Internal Affairs
Te Tari Taiwhenua

Regulatory Impact Statement: Digital Identity Services Trust Framework Regulations, Tranche Two

Decision sought	Analysis produced for the purpose of informing final Cabinet decisions and approval to authorise drafting instructions.
Agency responsible	Department of Internal Affairs
Proposing Ministers	Minister for Digitising Government
Date finalised	23 October 2025

The Digital Identity Services Trust Framework Act 2023 (the Act) came into force in 2024. The Act establishes a regulatory body, the Trust Framework Authority, that regulates the provision of digital identity products and services by providers. The Trust Framework is an opt-in scheme that enables public and private entities providing digital identity services, such as:

- organisations that provide digital identity information,
- deliver services like those that connect information to a person,
- provide products such as verifiable credentials to users, or
- those delivering any other service as defined under the existing Digital Identity Services Trust Framework Regulations 2024 [the regulations])

to seek accreditation for the provision of those decentralised digital identity services. Any entity that provides those services, including the government, private companies, and even individuals could theoretically opt into accreditation.

Working with accredited digital identity providers will enable people and organisations to verify information more easily, faster, and with a high level of confidence. Research suggests the benefit of a secure digital identity ecosystem is between 0.5-3% of GDP (approximately NZD$1.5-$9 billion).

The Minister for Digitising Government (the Minister) is proposing regulations for the Act that will support the Act's operation and provide certainty to groups wishing to participate in the Digital Identity Services Trust Framework.

The proposed regulations will:

- set out the **renewal process** for participating organisations to renew their accreditation;
- define **levels of assurance** so that providers of information or verification services have a legislative framework to assert how strong attributes are; and
- relieve the administrative burden of **reporting requirements** by amending the reporting periods set out in the first tranche of regulations to align with the year-end and government financial year-end periods.

Summary: Problem definition and options

What is the policy problem?

The Digital Identity Services Trust Framework needs further regulations to provide certainty on how the system will operate and minimise administrative burdens

The Digital Identity Services Trust Framework Act 2023 (the Act) established a regulatory framework for the provision of secure and trusted digital identity services (the Trust Framework), including verifiable credentials.

Due to the phased approach to regulations, some administrative areas essential to the running of a regulatory framework were not included in the first tranche of regulations, which focused on functions critical to beginning the accreditation of potential Trust Framework providers. As such, the Trust Framework does not have regulations for some of the functions that are expected of a regulator, such as specific renewal requirements.

The lack of certainty around these functions means that providers do not have certainty on how they will be regulated under the system and the ongoing obligations that they will need to meet to participate in the Trust Framework. This may inhibit uptake of providers seeking to become accredited within the Framework and reduce confidence of people and organisations in using accredited providers.

There is a further opportunity to reduce the administrative burden on providers by streamlining reporting requirements, which would further remove disincentives for providers to participate in an opt-in framework which, as of the time of the drafting of this regulatory impact statement, has no providers. If there continues to be little to no uptake in the Trust Framework by digital identity providers, this will hinder New Zealand's ability to provide digital solutions for, and increase efficiency in, identity verification and the benefits of the regulatory system will not be achieved.

Additionally, the strength of a piece of digital identity information is currently difficult to articulate to those that are not technical experts, including users and relying parties who will be the main users of digital identity products and services. Making the strength of that information easier to articulate would make it easier for users and relying parties to understand Trust Framework identity products and increase the attractiveness of participating in the Trust Framework.

We have considered non-regulatory options such as guidelines issued by the regulator (the Trust Framework Authority), but note that these would not provide sufficient certainty for those seeking to participate in the Trust Framework. This view was supported by stakeholders in our consultation.

What is the policy objective?

The proposed regulations aim to incentivise potential participants to enter the Trust Framework by clarifying the ongoing requirements of participation, as well as lessening the burden for participation. Having providers participate in the Trust Framework will lead to improved efficiency through enabling more, and safer, digital transactions and reduced risk of fraud. The lack of trusted digital identity service providers could exacerbate the risk of privacy breaches and fraud.

The Department has identified three policy objectives for this work:

- Minimise the barriers to participation in the Trust Framework, including any administrative burdens;
- Maintain the integrity of the Trust Framework, and confidence that the providers and services accredited under the Trust Framework are secure and trusted; and
- Ensure that the obligations set out under legislation are clear to all participants.

As there are no participants in the Trust Framework yet, it would be difficult to assess success through an objective measure. However, the regulations will have succeeded if organisations that begin to participate in the Trust Framework do not find participation overly burdensome and understand how different attributes should be dealt with.

What policy options have been considered, including any alternatives to regulation?

We have considered three aspects of the Trust Framework

Accredited providers need certainty on what they will need to provide to renew their accreditation before it expires

Three options have been identified in addition to the status quo. At a high level:

- **Option one: Status quo –** when seeking renewal, accredited Trust Framework providers need to provide the same information as a new application from an unknown service provider.
- **Option two: Standardised renewal –** renewal applications have requirements that are standard across all providers, but are less burdensome than a new application.
- **Option three: Risk-based renewals –** renewal applications have requirements that are different for providers, based on the level of risk that the Trust Framework Authority considers that the provider poses.
- **Option four: Hybrid model (preferred) –** renewal applications have requirements that are standard across providers within different tiers, which will be set out under regulations.

The different strengths of attributes under the Trust Framework should be clear to users, relying parties, and service providers

Three options have been identified in addition to the status quo. At a high level:

- **Option one: Status quo –** levels of assurance are set by identification standards, a non-regulatory set of guidance that is administered by the Department of Internal Affairs and aimed at technical experts.
- **Option two: Five levels of assurance –** a suite of levels with the “standard” level split between standard, which requires binding, and standard plus, which requires biometric binding.
- **Option three: Four levels of assurance –** a more stringent suite of levels of assurance, with a standard level of assurance needing biometric binding.
- **Option four: Four levels of assurance, with methods (preferred) –** a suite of levels that are similar to option two, but with the ability for the Trust Framework Authority to affix a ‘plus’ to attributes that have used biometric binding to reach the level.

Reporting periods should be amended to prevent placing unnecessary resourcing burden on accredited providers

Only the preferred option and the status quo have been considered.

- **Option one: Status quo –** six-monthly and annual reporting periods remain set at 1 January and 1 July.
- **Option two: Amendment (preferred) –** six-monthly and annual reporting periods are amended to be on 1 March and 1 September.

