requirements;
- Is not in receivership, liquidation, bankrupt or subject to a No Asset Procedure that would result in it being unable to deliver an accredited service;
- Has provided all the information specified in section 25 about the applicant and satisfied the TF Authority that any criminal conviction or any past practices as an identity services provider that have either been the subject of an investigation by the Privacy Commission or the TF Authority or resulted in a decision to previously decline, suspend or cancel an accreditation, will not compromise the security, privacy, confidentiality, or safety of the information of any Trust Framework participant or the integrity or reputation of the Trust Framework as a whole;

[12] We anticipate the TF Authority will provide further operational guidance to help TF providers determine when a conviction, privacy investigation or other matters are expected to present an unacceptable risk to the delivery of accredited services.

- Has policies and processes in place for ensuring its staff recruitment and service contracting practices meet accreditation standards and will not compromise the security, privacy, confidentiality, or safety of information of any Trust Framework participants, or present a risk to the integrity or reputation of the Trust Framework.

The regulations will confirm the TF Authority is responsible for applying the criteria and making decisions about the accreditation of digital identity services and providers. The regulations will also confirm that when applying these criteria and before making decisions in accordance with s 26 of the Act, the TF Authority will seek advice from the Privacy Commissioner on matters relating to an applicant's compliance with the Privacy Act.

To inform the TF Authority's application of the assessment criteria the regulations will also enable the TF Authority to obtain system level advice from the Government Communications Security Bureau and the New Zealand Security Intelligence Service on how it assesses national security risks. The TF Authority will also be able to obtain information security advice from the Government Chief Information Security Officer through GCSB and protective security advice from the Government Protective Security Lead through the NZSIS.

Duration

Section 30(2) of the Act provides that the accreditation of a TF provider or service expires at the end of the period set by regulations. We propose the regulations specify that a service accreditation ends three years (36 months) after the date it is granted by the TF Authority.

During the Trust Framework's establishment phase, we consider a standard three-year period should apply to all Trust Framework providers. In setting this accreditation period we recognise that the TF Authority's ability to monitor TF provider compliance and performance will be informed by the reporting requirements specified in regulations. Moreover, the TF Authority has the power to investigate and audit TF providers compliance with the Act, rules and regulations.

We anticipate that the accreditation period is a matter the TF Authority may wish to review based on its experience administering the regulatory system two to three years after commencement.

Renewal

We propose that the TF Board consider recommending the introduction of regulations that refine the renewal application requirements when developing the next tranche of regulations. The aim will be to establish a renewal application process that provides the TF Authority with assurance that TF providers can continue to meet accreditation requirements, in particular any changes that have been introduced since an applicant's original accreditation, while minimising renewal application compliance costs.

Accreditation mark

If approved, a TF provider will be able to deliver the accredited service or services under the Trust Framework and display an accreditation mark that would apply to each accredited service. The accreditation mark that would be applied to each specific accredited service is an important distinguishing factor, as some organisations with accredited services could also provide non-accredited services, which do not display the accreditation mark.

The TF Authority will establish accreditation mark requirements under section 13 – regulations are not required. To reduce the risk of a user or relying party misunderstanding whether a TF provider is delivering an accredited service, we anticipate that the TF Authority

will only allow accreditation marks to be displayed against specific services, rather than being displayed as a 'generic' accreditation by the organisation.

Provisional accreditation

We are not proposing to develop additional regulations for provisional accreditation. Under section 32(5) of the Act, applications for provisional accreditation will need to be made in the manner established by the TF Authority. In doing so the applicant will need to demonstrate to the TF Authority that the organisation and their proposed services - when fully developed - will meet the requirements in the Act and the proposed regulations and rules that apply to full accreditation.

In practical terms provisional accreditation is a means for the TF Authority to provide a qualifying assessment. It enables potential TF providers to test their proposed services for development and investment purposes and obtain assurance that if they proceed with development as proposed they will meet the requirements for accreditation. For the avoidance of doubt, as specified in the section 32, a provider or service with provisional accreditation is not a TF provider or an accredited service for the purposes of the Act.

COMPLAINTS AND DISPUTE RESOLUTION

Part 6 of the Act establishes processes for dealing with complaints and disputes. It enables any person to complain to the TF Authority if they believe a TF provider has breached the TF rules, regulations, terms of use of accreditation marks, or provisions of the Act.

Section 28 of the Act also provides for regulations that set out requirements for TF providers to operate their own internal complaints and disputes resolution processes. These processes can be used as a first port of call by complainants to address and resolve issues directly with the TF provider. Any complaints not resolved using this internal system can then be referred to the TF Authority for consideration.

