Regulatory Impact Statement: Additional policy decisions for the Digital Identity Services Trust Framework Bill

Coversheet

Purpose	
Decision Sought:	Analysis produced to inform final Cabinet decisions on additional policy matters for the Digital Identity Services Trust Framework Bill
Advising Agencies:	Department of Internal Affairs
Proposing Ministers:	Minister for the Digital Economy and Communications
Date:	11 August 2021

Problem Definition

Digital identity services enable individuals and organisations (users) to prove who they are online by verifying their information and allowing them to securely share information with third parties. Currently, these services are not properly regulated. Cabinet has agreed to establish a Trust Framework to accredit trusted digital identity services that meet rules for security, privacy, identification management, information and data management, and information sharing. The Trust Framework will enable the provision of safe and secure digital identity services so people can more efficiently access services digitally and have more control over their information.

This analysis focusses on the two in principle Cabinet decisions made in February:

- providing the ability to issue variable pecuniary penalties (via a Rulings panel) to digital identity service providers to enforce non-compliant conduct; and
- establishing a framework outlining when digital identity service providers should or shouldn't be held liable for harm caused by reliance on their services.

Pecuniary penalties

For the Trust Framework to effectively enable trust in digital identity services (and to realise the benefits they offer), accredited digital identity services must comply with the rules. This RIS considers whether the use of pecuniary penalties (to be issued by a rulings panel) can support compliance within the Trust Framework and disincentivise serious rule breaches that may cause harm.

Liability framework

Currently, there is a lack of clarity as to when and how liability for loss would apply in civil claims to actors operating or using digital identity services. It is therefore unclear whether liability would properly be applied to those whose actions are responsible for harm and when accredited digital identity service providers would be protected from liability for harm resulting from reliance on their services. This RIS analyses options to provide clarity for digital identity service providers potentially liable for damages.

Executive Summary

Digital identity services are emerging technology services allowing people to verify and share their information. Currently, there is no regulation outlining how these services operate, resulting in a lack of trust in these services. Trusted digital identity services can improve access to services, by easily proving eligibility and identity information, and are therefore a critical enabler of participation in the digital economy through use of digital services. Trusted information sharing is a foundation for the economy and is increasingly recognised as a global issue.

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

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

Several jurisdictions (including the United Kingdom and Australia) are establishing trust frameworks to support the provision of trusted digital identity services, but all are in the early stages. In July 2020, Cabinet agreed to establish a trust framework for digital identity services to ensure minimum standards are consistently applied across the digital identity system [CAB-20-MIN-0324 refers].

The Digital Identity Services Trust Framework (Trust Framework) is a policy and regulatory framework that sets and applies standards for the provision of secure and trusted digital identity services. Under the Trust Framework, digital identity service providers that meet rules, including service requirements for security, privacy, identification management, information and data management, and information sharing, can have their services accredited and become accredited digital identity service providers (under the Trust Framework, both providers and services may be accredited by an Accreditation Authority – to be established).

In broad terms, the proposed intervention will bring consistency, trust, structure and efficiency to the digital identity system. This will produce a wide range of benefits for people, businesses and organisations, government and wider society. Key benefits include minimising identity theft, improving information sharing efficiency and user-control, reducing unnecessary sharing of information, and improving access to services.

In February 2021, Cabinet agreed to detailed policy for the Bill, including establishing the Trust Framework as an opt-in regime, forming the governance and accreditation bodies within the public service, and providing enforcement mechanisms to ensure compliance with the rules.

Cabinet also agreed in principle to provide that pecuniary penalties may be issued for non-compliance with the Trust Framework's rules, and to establish the circumstances where accredited digital identity service providers would be liable for civil harms (a liability framework) to ensure accredited digital identity service providers are not vulnerable to indeterminate liability.

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

As part of the Cabinet paper seeking approval to introduce the draft Bill, substantive policy decisions are required on the inclusion of pecuniary penalties and the establishment of a liability framework. Neither of these decisions affect the ability to enforce other legislation, or offences under this Bill.