We considered non-legislative options during policy development

During the development of the levels of assurance regulations, we also considered non-legislative options, including using guidance to support understanding of the identification standards. These were ultimately dismissed as we consider that legislative options would provide the certainty that users, relying parties, and providers will need to participate in the Trust Framework. Other regulatory frameworks that deal with identity (such as those that verify age or entitlement to services) also need legislative certainty before they are able to align with the Trust Framework and Trust Framework products and services. A strong preference for certainty provided by setting requirements in legislation was shown in feedback from stakeholders.

What consultation has been undertaken?

Targeted consultation took place between Monday 11 August 2025 to Monday 1 September 2025, a period of three weeks. This approach was appropriate as the proposed regulations focus on administrative requirements solely relevant to service providers. We received 24 submissions in response.

The preferred option for the **renewal process** was developed in response to feedback from submitters. Stakeholders were broadly supportive of the preferred option for setting **levels of assurance**, and strongly supportive of amending the reporting periods set out in the first tranche of regulations to relieve the administrative burden of **reporting requirements**.

Is the preferred option in the Cabinet paper the same as preferred option in the RIS?

Yes.

Summary: Minister’s preferred option in the Cabinet paper

Costs (Core information)

The proposals do not impose any additional direct costs relative to the status quo. Each of these regulations deal with processes that already exist under the status quo – there is a renewal process in place currently, levels of assurance are governed under existing identification standards, and reporting requirements remain identical to the proposals.

Benefits (Core information)

The benefits of the proposed regulations will accrue to providers participating in the Trust Framework as they will face less administrative burden. This will encourage participation in the Trust Framework which will help grow the digital identity market.

The establishment of a trusted digital identity market will enable people and organisations to verify information more easily, faster, and with a high level of confidence. Research suggests the benefit of a secure digital identity ecosystem is between 0.5-3% of GDP (approximately NZD$1.5-$9 billion).

If there continues to be little to no uptake in the Trust Framework by digital identity providers, this will hinder New Zealand's ability to provide digital solutions for, and increase efficiency in, identity verification and the benefits of the regulatory system will not be achieved. The lack of trusted digital identity service providers could also exacerbate the risk of privacy breaches and fraud.

Balance of benefits and costs (Core information)

Does the RIS indicate that the benefits of the Minister’s preferred option are likely to outweigh the costs?

Yes. There are no ongoing costs to any of the proposals as they deal with already existing processes or requirements. The benefits would be that providers may be more strongly encouraged to opt into the Trust Framework and as such create a trusted digital identity market in New Zealand.

Implementation

How will the proposal be implemented, who will implement it, and what are the risks?

The Trust Framework Authority will be responsible for administering the accreditation renewal framework, as well as to ensure accredited providers are meeting reporting requirements. They will also be responsible for monitoring the different levels of assurance of attributes. The Trust Framework Authority already has existing responsibility for renewals and monitoring as they are the regulator established under the Act, so the implementation risks are minimal.

The proposed regulations are expected to come into force in early 2026. Although the regulations setting out the renewal process will not be required for at least three years, when the first accredited providers accreditation period ends, having regulations in place is expected to encourage providers to enter the Trust Framework. The levels of assurance regulations will be needed when providers enter the Trust Framework, and there are also interdependencies with other regulatory regimes which are incorporating the Trust Framework and which we anticipate will refer to levels of assurance.

Limitations and Constraints on Analysis

Focused targeted consultation occurred over three weeks and was limited to a very targeted group of stakeholders

Targeted consultation occurred over a short period of time and with potential Trust Framework providers, peak industry bodies, and the public sector. A key limitation is that there are, as of the writing of this assessment, no participants within the Trust Framework, so submitters gave their feedback based on what they anticipated to be the issues, rather than experience within the system. There were also low levels of response.

We consider that the limitations and constraints described above have limited impact on the quality of the analysis as the proposals focus mainly on requirements that are placed on accredited providers. One of the proposals that interprets the current identification standards places no requirements on any party, but will be of most relevance to providers who may wish to reach a certain level of assurance for the products they wish to provide. The Trust Framework remains voluntary, and these requirements do not impact those who are not part of the framework.

Key assumptions were made

The key assumptions underpinning this analysis are that:

- relieving the administrative burden will incentivise more digital identity service providers to enter the Trust Framework;
- providing clarity on how digital identity credentials will be treated will encourage users and relying parties to use them; and
- more accredited providers will result in better digital identity verification.

The Department has not completed an integrated and quantified cost-benefit analysis of the proposed regulations. Our assessment of the regulations is qualitative and draws on the professional judgement of Departmental legislative and regulatory subject matter experts and feedback from stakeholder engagement. While there is not a clear impact value available for participation in the Trust Framework, research suggests the benefit of a secure digital identity ecosystem is between 0.5-3% of GDP (approximately NZD$1.5-$9 billion) and the United Kingdom Government's *State of digital government review* found that the full digitisation of public sector services could bring savings and productivity benefits to the effect of 4-7% of public sector spend, which a trusted digital identity would bring us closer towards.[1]

[1] State of digital government review - GOV.UK, pp. 5 and 14

I have read the Regulatory Impact Statement and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the preferred option.

Responsible Manager(s) signature: ______________________

Kelsea Whyte
Policy Manager, Digital and Identity
23/10/2025

Quality Assurance Statement

Reviewing Agency: Department of Internal Affairs	**QA rating:** Meets criteria

Panel Comment:

The panel considers that the information and analysis summarised in the RIA meets the Quality Assurance criteria.

The Department of Internal Affairs has reviewed the Regulatory Impact Statement (RIS) prepared by the Department of Internal Affairs. We have met several times and requested additional changes to the original document. The last full meeting was on 17 October 2025, with some subsequent changes suggested at this time.

The panel noted that the authors have been very proactive in taking on board recommendations from the panel. While the length of the document has been a consideration, we recognise this is an evolving and important issue to address, particularly so that providers have increased certainty about their requirements and compliance requirements going forward. Also so that the community can have trust in the digital identity services that they access.

Consultation with appropriate stakeholders has been undertaken. This is important given the limited number of present providers involved, but also recognising the ongoing importance of the issue to overall digital security integrity.

We recognised that this RIS is dealing with a process that is still in it its initial phase; however, the framework appears to provide increased recognition of the changes that might be needed to both ensure continued confidence in users, but also to reduce on-going compliance costs for providers of these services.