TF Provider internal complaints process

We propose that the regulations require that every TF provider must:

- Receive and consider complaints about any service provided by it where the provider has failed to comply with the TF rules, regulations, terms of use of accreditation marks, or other requirements arising from provisions in the Act;
- Establish and maintain policies and procedures for providing an accessible process for dealing with such complaints fairly, promptly, without undue formality and with due regard to tikanga Māori;
- Incorporate the use of any disputes resolution scheme or process the TF provider is a party to through their membership of a particular industry;
- Publicise its complaints policies and procedures to users, prospective users, relying parties and other stakeholders with an interest in its services; and
- Ensure that complainants are aware that in the event they are dissatisfied with the outcome of the internal complaints process they may lodge a formal complaint with the TF Authority.

The ability of an applicant to comply with these requirements will be assessed by the TF Authority when they apply for accreditation.

We anticipate the TF Authority will provide further guidance to TF providers on how their complaints processes should have due regard to tikanga Māori. The development of that guidance will be informed by advice received by the TF Board from the Māori Advisory Group

and any consultation with iwi and hapū undertaken by the Board and MAG in accord with their engagement policy when it is established.

Potential future regulations for a dispute resolution scheme

The Act also allows for the development of regulations to establish requirements and criteria that would enable the TF Authority to recommend a dispute resolution scheme for the Minister's approval. Any scheme would need to complement and operate alongside the TF Authority's complaints process which can lead to the TF Authority applying a range of remedies where it finds a TF provider has breached legislative requirements.

It is, however, too early to determine whether a disputes resolution scheme is necessary to support or complement the TF Authority's complaints, investigation and compliance management functions. We propose, therefore, that the TF Board consider whether to recommend the establishment of enabling regulations to the responsible Minister after it has had the opportunity to review the operation of the TF Authority's complaints process. We propose that this review would take place within 3 years of the Act's commencement.

Complaints and dispute resolution process

Appendix B.1 places the proposed regulations within the context of the overall complaints and dispute resolution process provided for in the Act.

RECORDKEEPING

The Act enables the establishment of regulations requiring TF providers to collect required information about its activities and hold that information for a set period.

In accordance with section 42 of the Act, the regulations will require TF providers to collect and retain information about their activities, store it securely, and provide the TF Authority with access to those records at all reasonable times upon request.

The regulations will require the TF provider to retain information necessary to provide assurance that it has delivered accredited services in accordance with the requirements specified in the Act, rules and regulations. Where information received by the TF provider is personal information as defined in the Privacy Act 2020, the regulations will allow the provider to keep a record of the source of the information used in the provision of digital identity services rather than the personal information itself.

Content: The records to be retained by TF providers will include information such as data about transaction activities, events and actions that occur in the normal course of users starting, progressing and completing their digital transaction.

Duration: The regulations will require TF providers to retain their records for a minimum of 12 months from the date of last use (for compliance with complaints and dispute resolutions purposes) or for the period in which the accreditation is valid plus a further 12 months from the date of last use where required. These durations should ensure the TF Authority can access records necessary for regulatory system monitoring and compliance management activities without imposing unnecessary recordkeeping compliance costs on TF providers.

Timely Access: The regulations will specify that TF providers must retain records in a manner that ensures timely access to them by the TF Authority upon request. The timeframes that TF providers must meet in providing access to those records is established under s 62.

Data Security and Integrity: The regulations will include an obligation for the TF provider to have systems in place for ensuring their records are stored securely in a manner that ensures they remain unaltered and true to their original state.

Record Disposal: The regulations will specify that TF providers must have a secure way of disposing of records.

The regulations establish the recordkeeping requirements necessary to provide assurance that a TF provider has met their obligations and delivered accredited services in accordance with the requirements specified in the Act, rules and regulations.

TF providers will also need to meet recordkeeping obligations established under other legislation such as, for example, the Companies Act 1993, the Goods and Services Tax Act 1985, Securities Act 1978, Tax Administration Act 1994, the Consumer Guarantees Act 1993, the Public Records Act 2005 or the Privacy Act 2020.

REPORTING

Section 42 of the Act enables the regulations to establish TF provider reporting requirements.