Pecuniary penalties

Pecuniary penalties are civil penalties (non-criminal monetary penalties usually imposed by a court in civil proceedings). If provided for in legislation, the Accreditation Authority could refer a rule breach to a rulings panel (to be established to act in place of a court for the purposes of issuing pecuniary penalties – similar to the Gas Act 1992 and Electricity Industry Act 2010) who would determine whether to impose pecuniary penalties and at what rate.

This RIS assesses whether pecuniary penalties would be a desirable enforcement mechanism (in addition to other enforcement mechanisms previously agreed by Cabinet) to enforce compliance with the Trust Framework rules. The Cabinet agreed enforcement mechanisms have not been reconsidered and were analysed in the February 2021 RIS.

Option 1 – that the power to issue pecuniary penalties is not included in legislation (preferred option);

Option 2 – that the Accreditation Authority may issue pecuniary penalties (via a rulings panel) to accredited digital identity service providers for non-compliance with the rules.

Pecuniary penalties would provide an additional (although minimal) financial mechanism to enforce non-compliance with the rules. However, they would be onerous and costly to administer, are not supported by stakeholders and could deter participation in a voluntary regime where the same penalties do not apply to those choosing not to opt-in. For these reasons, Option 1 – not including pecuniary penalties – is preferred.

Liability

Digital identity service providers may be subject to civil proceedings where reliance on their services leads to (realised) losses on behalf of a user or relying party (the user or relying party would typically initiate proceedings if they were subject to loss). Accredited digital identity service providers therefore have an interest in understanding when they could be held liable for harm resulting from use of the identity information they share when complying with the rules. This RIS considers the circumstances where accredited digital identity service providers should (or shouldn't) be liable for harm resulting from use of their services. Options to extend liability protections to non-accredited parties (e.g. non-accredited digital identity service providers or relying parties) were not considered as they are not subject to this regulatory framework.

Option 1 – no liability protections (status quo);

Option 2 – immunity from civil liability for accredited service providers strictly complying with the rules;

Option 3 – immunity from civil liability for accredited service providers acting in good faith.

Immunity from civil liability was identified by stakeholders expecting to participate in the digital identity system (as either service providers or relying parties) as a strong incentive to become accredited to the Trust Framework as it provides assurance against risks that do not exist in the unregulated market (the status quo). A wide range of stakeholders emphasised that 'good actors' should not be liable for damages when they were following the rules or acting in good faith. It is considered that immunity from any potential liability would be a strong incentive for accredited digital identity service providers to comply with the rules or act in good faith.

While accredited service providers should comply with the rules (and can be punished for not doing so), stakeholders noted that in some cases, despite their good intentions, they may fail to comply with the rules, leading to harm. Option 3 (extending immunity from civil liability for accredited service providers acting in good faith and in the absence of gross negligence) is preferred as it provides assurance for accredited service providers and promotes participation while maintaining accountability for 'bad actors'. It is considered that a rigorous accreditation process that ensures that participants have the capability and knowledge to comply with the rules will effectively protect users and relying parties under this option.

Limitations or Constraints on Analysis

Decisions already made in previous Cabinet papers, and analysed in the Regulatory Impact Statements from June 2020 and February 2021 have been taken as given and have not been reconsidered.

This analysis is limited to specific decisions on the use of pecuniary penalties and the establishment of a liability framework. These in-principle decisions were made by Cabinet subject to the development of the Trust Framework's rules and assessment of the potential risks. However, the Bill has a category three legislative priority and the rules will not be developed prior to introducing the Bill. This has limited analysis of pecuniary penalties to whether they are appropriate in an opt-in accreditation scheme without knowing what conduct they could be applied to.

As the digital identity service sector is not yet mature, the Trust Framework is not yet operational and its rules have not been publicly consulted on, there is minimal evidence to inform the effect of including pecuniary penalties, and the types of civil liability cases that will emerge. This has constrained the use of evidence in the analysis. Where possible, stakeholders from the digital identity sector have provided insights into how the digital identity service market operates (or could operate under the Trust Framework).