Glossary of terms

Term	Meaning
Accredited provider	A digital identity service provider accredited by the Trust Framework Authority.
Accredited service	A digital identity service accredited by the Trust Framework Authority to be provided by an accredited provider.
Attribute	An attribute is a piece of information, such as a date of birth or a name. An attribute will most likely make up part of someone's digital identity.
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. An example is a binding service, which connects information from a user to a credential.
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.
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.
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.
Trust Framework Authority	The regulator of the Trust Framework under section 58 of the Act, which oversees the running of the Trust Framework.
Trust Framework participants	Anyone participating in the Trust Framework, including providers, relying parties, and users.
User	An individual who shares personal or organisational information, in a transaction with a relying party, through one or more accredited digital identity services.

Section 1: Diagnosing the policy problem

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

The Digital Identity Services Trust Framework is operational but does not have all the administrative functions expected of a regulator

1. Many government and private sector services are now provided online. New Zealanders should be able to access services and complete transactions remotely, rapidly, and with minimal paperwork.
2. The Digital Identity Services Trust Framework Act 2023 (the DISTF Act) came into force in 2024. The DISTF Act established a regulatory body – the Trust Framework Authority (the Authority) – which regulates the provision of secure and trusted digital identity services through an accreditation framework (the Trust Framework). This enabled organisations such as those that provide digital identity information, deliver services like those connecting information to a person, or provide products such as verifiable credentials to users to seek accreditation for the provision of those services (or any other as specified under the first tranche of regulations).
3. In October 2024, an initial tranche of regulations was made to support the implementation of the DISTF Act, which enabled the operation of the Authority and established the legal and administrative requirements for digital identity service providers looking to enter the Trust Framework. The tranche covered matters that the Department considered critical to starting the Trust Framework but did not cover all the administrative functions expected of a regulator as it was part of a phased process. The Department has identified three areas where further regulations could support the smooth operation of the Trust Framework.

There are no regulations specifying a distinct renewal application process for accredited providers under the Trust Framework

4. The first area is around **renewing an accreditation** under the Trust Framework. The first tranche of regulations established a three-year period of accreditation, after which accredited providers need to renew their accreditation if they wish to remain in the Trust Framework. Section 31(5) of the DISTF Act provides that unless otherwise specified in regulations, applications to renew accreditation from accredited providers must contain the same amount of information as an original application for accreditation (that is, from providers who are not accredited).
5. There are currently no regulations specifying a renewal application process. As such, accredited providers looking to renew their accreditation must provide all of the information specified under Regulation 6 of the Digital Identity Services Trust Framework Regulations 2024 (the first tranche of regulations).

Legislation does not differentiate between the strengths of attributes under the Trust Framework

6. The second area is around **the strength of different attributes**. Under the Trust Framework, participants use and rely on personal identity information that comes from different sources. These sources vary in how rigorous their verification processes are, and therefore how "strong" an attribute is. For example, name information on a driver licence is not as strong as name information from a birth certificate, because birth certificates are direct copies of an authoritative source (i.e. the birth registry).

7. These differences in strength are currently governed by the identification standards, which express assurance along three distinct aspects: information, binding, and authentication assurances. Under the standards, the strength of a service, or attribute within that service, is currently asserted as Information Assurance X, Binding Assurance Y, Authentication Assurance Z (where X, Y, and Z are the levels to which each aspect is met). This is a complex assertion.

8. Additionally, the identification standards are not currently set out in legislation, meaning that these assertions do not hold legal weight.[2]

The reporting periods set out in the first tranche of regulations overlap with resource-intensive times of years for organisations

9. The third area is a minor issue around **reporting requirements**. The first tranche of regulations set a requirement that accredited providers must provide the Authority with six-monthly reports on 1 January and 1 July, and a 12-monthly report on 1 January. These periods overlap with the year-end and government financial year-end period, which are likely to be resource-intensive times of the year for organisations and increase the administrative burden on them for participating in the Trust Framework. 1 January is also a public holiday.

How is the status quo expected to change and evolve in the absence of action?

The Trust Framework is a voluntary framework that is still emerging

10. The Trust Framework is a voluntary framework. Its impact is reliant on providers opting into the framework and providing a variety of digital identity products and services in New Zealand. There are no accredited providers in the system as of the drafting of this Regulatory Impact Statement.

11. The technology, products and services that the Trust Framework will regulate, such as verifiable credentials and the technical infrastructure that will allow them to be held on devices, are still evolving in New Zealand and internationally. As such, there is no robust evidence base for the Department to draw on and it is difficult to say how the market will develop in the absence of any change.

12. While we are anticipating that some accredited providers will enter the Trust Framework in late 2025, it is still unclear what the level of participation will be. Continued low levels of uptake in the Trust Framework would hinder New Zealand's ability to provide digital solutions for, and increase efficiency in, identity verification.

13. While we cannot draw a direct line from the administrative burden of participating in the Trust Framework and uncertainty as to how providers might be regulated to the low levels of participation within the Trust Framework, removing unnecessary barriers would incentivise potential participants to opt into the voluntary Trust Framework.

The three areas we identified above will continue to create barriers to participation in the Trust Framework in the absence of action

14. The first area we identified deals with **accreditation renewal requirements**. With no regulations specifying a renewal application process, accredited providers must undergo a full application process to renew their accreditations. This goes against standard regulatory practice and places an unnecessary level of administrative and financial

[2] The identification standards are developed and maintained by the Department of Internal Affairs' identification management team (Identification Standards | NZ Digital government).

burden on accredited parties looking to renew their accreditation. Without action, this will likely continue disincentivising organisations from entering into the Trust Framework.

15. The second area we identified deals with **levels of assurance** (at paragraph 7). The complex assertion under the current identification standards means that participants within the Trust Framework, particularly users and relying parties, will find it difficult to understand how strong a certain attribute or credential is. Without action it will continue to be difficult for people – especially those that lack technical expertise – to determine if Trust Framework attributes sufficiently meet their needs (e.g., a legal obligation or an internal appetite for risk). The identification standards are also not set out in legislation, and without action it will be difficult for other regulatory regimes to rely on Trust Framework attributes.

16. The third area is on **reporting requirements** (at paragraph 10), which are currently set during periods that are likely to be resource-intensive as organisations work to comply with other regulatory regimes. This overlap increases the administrative burden of reporting to the Authority and as such without action would continue to be a barrier to entry into a voluntary framework.

The Customer and Product Data Act 2025 established a similar framework that allows businesses to share customer and product data

17. The Customer and Product Data Act 2025 (CPD Act) establishes an overarching framework to enable greater access to, and sharing of, customer and product data between businesses. The Trust Framework will support this framework as it will make it easier for businesses to verify people seeking to access their data. If the Trust Framework continues to have little to no uptake among providers, it will not be able to support the CPD Act.