Periodic Reporting: The regulations will require every TF provider to provide periodic reports to the TF Authority. This will contribute to the TF Authority's ability to monitor and assess the performance of each TF provider and the overall regulatory system. TF providers will need to submit information on a template provided by the TF Authority on:

- *Service use:* Service transaction volumes and the number of credentials issued (six-monthly and annually);
- *Service Delivery:* Steps taken to ensure accredited services are delivered in accordance with required service standards; any breaches of service standards, and actions taken to remedy them; and steps taken to improve service delivery (annually);
- *Complaints and Disputes Resolution:* Number and type of complaints made to the provider; and the outcomes achieved by the TF provider's complaints and disputes resolution processes, including instances where the TF provider has upheld the complaint and implemented remedies to ensure its service meets compliance requirements (annually);
- *Incident reporting:* The status and outcome of any cyber-security incidents, actual or suspected fraud events, or any other events that adversely affect privacy or confidentiality, the integrity or availability of the digital identity service, or have caused or present a risk of causing, serious harm to TF participants which have been the subject of notification to the TF Authority in the reporting period (annually); and,
- *Incident Notification:* Requirements for notifying the TF Authority of any cybersecurity incidents, fraud events, or any other events that adversely affect privacy or confidentiality, the integrity or availability of the digital identity service, or have caused or present a risk of causing serious harm will be established in regulations under s 28(2). We anticipate that the TF Authority will require TF providers to provide an update on the outcome of any event notified to it. At the TF Authority's discretion this may substitute for annual incident, status or outcome reporting.

For the avoidance of doubt, the regulations will also refer to TF providers' obligations under the Privacy Act 2020 to report privacy breaches that have caused serious harm to the Privacy Commissioner and require the provider to also inform the TF Authority.

These reporting requirements are designed to ensure the TF Authority is aware of significant events and can intervene or assist to resolve issues where appropriate. The regulations will also align the definition of serious harm and notification expectations and processes with those established under the Privacy Act by the Privacy Commissioner.

Accordingly, serious harm is the unwanted sharing, exposure or loss of access to personal or organisational information that may cause individuals or groups serious harm. Examples of serious harm include:

- Physical harm or intimidation;
- Financial fraud including unauthorised credit card transactions or credit fraud;
- Family violence;
- Psychological or emotional harm; and,
- Disruption to international trade, or New Zealand's economic wellbeing and security.

TF providers will be required to notify the TF Authority of any events as soon as they are practically able. The TF Authority will provide operational guidance to TF providers on the reporting requirements. This advice will be developed in consultation with other government agencies including the Office of the Privacy Commissioner, the Government Chief Information Security Officer and the Government Protective Security Lead.

The regulations do not need to cover notification of changes that may impact on an applicant or TF provider's accreditation status. Section 33 of the Act already includes an obligation for applicants and TF providers to tell the TF Authority of any changes to the information provided under s 24(1)(b)(i) and s 25(1) relating to their application for accreditation within 5 working days of the change occurring. This may, for example, include changes to TF provider ownership, changes in personnel, business processes or systems.

The TF Authority can then take this information into account and where necessary reconsider a TF provider's accreditation status in accordance with its accreditation decision criteria.

COST RECOVERY

The Act includes provision for the establishment of regulations to recover certain costs through fees, including the cost of administering the accreditation process and more generally the costs of operating the Trust Framework.

It is anticipated that the TF Authority's initial establishment and first two years of operating costs will be met from Crown funding without a contribution from fees.

Consultation on cost recovery regulations relating to the TF Authority's administration of the accreditation process and the Trust Framework more generally will take place before they are established.

We recognise that participation from users, TF providers, and relying parties in the digital identity system enabled by the Trust Framework is essential to giving people greater control of information about themselves, and to access services more easily.

In recommending any cost recovery regulations we anticipate the TF Board will, therefore, consider what impact cost recovery arrangements have on participation. In setting fair and equitable fees, it is anticipated the TF Board will distinguish between the TF Authority's services that deliver a significant private good and those that are more generally considered to deliver a merit or public good.[13]

[13] According to NZ Treasury Guidelines, a private good is one where people can be excluded from its benefits at a lower cost and use by one person conflicts with use by another. Examples of private goods include passports, birth certificates and licenses. In our case the provision of an accreditation can be considered a private good.

A merit good is one that is likely to be produced at a lower level than the community desires in a free market situation. This may be because the public benefit of the good is greater than the private benefit, and consumers only consider the private benefit when making decisions.

A public good is one where excluding people from its benefits is either difficult or costly and its use by one person does not detract from its use by another. There is a good case for recovering the cost of a public good through general taxation or, if the benefits are localised, from local government revenue. Examples include national security and street lighting. Many services provided by Government share the characteristics of public goods to some extent. Although such services might have some elements of public good, there still might be justification for recovering costs.