Targeted consultation has been undertaken with representatives from multiple sectors (a representative list is provided on page 11), including those who are expected to be users, relying parties and digital identity service providers within the future digital identity system. Consultation has focussed on a range of detailed policy proposals, including proposals on liability and pecuniary penalties. Given time constraints and the broad

range of policy issues consulted on, discussion on the issues in this analysis has been limited to broad views. These broad views are reflected in the analysis. Further opportunity for feedback on these proposals will be sought at Select Committee.

Public consultation, representing the user perspective, has not been undertaken due to time constraints and the technical nature of the Bill. Therefore, evidence of the user perspective of these issues is limited to that sought during targeted consultation. Targeted consultation included engagement with representatives of user groups, including Consumer NZ. We also received significant feedback from stakeholders highlighting the user-perspective and the implications of policy decisions for users. Users will have an opportunity to provide feedback on the Bill (and the proposals in this analysis) at Select Committee.

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

Quality Assurance (completed by QA panel)	
Reviewing Agency/Agencies:	Department of Internal Affairs Quality Assurance Panel
Panel Assessment & Comment:	The panel considers that the information and analysis summarised in the RIA partially meets the quality assurance criteria. The impact assessment provides good background information and helpfully explains the broader digital identity system and its complexities. In addition, the impact assessment is clear and upfront in setting out the constraints on analysis from previous Cabinet decisions on the Digital Identity Services Trust Framework. While the impact assessment did evidence the consultation that occurred, drawing out a wider range of perspectives during consultation, particularly the user perspective, would have assisted.

Section 1: Outlining the problem

Context/Background Information

What are digital identity services?

Digital identity services enable users to prove who they are online by checking and sharing personal or organisation information in digital form in a transaction with a third party (a relying party). The user-authorised sharing of information through digital identity services allows people to assert their personal attributes, such as their income, qualifications, date of birth, or iwi affiliation to access services and entitlements, or to complete transactions. Digital identity services rely on relationships between individuals and service providers, as part of a 'digital identity system' that includes:

- **users** who are subject to and initiate their own transactions within the ecosystem;
- **digital identity service providers** who enable users to share personal or organisational information in transactions with third parties (relying parties). Examples of digital identity services include services that:
    - check the accuracy of information;
    - check the information's connection to the authorising user; or
    - facilitate secure sharing of information between users and relying parties**;**
- **relying parties** who use the trusted personal and organisational information supplied by digital identity service providers to provide services to users (e.g. banks, government, telecommunications companies, health providers, and providers of age restricted services such as liquor stores).

Currently, one of the main ways people can assert their core identity information online is through the government provided RealMe service. RealMe is a centralised model of digital identity in which credentials are stored and controlled by a central authority. Since RealMe was introduced, the digital identity environment (and associated technology) has changed significantly, with the emergence of decentralised digital identity services through which users collect verified information about themselves from other sources to store and control themselves (e.g. in a digital wallet).

Cabinet has decided to establish a Digital Identity Trust Framework

In July 2020 Cabinet agreed to support the provision of safe, secure and trusted digital identity services as part of New Zealand's digital infrastructure via the implementation of a regulatory framework to ensure digital identity service providers consistently apply standards across the digital identity system [CAB-20-MIN-0324 refers]. Cabinet agreed to the establishment of:

- a statutory trust framework enabling government to set rules (standards) for New Zealand's digital identity system;
- a representative governance board appointed by a Minister (the Board); and
- a department-based team to undertake accreditation of digital identity service providers (the Accreditation Authority).

Several jurisdictions (including the United Kingdom and Australia) are establishing trust frameworks to support the provision of trusted digital identity services, but all are in the early stages. A trust framework is a policy and regulatory framework that sets and applies rules for security, privacy, identification and information management, and information sharing; and enforces the rules through accreditation of digital identity service providers.