What is the policy problem or opportunity?

18. The first tranche of Digital Identity Services Trust Framework Regulations did not cover all the administrative functions expected of a regulator, meaning that the level of administrative burden of some of the functions is unnecessarily high. There has also been no uptake in the Trust Framework to date.

19. There is an opportunity to lessen the administrative burden of participating in the Trust Framework, which would likely incentivise and provide certainty to service providers who may be interested in entering the Trust Framework, and support the smooth operation of the Trust Framework.

20. It is assumed that the development of the Trust Framework will be of benefit to New Zealand as it provides a more secure and trusted way for people in New Zealand to verify digital identity and paves the way for further development of a digital identity market. Research suggests that the benefit of a secure digital identity ecosystem is between 0.5-3% of GDP (approximately NZD$1.5-$9 billion), and that the full digitisation of public sector services could bring savings and productivity benefits to the effect of 4-7% of public sector spend.

21. If uptake in the Trust Framework continues to be low, a trusted digital identity ecosystem would be difficult to establish, possibly leading to a loss in confidence in digital identity more generally. This would hinder New Zealand's ability to provide digital solutions for, and increase efficiency in, identity verification.

22. The Department is assuming that lessening the administrative burden of participating in the Trust Framework and providing clarity on how participants will be regulated will encourage digital identity service providers to enter the framework.

We could set specific accreditation renewal requirements under Trust Framework regulations which relieve some of the administrative burden on accredited providers

23. There is an opportunity to relieve the administrative burden of the **accreditation renewal requirements**. Currently, applications to renew accreditation must contain the same amount of information as an original application under section 31(5) of the Act.

24. While the status quo would allow the Trust Framework Authority (the Authority) to have a high level of certainty that accredited providers and services continue to be fit-for-purpose, requiring this amount of information goes against standard regulatory practice, and places an unnecessary level of administrative and financial burden on accredited parties looking to renew their accreditation.

25. These requirements would impact on accredited providers and digital identity service providers who are considering whether they want to participate in the Trust Framework. During targeted consultation, we found that many service providers were concerned that renewal requirements – especially the requirement for continued refreshed independent assessments – could pose too high a barrier for compliance and could disincentivise organisations from entering the Trust Framework.

Defining levels of assurance in regulations could make it clearer how strong identity information is

26. There is an opportunity to define **levels of assurance** in regulations, so that providers of information or verification services have a legislative framework to assert how strong attributes are. There is an additional opportunity to support relying parties and consumers to assess whether an accredited service meets their needs by defining the relative strength of accredited services using more natural language. This will particularly impact groups that are more likely to disproportionally have lower levels of technical expertise or face digital exclusion, such as older people, rural communities, and Māori, by supporting their use of trusted digital identity products and services.

27. Defining the levels of assurance of attributes would also encourage Trust Framework participants to deal with identity information consistently and, when defined in regulations, would also make it easier for other regulatory regimes, such as anti-money laundering or sale and supply of alcohol, to refer to (and align with) the Trust Framework if they wished. It would make it more attractive for participants such as users and relying parties to use Trust Framework products and services.

28. During targeted consultation, we found that there were diverging views on how the levels of assurance should be set. Most submitters agreed that levels of assurance should be set in regulations, with varying views on how the levels should be described.

We have an opportunity to relieve some administrative burden by changing reporting periods

29. There is an opportunity to relieve the administrative burden of **reporting requirements** by amending the reporting periods set out in the first tranche of regulations so that they don't overlap with the year-end and government financial year-end periods. This would mean that accredited providers would not need to provide reporting during resource-intensive periods and reporting can be done during periods where they have more resource.

The proposals will mostly impact providers that are already accredited, although will affect whether providers enter into the digital identity market more generally

30. Two of the proposals – accreditation renewal requirements and the amendment to the reporting requirements – will affect accredited providers and digital identity service providers who are considering whether they want to participate in the Trust Framework.

31. Given that the Trust Framework is a voluntary framework, the impact on service providers is likely to be minor. Digital identity service providers can provide their services regardless of whether they are accredited under the Trust Framework.

32. Levels of assurance will likely impact on how providers set up their processes – and whether they wish to meet certain levels – but will also assist users and relying parties in understanding the strength of information being handled in the Trust Framework.

What objectives are sought in relation to the policy problem?

33. As a voluntary framework, the Trust Framework is most effective if digital identity service providers opt into the Trust Framework. Additionally, as a framework regulating the provision of trusted and secure digital identity services, trust is key to its success.

34. As such, the Department has identified three key objectives, which are to:

    a. **Minimise the barriers to participation** in the Trust Framework, including the administrative burden to participation;

    b. **Maintain the integrity of the Trust Framework**, as well as trust and confidence in its services and products; and

    c. Ensure that the **obligations set out under legislation are clear** to all participants.

35. These objectives support the wider aim of incentivising digital identity service providers to enter the Trust Framework by clarifying the ongoing requirements of participation, as well as lessening the burden for participation as much as is practicable. Without service providers in the framework, there are little-to-no benefits of having a Trust Framework in New Zealand.

36. However, the objectives of minimising barriers to participation and maintaining integrity of the Trust Framework can at times conflict with each other. A careful balance between the two must be maintained.

What consultation has been undertaken?

37. The Department undertook targeted consultation from Monday 11 August 2025 to Monday 1 September 2025, a period of three weeks. The consultation paper was provided to:

    a. the Trust Framework Authority and Trust Framework Board;

    b. Digital Identity Working Group members;

    c. Peak industry bodies, such as Digital Identity New Zealand and Fintech;

    d. Key government agencies;

    e. Māori stakeholders, including iwi, peak bodies, and private businesses, using advice from the Trust Framework Board's Māori Advisory Group; and

    f. Digital identity service providers in the private sector.

38. Targeted consultation was considered appropriate as the proposed regulations focus on administrative requirements solely relevant to service providers already in the Trust Framework.

39. 24 submissions were received. A high-level summary of feedback is below. Feedback relating to specific areas are set out where relevant under **Sections 2A, 2B, and 2C.**

Broad themes from stakeholder feedback

40. Stakeholders generally supported the objectives of minimising the barriers to participation in the Trust Framework, maintaining the integrity of the Trust Framework and confidence in its services and products, and ensuring that any obligations under the Trust Framework are clear to all participants.