Appendix B.1 – Complaints and Dispute Resolution Process

Figure 2 places the proposed regulations within the context of the overall complaints and dispute resolution process provided for in the Act.

Complaints must be about breaches: Under the Act the TF Authority is charged with addressing complaints received from any person that believes a TF provider has breached the provisions of the Act, the rules, the regulations, or the terms of use for the accreditation mark.

The Complainant must try and resolve a complaint directly with the TF Provider before involving the TF Authority: Complainants are expected to make reasonable efforts to resolve a complaint directly with the TF provider concerned before involving the TF Authority. This should involve using a TF provider's internal complaints resolution process and utilise any disputes resolution scheme or process that the TF provider is a party to through their membership of a particular industry.

Preliminary Assessment: When the TF Authority receives a complaint, it will complete a preliminary assessment. The assessment process will include providing the TF provider with the opportunity to comment on the complaint. The preliminary assessment can result in the TF Authority:

- Referring the complaint (in full or in part) to the Ombudsman, the Privacy Commissioner, the Inspector-General of Intelligence and Security[14] or another officeholder when, following consultation with those officeholders, the TF Authority determines the complaint falls within their jurisdiction and would be more appropriately dealt with by them;
- Informing the parties to the complaint that it will not consider the complaint further and explaining its reasons (the reasons for not further considering a complaint are outlined in section 73 of the Act); or
- Deciding that a breach appears to have occurred.

The TF Authority will advise the complainant and the TF provider or providers of its preliminary assessment and its reasons for it. Where its assessment is that it a breach may have occurred, the TF Authority will inform the parties about its powers of investigation and the remedies it may grant, and also provide information on any dispute resolution scheme run by the Authority.

Investigation: Following the preliminary assessment process the TF Authority may commence an investigation after notifying the TF provider of its intention to do so. The requirements the TF Authority must meet for conducting an investigation are established in section 80 of the Act.

[14] The Inspector-General of Intelligence and Security provides independent oversight of the New Zealand Security Intelligence Service and the Government Communications Security Bureau. The Inspector-General can investigate complaints against the intelligence agencies.

Findings: If the TF Authority is satisfied that a breach has occurred, it will provide the TF provider and the complainant with written notice of its decision and the reasons for it.

Remedies: The TF Authority may also apply one or more of the following remedies after first giving the TF provider a reasonable opportunity to make submissions on the remedies:

- Issuing a private or public warning;
- Requiring the TF provider to meet additional record-keeping or reporting requirements;
- Issuing a compliance order requiring the TF provider to remedy the breach;
- Suspending the TF providers accreditation or the accreditation or the relevant service; and
- Cancelling the TF provider's accreditation or the accreditation of the relevant service.