A private sector response to support the provision of trusted digital identity services in a comprehensive fashion was considered unlikely to emerge (and an international approach is not considered enforceable). Therefore, a government-led response was preferred, and was also supported by the private sector. For further details on the decision to establish a Trust Framework, please see the RIS released alongside the July 2020 Cabinet paper (*Progressing Digital Identity: Establishing a Trust Framework*).

The development of the Trust Framework has linkages with several other ongoing government work programmes. These include:

- the Government Chief Digital Officer's digital inclusion workstream, which is promoting equitable opportunities to participate in society using digital technologies;
- Te Ara Manaaki programme, which is transforming government systems for effective service delivery with a focus on identity and life events; and
- the establishment of a consumer data right (CDR) through legislation (agreed by Cabinet in June 2021). The CDR will require businesses that hold data to share prescribed data that they hold about consumers with trusted third parties, on the authorisation of the consumer.

The Digital Identity Services Trust Framework is integral to the future state of New Zealand's digital economy. Trusted digital identity services will be pivotal cogs in supporting trust in digital technologies; facilitating better information sharing and verification; and enabling the CDR's functionality through the provision of means for information verification and sharing.

For people, the Trust Framework - as a framework based on user-authorisation and secure information sharing to access services - will support consumer confidence and trust within an increasingly digital economy (in combination with the related workstreams listed above).

Cabinet has agreed detailed policy decisions for the Trust Framework Bill

Following the decision to establish a statutory Trust Framework for the digital identity system, Cabinet agreed to detailed policy decisions for the Trust Framework in February 2021. These detailed policy decisions included:

- That the purpose of the Trust Framework Bill is to promote the provision of secure and trusted digital identity services that meet essential minimum requirements for security, privacy, identification and information management, and interoperability; and to support community resilience and realise the wider benefits of digital identity.
- That the governance and accreditation functions be guided by seven principles; to be people centred, inclusive, secure, privacy-enabling, enabling of te ao Māori approaches to identity, sustainable, interoperable, and open and transparent.
- To establish a the Board in a public service department with the role of monitoring and supporting the performance of the Trust Framework and updating its rules.

- To establish the Accreditation Authority within a public service department with full responsibility for the accreditation regime (including compliance), and that it may certify third-party assessors as part of the accreditation process.
- That the Accreditation Authority have the power to enforce the Trust Framework rules through issuing warnings, requiring additional record-keeping, suspending or revoking accreditation, or making a compliance order.
- To establish a disputes resolution process for users, relying parties and digital identity service providers.
- To authorise the Accreditation Authority to issue infringement notices for certain offences.
- That offences in the Bill would include:
    - knowingly and representing oneself as being an accredited digital identity service provider when they are not; and
    - knowingly or recklessly supplying false or misleading information to the Authority or obstructing the authority.

Detailed regulatory impact analysis of Cabinet's decisions in February 2021 can be found in the RIS proactively released alongside the Cabinet paper (*Detailed policy for a Digital Identity Trust Framework*).

In February 2021, Cabinet also agreed in principle:

- that the Authority have the power to issue pecuniary penalties for non-compliance with the Trust Framework's rules, subject the development of the rules and the identification of conduct that will be subject to a penalty; and
- to the establishment of a liability framework, subject to the development of the rules and an assessment of the potential risks to users, ruling parties and accredited digital identity service providers, as well as the impact on participation.

Following these Cabinet decisions, the Digital Identity Services Trust Framework Bill has been drafted with the Parliamentary Counsel Office. The draft Bill is to be considered by Cabinet alongside the policy decisions analysed in this RIS.

Given the significance of any proposal to provide immunity from liability or to establish pecuniary penalties, Treasury's Regulatory Quality Team advised that a new RIS on these significant issues would be required to support the detailed policy paper. Treasury also advised that this RIS would not need to include minor policy decisions made through the drafting process. Minor policy decisions not included in this regulatory impact analysis (and exempted by Treasury) are:

- the decision not to explicitly outline the principles in the Bill (substantive provisions in the Bill incorporate the principles, which were also used to evaluate policy options);
- the removal of infringement offences for breaches of the Act (this conduct is covered by criminal offences);
- the establishment of a permanent Māori advisory group to advise the Governance Board on Māori interests and knowledge (this group does not have substantive decision-making powers); and

- the ability of the responsible Minister for the Trust Framework to establish its rules either through statutory rules or as regulations.