41. Where support was not explicitly stated, stakeholders supported amending the regulations, either agreeing with our proposals or recommending alternatives where they disagreed with either option. No submission suggested or recommended that we should retain the status quo.

42. Of note, there was clear concern around the potential for continued requirement for independent evaluations when seeking accreditation renewal and there was support for accreditation renewal requirements to be amended; however, stakeholders did not strongly prefer one option over another. In particular, there was a mild consensus that any renewal regime should have some level of proportionality. The Department has developed a new option as a result of this feedback, which will be discussed further under **Section 2A**.

Section 2A: Assessing options to address the policy problem – Renewal requirements

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

43. Five criteria have been developed to evaluate policy options for renewals against the status quo. A specific accreditation renewal process should: minimise barriers to participation, maintain the integrity of the Trust Framework, and provide clarity to Trust Framework participants.

Effectiveness	Does the option lessen the administrative burden for parties looking to renew their accreditation under the Trust Framework while maintaining the integrity of the Trust Framework?
Proportionality	Are the requirements sized correctly for the variety of organisations that may participate in the Trust Framework?
Certainty	Does the option provide parties with certainty on how they will be regulated?
Transparency	Will participants in the Trust Framework understand why they are being regulated in the way that they are?
Flexibility and durability	Will the regulations enable the regulatory system to evolve in response to new information and changing circumstances?

44. We have weighted all these elements equally, as each of these criteria will support trust and confidence in the accreditation renewal process and maintain the integrity of the Trust Framework.

What scope will options be considered within?

45. These options have been considered within the scope of the regulation-making powers set out under the primary DISTF Act. Non-regulatory options have not been considered as they would not meet the objectives set out above.

What options are being considered?

Option One – Status quo

46. No renewal requirements are set and applications for accreditation renewal would require a full application, as described under **Section 1**.

Shared features across Options Two, Three, and Four

47. Option Two, Three, and Four share similar features. **Under these options**, accredited providers seeking renewal will be assessed against a basic set of criteria looking at provider performance and any changes since the original application or last renewal was made:
    a. any changes to the application details (i.e., key information required in provider accreditation applications as stated in regulation 6 of the Regulations);
    b. any changes to the accredited service that the provider is providing;

c. the Trust Framework provider and service's performance, including against any Digital Identity Services Trust Framework Rules that have been established since the previous application; and
d. any information within the provider's records, including any complaints, investigations, compliance orders, or reporting issues.

Option Two – Standardised approach

48. **Option Two** would establish a standardised accreditation renewal process and include a further requirement in **all** renewal application from all accredited providers for "refreshed independent evaluations of the provider in the areas of security, privacy, and identification management".

Option Three – Risk-based approach

49. **Option Three** would include a further requirement for "any other information that the Authority deems appropriate, including refreshed independent evaluations if requested, based on the provider's risk profile".
50. This requirement would mean renewal requirements will vary according to the risk associated with each provider and service, as determined by the Authority. This will reduce the requirements for providers who have shown high compliance and been assessed as being low-risk. However, this approach is likely to be more resource intensive for the Authority, and will rely on a clear and transparent assessment of risk based on monitoring from the Authority.

Option Four – Hybrid approach – *Preferred option*

51. **Option Four** would include a tiered requirement to the accreditation renewal process on top of the basic criteria. Regulations will set out the following tiers:
    a. **Light renewal requirements** will apply to accredited providers that have not gone through much change and have complied well during accreditation. Light renewals will require reconfirmation of independent security, privacy, and identification management evaluations;
    b. **Moderate renewal requirements** will apply to accredited providers that have gone through some change or have made some breaches during accreditation. These renewals will require refreshed independent security evaluations and reconfirmation of privacy and identification management evaluations;
    c. **Full renewal requirements** will apply to accredited providers that have gone through much change or have made major breaches during accreditation (which have not reached a threshold where their accreditation has been suspended or cancelled). These renewals will require refreshed independent evaluations in the areas of security, privacy, and identification management.
52. The proposed tiered accreditation renewal process makes a distinction between a 'refreshed independent evaluation' which will be similar to the initial independent evaluation undertaken on accreditation, and a 'reconfirmation of independent evaluation' which will only focus on areas of change or previous non-compliance.
53. Certainty around which tier a provider will fall into will be provided by the Trust Framework Authority through guidance, as well as advice as part of the monitoring and reporting process during the accreditation period, and formally advising the provider prior to the renewal process.

Our preferred option was developed to reflect feedback we received during consultation

54. Our preferred option is option four – a hybrid approach. All submissions agreed with the setting of specific renewal requirements under regulations. There was mixed feedback on whether the Department should follow a standardised option or a risk-based option. 6 out of the 12 submissions that gave feedback specifically on the renewal regulations suggested that we consider a hybrid model.

55. Some stakeholders noted that they preferred a risk-based approach to renewals as it would allow the Authority to focus on areas with the most likely areas of weakness and concern. Some stakeholders noted that a standardised approach could disincentivise smaller companies.

56. During targeted consultation, it became clear that we needed to consider a “hybrid” option that had elements of both the Standardised and a Risk-Based approach.

How do the options compare to the status quo? – Renewal approach to accreditation

	Option One – *Status quo*	Option Two – *Standardised approach*	Option Three – *Risk-Based approach*	Option Four – *Hybrid approach*
Effectiveness	0	+ The standardised renewal process slightly relieves the administrative burden on all accredited providers but greatly maintains the integrity of the Trust Framework.	+ A risk-based renewal process would relieve the administrative burden on some accredited providers and would maintain the integrity of the Trust Framework (although to a lesser extent than the standardised approach).	+ A hybrid renewal process relieves the administrative burden on some accredited providers (similar to the risk-based approach) and would maintain the integrity of the Trust Framework (although to a lesser extent than the standardised approach).
Proportionality	0	0 A standardised renewal process has the same level of proportionality as the status quo – all requirements are the same.	+ Providers that show high levels of compliance while accredited will have less strict requirements under a risk-based framework.	+ Providers that have not changed much, or have shown high levels of compliance, would have less strict requirements under a hybrid approach.
Certainty	0	0 A standardised approach provides the same level of certainty as the status quo.	- A risk-based approach makes it less certain for all providers what information they will need to compile ahead of a renewal application. While the status quo is more administratively burdensome, the requirements are certain.	0 The renewal process would be standard across categories rather than a bespoke estimation of risk, providing a similar level of certainty to the status quo.
Transparency	0	0 Setting regulations for the standardised approach will make clear why the Trust Framework Authority needs the information they have asked for.	- Under a risk-based approach, the Trust Framework Authority would make an assessment on the level of risk that a provider poses to the Trust Framework. Providers may not understand why that assessment has been made without a clear declaration and can challenge the determination that is made.	0 Setting regulations for the hybrid approach would make it clear why tiers have been organised in the way that they are, as well as why the Trust Framework Authority needs the information they have asked for.
Flexibility and durability	0	0	+ Provides the Trust Framework Authority with the flexibility to assess the risk that a provider poses to the Trust Framework.	+ Provides the Trust Framework Authority with flexibility to require different information based on the profile of the accredited provider.
Overall assessment	0	+ A standardised approach improves on the status quo without introducing uncertainty into the renewals process.	+ A risk-based approach would improve on the status quo and provides a high level of flexibility for providers. However, it introduces uncertainty into the renewals process.	++ ***Preferred approach*** The hybrid approach improves on the status quo and allows for certainty while ensuring proportionality in the renewal process.