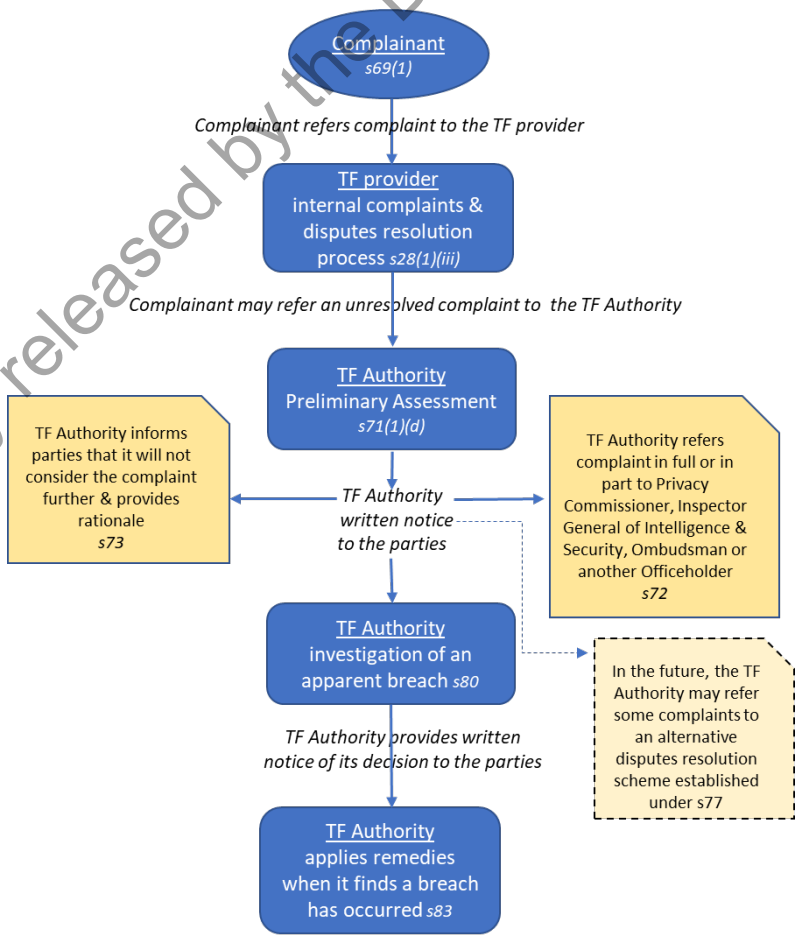
Redress through the courts

The Act enables the provision of accessible, fair, efficient, and effective complaints and dispute resolution processes that have particular regard to tikanga Māori.

Participants in the Trust Framework system are also able to pursue civil claims under the general law in the usual way (for example, any private contractual disputes or negligence claims, subject to the limited immunity in section 104 of the Act for TF providers).

Decisions made by the TF Authority, including those relating to the complaints and dispute resolution process, may be subject to judicial review by the High Court.

Figure 2: Trust Framework Complaints and Dispute Resolution Process



Appendix C – Targeted Stakeholder Engagement

The Department released a discussion paper in August 2023 that reflected the key elements of option 2. It informed a 4-week targeted engagement process on the proposed regulations.

The paper was circulated to 40 private sector and non-government organisations, the Data Iwi Leaders Group, and 40 public service organisations and introduced at two online engagement workshops. The Department received submissions and other feedback from 19 organisations. This included submissions from peak bodies including Digital Identity New Zealand that represents over 100 organisations, and the Data Iwi Leaders Group.

The targeted engagement process confirmed there is broad support for the Trust Framework. There was also support for our preferred approach to developing the enabling regulations, subject to some proposed modifications.

The Department's preferred approach to the development of the regulations has been refined to address stakeholder concerns and suggested improvements where they align with good regulatory practice and the achievement of the Act's objectives.

The changes proposed by stakeholders, which we have adopted, define the intent of the regulations more clearly, reduce compliance costs, better mitigate risks to the Trust Framework's integrity and signal the intent to provide operational guidance to TF providers on how to meet regulatory requirements.

The changes to the preferred as a result of stakeholder engagement include:

a. *Digital Identity Services:* Providing fuller descriptions of the five digital identity services to be specified in regulations to clarify their scope and the rationale for them.
b. *Accreditation Requirement - Residency in New Zealand:* Replacement of a 'New Zealand incorporation' requirement with a more clearly defined 'residency in New Zealand' requirement for individuals and entities seeking accreditation.
c. *Accreditation Requirement – Receivership, Liquidation or Bankruptcy Information:* Replacing a requirement for applicants to provide information that would support a financial sustainability assessment with a narrower and more readily verifiable declaration that applicants are not in receivership, liquidation, bankrupt or subject to a No Asset Procedure.
d. *Accreditation Requirement – Section 25(1) Verification:* Replacement of a Police vetting check with a Ministry of Justice criminal record check. Clarification of the requirements that apply to new staff and service providers a TF provider wishes to contract, including the expectation that the TF Authority will provide further guidance to help providers determine when a conviction, privacy investigation or other matters are expected to present an unacceptable risk to the delivery of accredited services.
e. *Accreditation Requirement – Service Levels:* Removal of a requirement for applicants to meet a separate 'Service Level' capability requirement in addition to the level of assurance requirements provided for in the rules (upon reflection we consider the levels of assurance requirements which will be specified in the rules are sufficient).
f. *Accreditation Assessment Criteria:* Refined criteria that reflect the amended accreditation application requirements together with the inclusion of criteria relating to national security.

g. *Accreditation Assessment Criteria Advice:* Clarification that while the TF Authority will make all accreditation decisions, it will first obtain advice from the Office of the Privacy Commissioner on matters relating to an applicant's compliance with the Privacy Act. In addition, provision has been made for the TF Authority to obtain system level advice from GCSB and NZSIS on how it assesses national security risks. The TF Authority will also be able to obtain information security advice from the Government Chief Information Security Officer through GCSB and protective security advice from the Government Protective Security Lead through NZSIS.

h. *Duration:* Increasing the accreditation period from two years to three years.