Simultaneously, the Department is undertaking work (as agreed by Cabinet in June 2021) to assess options for government investment in digital identity infrastructure to enable government agencies to issue trusted credentials for users in the digital identity system. This will enable users to share a range of government-held attributes within the digital identity system.

What is the policy problem or opportunity?

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

New Zealand lacks consistently applied standards and processes for sharing, storing and using information in a digital environment. Legislation and standards exist but they are found in a variety of places, and while some of these requirements are legally binding, some are non-binding guidance or best practice. Consequently, organisations vary in how they manage information, creating inefficiencies and undermining trust and confidence in the digital identity system for individuals, the private sector and government agencies.

Without trust in services enabling secure information sharing and assertion, people lack the ability to efficiently prove who they are online and easily access services. Ultimately, this undermines people's expectations regarding privacy and security, stifles innovation in service provision, and hinders the realisation of the significant social and economic benefits digital identity services offer.

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

Focus group research shows Māori have lower levels of trust than other groups over government holding and sharing information about them. Participants in the focus groups attributed this distrust to the misuse and abuse of Māori data, creating biased assumptions about Māori and a narrative not informed by Māori.

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

Research with sector stakeholders also tells us that trust depends on the perceived motivations of the organisation they're dealing with, and the context. Context factors for building trust include the type of organisation that is requesting the information, what information is requested and the brand reputation for that company. Commercial enterprises were also seen to focus on their own interests and more likely to contravene rules if not

enforced. Therefore, people would be reluctant to see them have access to personal information held by government without appropriate reassurances and controls in place.

While RealMe seeks to address some of these issues by providing an all-of-government digital identity service that provides a high degree of trust and security, the regulatory requirements of the Electronic Identity Verification Act 2012 (including that all participating entities be approved by Cabinet) have stymied uptake. Additionally, RealMe focusses only on core identity attributes (name, sex, date of birth and place of birth) which do not enable access to a wide-range of services. RealMe is also a centralised model for digital identity and is government-owned and operated, meaning some groups are excluded due to a lack of trust in government and users do not have control of their information.

Digital identity has the potential to deliver significant benefits to a wide variety of stakeholders

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

- people - for example, improved access to online services; improved customer experience; greater confidence that personal and organisational information is secure and private; reduced risk and reduced identification fraud;
- businesses and organisations - for example, improved service delivery potentially resulting in an expanding customer base; greater efficiencies (e.g. less duplication and process streamlining); reduced fraud resulting from improved risk assessment;
- government – for example, improved service delivery; greater efficiencies (e.g. less duplication); improved record keeping; increased opportunities to break down information silos between business units and government agencies; improved ability to detect and deter security or privacy breaches of personal and organisational information; improved digital inclusion by promoting trust in digital services; greater trans-Tasman alignment; and
- society – for example, greater interoperability between digital identity service providers; clear and consistent rules for accredited digital identity services, resulting in greater confidence in digital identity services; increased effectiveness in countering certain crimes; and greater economic opportunities.

By establishing legally enforceable rules for accredited parties, the Trust Framework will bring coherence to the digital identity system and consistency in the standards followed by digital identity services. This approach has been supported by the digital identity sector throughout our engagement since 2018 as a way to enable multiple parties to participate in a safe and trusted way.

For example, in the future someone that wants to apply to study could digitally access their identity information and other information about themselves they need to provide, such as their record of learning and residency status. They could then use an accredited digital identity service to store this information on their phone or a web-based sharing tool and share it with the agencies or organisations that need this information, such as tertiary providers and StudyLink, making it easier to apply for study.