Key: + + much better, + better, 0 about the same, - worse, - - much worse.

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

57. **Option Four** is the Department's preferred option as it most sufficiently meets the assessment criteria and was developed after targeted consultation with key stakeholders. While the status quo and the standardised renewal process under Option Two both also provide certainty for providers on what information they need to prepare when applying for a renewal, it does not allow for proportionality in line with common regulatory practice. Option Four achieves certainty while still providing for a level of proportionality, which was a common theme that emerged during consultation.

58. Option Four also meets the objective of lessening the amount of information that an accredited provider would need to provide when applying for a renewal compared to the status quo. While this is true across all the options, Option Two does not lessen this information greatly (requiring all renewal applications to include independent assurance on the level of risk that providers pose to the Trust Framework).

59. Option Four risks being less effective at maintaining the integrity of the Trust Framework as the independent assurance is less than in Option Two. However, we are confident that grouping providers into appropriate tiers will support the maintenance of security.

60. While Option Three has the advantage of allowing some providers and services to provide less information when applying for renewal, this would not be the case across the board. It also introduces uncertainty for providers and services as to what they may need to provide to meet these renewal requirements. This option also provides the Authority with a high level of discretion on the renewal criteria – which is not as transparent as the status quo and risks subsequent challenge. Option Three is also a less rigorous renewal process than Option Two, as there is no requirement for independent assurance, and would introduce a higher level of risk into the Trust Framework.

Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

61. Yes.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups	None compared to the status quo.	N/A	N/A
Regulators	None compared to the status quo.	N/A	N/A
Others (eg, wider govt, consumers, etc.) *For fiscal costs, both increased costs and loss of revenue could be relevant*	The status quo provides a strict series of requirements that are appropriate to onboard a completely unknown provider. Creating lesser requirements for renewal of a known provider will be less stringent, which could introduce some risk.	Low	Low
Total monetised costs	*None.*	N/A	N/A
Non-monetised costs	*Some security risks could be introduced by creating a new renewal framework.*	*Low*	*Low*
Additional benefits of the preferred option compared to taking no action			
Regulated groups	Lower administrative requirements will mean accredited providers will not need as much resource when renewing their accreditation.	Medium	Medium
Regulators	Lower administrative requirements will require less resource from the Trust Framework Authority.	Low	Medium
Others (e.g., wider govt, consumers, etc.)	None compared to the status quo (renewal will occur regardless).	N/A	N/A
Total monetised benefits	None.	N/A	N/A
Non-monetised benefits	Lower administrative requirements will benefit both regulated groups and the regulator.	*Low*	*Low*

Section 2B: Assessing options to address the policy problem – Levels of assurance

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

62. Four criteria have been developed to evaluate policy options for **levels of assurance** against the status quo. Levels of assurance should: maintain the integrity of the Trust Framework and clearly define the strengths of attributes.

Effectiveness	Do the levels of assurance maintain the integrity of the Trust Framework, and are they feasible?
Certainty	Are Trust Framework participants certain as to how strong Trust Framework attributes are?
Transparency	Will participants in the Trust Framework understand why the levels of assurance have been set in the way that they are?
Flexibility and durability	Will regulations enable the levels of assurance to adapt and evolve in response to new information and changing circumstances?

63. Proportionality has been removed as part of the criteria as the proposals do not set out requirements, simply a standard that different attributes may or may not meet. As such, proportionality is not needed.

64. The rest of the criteria have been weighted the same as each is necessary to ensure that the levels of assurance are defined in a way that supports the security of the Trust Framework, can align with the identification standards, and are well-understood by laypeople.

What scope will options be considered within?

65. These options have been considered within the scope of the regulation-making powers set out under the primary DISTF Act.

66. We have considered a non-regulatory option, which would continue the status quo where identification standards are set out as standards. We have also considered the approach taken in other jurisdictions. While it is not a goal for this tranche of regulations to align with other international frameworks, the levels of assurance have been presented in a way that is similar to how they are presented in Australia and the United Kingdom. This is so that if in future we wanted alignment between those jurisdictions, the naming conventions would not be a barrier. That said, the proposed levels of assurance do not alter or supersede New Zealand's existing identification standards, or how identity products and services will be handled.

What options are being considered?

Option One – Status quo

67. No levels of assurance are set out in regulations, and the differences in strengths of attributes are left to the identification standards, as set out under **Section 1**.

Summary of levels of assurance under Options Two, Three, and Four

68. The Table below summarises the levels of assurance that will be set out under **Options Two, Three, and Four.** The specific definitions of the options will be described in more detail in the sections that follow.

Option 2: Five levels of assurance	**Option 3:** Four levels of assurance	**Option 4:** Four levels of assurance (with method)
Basic	Basic	Basic
Standard	Standard	Standard (Plus if biometric is used)
Standard Plus		
Strong	Strong	Strong (Plus if biometric is used)
Very strong	Very strong	Very strong

Shared features across Options Two, Three, and Four

69. **Option Two, Three, and Four all set** at least four different levels of assurance: *basic*, *standard*, *standard plus*, *strong*, and *very strong*. In all these options, the *basic* and *very strong* levels are identical:

Level of assurance	**Information assurance**	**Binding assurance**	**Example**
Basic	Information is **not verified** against an authoritative source.	**No binding is required**.	Relies on self-asserted identity or a low level of verification. Suitable for services where the consequences of incorrect verification are minimal.
Very strong	Evidence must be either: • the **authoritative source**; or • **continuously synchronised** to an authoritative source so that the evidence and the source are considered equivalent.	Information must be bound in two different ways. **One of these ways must be biometric**, with strict anti-spoofing controls and counter fraud processes.	Reserved for services with the highest risk, requiring even more stringent identity proofing measures beyond strong.