i. *Accreditation Mark:* Clearer explanation that accreditation marks will be established under s13 and that regulations will not be required.

j. *Provisional Accreditation:* Clearer explanation that provisional accreditation – which is enabled directly by the Act and will not be subject to further requirements prescribed in regulations in this phase - is a means for the TF Authority to provide a 'qualifying assessment' and that provisional accreditation does not enable the provider to trade as an accredited provider or offer an 'accredited service.'

k. *Complaints:* Explanation that the TF Authority will provide further guidance to TF providers on how their complaints processes should have due regard to tikanga Māori with acknowledgement that this guidance will be developed in accord with the engagement policy established by the TF Board and MAG.

l. *Recordkeeping:* Better definition of the records that need to be retained by TF providers, a reduction in the period they need to be retained for, together with improved data security, retention and disposal requirements.

m. *Reporting:* Replacement of an annual report requirement with narrower periodic reporting requirements using TF Authority templates, including the removal of financial reporting.[15] Improved incident notification requirements that include cyber security incidents together with the inclusion of a definition of serious harm and incident notification expectations and processes that are better aligned with those established under the Privacy Act.

n. *Reporting guidance:* Recognition of the need for the TF Authority to provide operational guidance to TF providers on periodic and incident reporting that takes account of guidance from other government agencies including the Office of the Privacy Commissioner, the Government Chief Information Security Officer and the Government Protective Security Lead.

There may, however, be some residual stakeholder concern around our intention to address cost recovery and accreditation renewal arrangements in a second round of regulations. Likewise, some stakeholders may continue to advocate for early introduction of experience or risk-based distinctions in the accreditation process.

Some submitters are concerned that leaving the development of cost recovery and renewal arrangements until later in the Trust Framework's implementation phase created short term uncertainty for potential entrants and could impact adversely on uptake.

We consider this concern is outweighed by:

- The delay in enabling the establishment of the regulatory system that would be required to develop these additional regulations;

[15] TF provider financial information obtained through periodic reporting is not considered necessary to discharge the TF Authority's core functions at this time.

- The higher risks associated with setting fees at this time given the uncertainties around uptake, the operation of the regulatory system and the TF Authority's cost structure; and,
- The incentive available to applicants to obtain accreditation before any fee regime is established.

Some stakeholders have suggested that there was scope to differentiate between applicants for accreditation based on the type of organisation and their risk profile (for example public service organisations could be exempt from meeting some requirements). Other stakeholders raised concerns with this approach. While we see merit in a regulatory system that takes account of the risks posed by regulated parties it presents development and implementation risks in the establishment phase.

We consider standard requirements should apply to all applicants in the regulatory system's establishment phase. The introduction of provisions that enable regulated party experience (performance and risk rating) to be considered or distinctions to be made between different types of provider is something that the TF Board may wish to consider as the regulatory system matures, and the TF Authority develops a better understanding of regulated party behaviour.

The engagement process also highlighted wider implementation issues and risks that go beyond the development of the regulations. This wider feedback will inform the approach adopted by the TF Board and TF Authority to the implementation of the Trust Framework.

Appendix D – Glossary of key terms

Term	Definition
Accreditation	An act to give approval to a digital identity service provider who has demonstrated they meet the applicable requirements of the Trust Framework.
Accredited digital identity service or accredited service	A digital identity service accredited by the TF Authority to be provided by a particular TF provider.
Digital identity	A digital representation of a person's identity information and other attributes about them they can use to prove who they are online and digitally to access services.
Digital identity service	A service or product that, either along or together with one or more other digital identity services, enables a user to share personal or organisational information in digital form.
Digital identity service provider	An individual or organisation that provides a digital identity service, whether the provider or service is accredited under the Trust Framework or not.
Digital Identity Services Trust Framework; or Trust Framework	Has the meaning given in section 8 of the Act. The legal framework established to regulate the provision of digital identity services for transactions between individuals and organisations.
Relying party	An individual or an organisation that relies on personal or organisational information shared, in a transaction with a user, through one or more accredited digital identity services
TF Authority	The Authority established under section 58 to oversee the running of the Trust Framework.
TF Board	The Board established under section 42 of the Act to oversee the TF Authority.
TF provider	A digital identity service provider accredited by the TF Authority to provide one or more accredited digital identity services.
User	An individual who- (a) shares personal or organisational information, in a transaction with a relying party, through one or more accredited digital identity services; and (b) does so for themselves or on behalf of another individual or an organisation