Option Two – Five levels of assurance

70. **Option Two** sets three additional separate levels of assurance: *standard*, *standard plus*, and *strong*, which are derived from criteria under the information assurance and binding assurance aspects of the identification standards. These levels are concerned with:
    a. where information has come from, and
    b. how that information has been bound (i.e., connected) to a person.

Level of assurance	Information assurance	Binding assurance	Example
Standard	Evidence must reference at least a copy of an authoritative source.	Information must be bound to the person using a single method, either through possession of a credential or knowledge factor.	Requires verification information from a known source.
Standard plus	Same as standard – i.e., evidence must reference at least a copy of an authoritative source.	Information **must be bound using biometric methods**.	Requires verification information from a known source, with biometric matching.
Strong	Evidence must reference at least a copy of an authoritative source that has been verified.	Information must be bound in two different ways, **one of which must be biometric.**	Demands more robust verification, including biometric matching against an authoritative source image and verification of authoritative information.

Option Three – Four levels of assurance

71. **Option Three** sets two additional levels of assurance: *standard* and *strong*. Under this option, the *standard* level is equivalent to *standard plus* in **Option Two**.

Level of assurance	Information assurance	Binding assurance	Example
Standard	Evidence must reference at least a copy of an authoritative source.	Information **must be bound using biometric methods**.	Requires verification information from a known source, with biometric matching.
Strong	Evidence must reference at least a copy of an authoritative source that has been verified.	Information must be bound in two different ways**, one of which must be biometric**.	Demands more robust verification, including biometric matching against an authoritative source image and verification of authoritative information.

Option Four – Four levels of assurance (with method) – *Preferred option*

72. **Option Four** sets two additional levels of assurance: *standard* and *strong*. However, unlike **Options Two and Three** the *strong* level no longer requires one of the methods to be biometric.

73. Instead, regulations would also provide for the Trust Framework Authority to add a 'Plus' to the level where a biometric binding method has been used to bind information to a person. The 'Plus' therefore only signals that a biometric method was used to reach that level.

74. As such, under this model, there is the possibility for 'standard' and 'standard plus', as well as 'strong' and 'strong plus'. Basic does not require binding, and very strong will always require biometric binding, so there would be no 'basic plus' or 'very strong plus'.

75. We developed this option in response to a key piece of feedback which pointed out weaknesses in both Options Two and Three, but in a way that maintained the advantages of Option Two, which was preferred by most stakeholders during engagement.

Level of assurance	Information assurance	Binding assurance	Example
Standard	Evidence must reference at least a copy of an authoritative source.	Information must be bound to the person either through possession of a credential, a biometric factor, or knowledge factor.	Requires verification information from a known source.
Strong	Evidence must reference at least a copy of an authoritative source that has been verified.	Information must be bound in two different ways.	Demands more robust verification, requiring multiple methods to connect information to a person.

Stakeholders wanted levels of assurance to be defined in regulations, but the preferred option blends elements of the other two options

76. Most submissions agreed with setting levels of assurance under regulations. During targeted consultation, there was strong support to have the levels of assurance set out under regulations. Out of 20 submissions on the levels of assurance:
    a. 15 stakeholders supported placing levels of assurance in regulations;
    b. 1 stakeholder disagreed with placing levels of assurance in regulations; and
    c. 4 stakeholders gave no feedback either way.

77. Out of the 15 who supported placing levels of assurance in regulations:
    a. 9 stakeholders agreed with the proposed option of five levels of assurance (1 with modifications);
    b. 4 stakeholders agreed with the alternative option of four levels of assurance (1 with modifications); and
    c. 2 stakeholders did not agree with either proposal.

How do the options compare to the status quo? – Levels of assurance

	Option One – *Status quo*	Option Two – *Five levels*	Option Three - *Four levels*	Option Four – *Four levels, with methods*
Effectiveness	0	+ Levels of assurance will provide more information to users and encourage trust.	+ Levels of assurance will provide more information to users and encourage trust.	++ Levels of assurance will provide more information to users and encourage trust. Including an indication where biometrics have been used will likely further this trust.
Certainty	0	++ Levels of assurance will clearly define the strength of attributes, which will provide certainty to users and relying parties.	++ Levels of assurance will clearly define the strength of attributes, which will provide certainty to users and relying parties.	++ Levels of assurance will clearly define the strength of attributes, which will provide certainty to users and relying parties.
Transparency	0	+ Levels of assurance will define the strengths of attributes based on where the information has come from and how that information has been connected to someone else.	+ Levels of assurance will define the strengths of attributes based on where the information has come from and how that information has been connected to someone else.	++ Levels of assurance will define the strengths of attributes based on where the information has come from and how that information has been connected to someone else. There will also be clear information how information has been bound.
Flexibility and durability	0	- Setting levels of assurance in regulations will be less flexible than relying on standards and guidance.	- Setting levels of assurance in regulations will be less flexible than relying on standards and guidance.	- Setting levels of assurance in regulations will be less flexible than relying on standards and guidance.
Overall assessment	0	+ This option will improve upon the status quo by providing certainty and encouraging trust.	+ This option will improve upon the status quo by providing certainty and encouraging trust.	++ ***Preferred option*** This option will more greatly improve upon the status quo by providing certainty and encouraging trust and will be more transparent than the other options.

Key: + + much better, + better, 0 about the same, - worse, - - much worse.

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

78. While the options are reasonably similar and all vastly improve upon the status quo, **Option Four** is our preferred approach. This is because **Option Four** will provide greater transparency on how the information has been bound to the owner of the information which is a key aspect of determining how 'trustworthy' an attribute is. However, it is worth noting that we have included an additional level, standard plus, which requires information to be bound through biometrics. This allows the assurance framework to take advantage of the security and assurances that biometric methods provide to boost what would otherwise be standard assurance. The additional standard plus level will likely better align with the Australian Identity Proofing standards.

79. While **Option Three** would increase the level of confidence in binding and likely create a more secure standard for digital identity assurance throughout the Trust Framework, we do not recommend this approach. This is because if biometric methods cannot be met for any reason, the best assurance a service can provide is basic, which could result in a higher proportion of services being provided at a lower level of security than in **Option Two**. The single standard level in this option further would likely not align as well with the Australian Identity Proofing standards as the standard and standard plus levels in **Option Two** but would likely still be interoperable with those standards.

Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

80. Yes.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups	None compared to the status quo – no additional requirements are being made on providers, who should already be asserting levels of assurance under the identification standards.	N/A	N/A
Regulators	None compared to the status quo. The levels of assurance are managed by the Department's Digital Policy team and Trust Framework group. There is no cost to the Trust Framework Authority.	N/A	N/A
Others (e.g., wider govt, consumers, etc.) *For fiscal costs, both increased costs and loss of revenue could be relevant*	None compared to the status quo – the Department already delivers the identification standards. This codifies those standards within regulations. There may be some confusion if the definitions begin to drift away from each other as a result of reviews, either of the identification standards or of regulations.	Low	Low
Total monetised costs	*None.*	*N/A*	*N/A*
Non-monetised costs	*Some confusion could be created through misalignment of standards and regulations.*	*Low*	*Low*
Additional benefits of the preferred option compared to taking no action			
Regulated groups	Accredited providers will have certainty as to how	Medium	Low

	they can achieve the level of assurance they wish to provide.		
Regulators	None	N/A	N/A
Others (e.g., wider govt, consumers, etc.)	Users and relying parties will be able to understand the strength of attributes under the Trust Framework. Additionally, strengths will be treated consistently across Trust Framework providers.	High	Medium
Others (e.g., wider govt, consumers, etc.)	Government will be able to refer to the strengths as they are set out under regulations, rather than as standards that do not have legal standing.	Medium	Medium-high
Total monetised benefits	*None*	*N/A*	*N/A*
Non-monetised benefits	*The levels of assurance are more widely understood and can be referred to in other pieces of legislation which may want to align with the Trust Framework (such as where legislation governs age or identity verification processes).*	*Medium*	*Medium*

81. Setting levels of assurance in regulations will benefit providers and support growth of the digital identity system. It will not impose any additional costs.

Section 2C: Assessing options to address the policy problem – Reporting requirements

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

82. We have used the same five criteria to compare the options as the criteria for assessing the renewals options.

Effectiveness (60%)	Does the option achieve the objectives and outcomes?
Proportionality (10%)	Are the requirements sized correctly for the variety of organisations that may participate in the Trust Framework?
Certainty (10%)	Will regulated parties understand what their obligations are?
Transparency (10%)	Will participants in the Trust Framework understand why they are being regulated in the way that they are?
Flexibility and durability (10%)	Will the regulations enable the Trust Framework to adapt and evolve in response to new information and changing circumstances?

83. We have heavily weighted effectiveness as the key criteria in this tranche of regulations as we are not changing the requirements; only the periods that those requirements need to be met. That said, the other criteria remain important in case there are inadvertent outcomes from making such a change.

What scope will options be considered within?

84. Options have been considered within the existing reporting requirements – we are not seeking to amending what needs to be reported on, simply when reports need to be provided to the Trust Framework Authority.

What options are being considered?

Option One – Status quo

85. No amendment is made to the reporting periods, as set out in **Section 1**.

Option Two – Amended reporting periods

86. **Option Two** would amend the reporting periods that are currently in regulations from 1 January and 1 July to 1 March and 1 September.

Option One – Status quo	Option Two – Amended periods
In this regulation – **6-month period** means a period of 6 months beginning on 1 January or 1 July	In this regulation – **6-month period** means a period of 6 months beginning on *1 March* and *1 September*
In this regulation – **12-month period** means a period of 12 months beginning on 1 January	In this regulation – **12-month period** means a period of 12 months beginning on *1 March*

How do the options compare to the status quo? – Reporting periods

	Option One – *Status quo*	Option Two – *Amended periods*
Effectiveness	0	+ Amending the reporting periods would lessen the administrative burden on providers. It removes the overlap between periods to report on Trust Framework 12-month and 6-month reporting with resource-intensive times of year.
Proportionality	0	0
Certainty	0	0
Transparency	0	0
Flexibility and durability	0	0
Overall assessment	0	+ ***Preferred option*** Option Two lessens the administrative burden that would be present under the status quo by shifting it away from a resource-intensive period.

Key: + + much better, + better, 0 about the same, - worse, - - much worse.

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

87. Option 2, the preferred option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits. It means that accredited providers face lesser administrative burden than the status quo.
88. This is a minimal change that is easily done alongside a suite of other regulations relating to the Act.

Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

89. Yes.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups	None	N/A	N/A
Regulators	None	N/A	N/A
Others (e.g., wider govt, consumers, etc.) *For fiscal costs, both increased costs and loss of revenue could be relevant*	None	N/A	N/A
Total monetised costs	*None*	*N/A*	*N/A*
Non-monetised costs	*None*	*N/A*	*N/A*
Additional benefits of the preferred option compared to taking no action			
Regulated groups	New reporting periods fall at less resource-intensive times.	Low	Medium
Regulators	None	N/A	N/A
Others (e.g., wider govt, consumers, etc.)	None	N/A	N/A
Total monetised benefits	*None*	*N/A*	*N/A*
Non-monetised benefits	*Lesser administrative burden.*	*Low*	*Medium*

90. This is a relatively straight-forward change that will benefit regulated groups by reducing administrative burdens without imposing any further costs.

Section 3: Delivering an option

How will the proposal be implemented?

Roles and responsibilities

91. The Trust Framework Board (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.

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

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

94. If regulations are made by Order in Council, the Authority will notify existing and potential providers and provide guidance on how the regulatory regime will operate. Consultation on the proposed regulations did not surface any significant implementation risks. There will be further opportunity to identify implementation risks by consulting on draft regulations.

How will the proposal be monitored, evaluated, and reviewed?

95. The TF Board has oversight of the monitoring, evaluation and review of the regulations, as well as monitoring the effectiveness of the Trust Framework. Given that we are not expecting any providers to seek renewal until (at the very earliest) mid-to-late 2027, we would not set a review and evaluation of that process until after a first round of renewals has been completed. Reporting requirements are also not likely to be relevant until (at earliest) mid-2026 and also requires participation before a review can occur. The TF Board will work closely with the Authority to get an understanding of provider experiences through the renewal and reporting processes and can make recommendations under section 45 of the Act where necessary to minimise undue delay on when regulations should be updated.

96. In terms of levels of assurance, the TF Board could review these regulations annually during their regular meetings and make a recommendation to update those regulations where the TF Board considers that changes to regulations should be made, so that the levels of assurance remain aligned with the identification standards and will maintain the integrity of the Trust Framework.

97. 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 and the processes the underpin the Trust Framework.