Digital identity can also support digital trade and other cross-border transactions. The development of the digital identity ecosystem will enable New Zealand to advance

discussions on digital identity in other jurisdictions. One example is the New Zealand and Australian Prime Ministers' commitment to mutual recognition of identity services. There is also potential for ongoing alignment with Canada and the United Kingdom with each of these countries developing their own trust frameworks.

Officials have worked with sector stakeholders and research bodies to gather a robust body of evidence to inform, develop and test proposals. This includes regular engagement with over 100 organisations (including public agencies, Crown agents and entities, private digital service providers, financial institutions, non-government organisations such as Internet NZ and Consumer NZ, and academic institutions such as the University of Auckland and the University of Otago). Stakeholders have expressed widespread support for the development of a government-led Trust Framework to support the provision of trusted and secure digital identity services.

Stakeholders are generally supportive of the detailed policy proposals for the Trust Framework, as agreed by Cabinet

To achieve the benefits of enabling trusted digital identity services, key policy decisions have been made by Cabinet for the establishment of the Trust Framework. These detailed policy decisions were tested with targeted stakeholders between May and July 2021. Stakeholders consulted on the Bill's detailed policy proposals (including the options in this analysis on liability and pecuniary penalties) included:

- Representatives from the digital identity sector, including Digital Identity NZ members, MATTR, and independent consultants;
- Other organisations with an interest in the Trust Framework, including banks, Consumer NZ, Internet NZ and Payments NZ;
- Public service agencies and the Office of the Privacy Commissioner; and
- A Māori technical working group with subject matter expertise, including leaders from Māori digital identity initiatives and public service members with relevant Māori expertise.

Generally, these stakeholders were supportive of the Bill's intent and the policy proposals agreed by Cabinet. They emphasised the need for flexibility in the Bill, the importance of providing incentives to participate, and the difficulty in creating an enforcement regime within an opt-in Trust Framework where those who don't participate would not be subject to enforcement mechanisms. Māori subject matter experts also noted the importance of honouring te tiriti o Waitangi, supporting Māori participation, recognising collective identity, and acknowledging iwi as trusted sources of identity information.

Stakeholders also emphasised the importance of maintaining trust in the Trust Framework if it is to be successful. Particularly, the digital identity sector noted that accredited providers must be held to account to ensure they comply with the rules, and those who fail to comply should be stripped of their accreditation. Other stakeholders supported this view as a way to ensure users could be sure that accredited digital identity service providers were trustworthy.

All stakeholders agreed that the success of the Trust Framework would rely on digital identity services becoming accredited, and that this would only happen if the benefits outweighed the costs. A key potential benefit for digital identity service providers included the assurance that compliance with the rules would protect them from punishment. Other stakeholders agreed

that to protect ‘good actors’ who comply with the rules ‘bad actors’ should not be in the scheme.

Enforcing compliance in the Trust Framework

Pecuniary penalties are non-criminal monetary penalties typically imposed by the courts in civil proceedings. If included, pecuniary penalties would form a part of the enforcement regime administered by the Accreditation Authority to enforce compliance. The enforcement mechanisms agreed by Cabinet did not include the ability to issue financial penalties of any sort. Enforcement mechanisms already agreed by Cabinet include:

- issuing a private warning or reprimand to an accredited digital identity service provider;
- making an order that a public warning or reprimand be issued to an accredited digital identity service provider;
- imposing additional or more stringent record-keeping or reporting requirements in connection with Trust Framework standards and rules;
- suspension or revocation of accreditation; and
- making a compliance order requiring any action that is necessary to restore it to a position of compliance with the rules of the Trust Framework (with the threat of suspension or revocation of their accreditation if not met).

Stakeholders have emphasised the need for enforcement within the Trust Framework to discourage and remediate non-compliant behaviour that affects the trusted nature of accredited services (and of the Trust Framework). While this is an opt-in regime, enforcement remains a necessary tool to ensure users and relying parties can identify trusted digital identity services. Without such mechanisms, it is possible that accredited parties would not feel obliged to comply with regulations and standards, leading to a situation where the public’s trust and confidence in their products, systems and services would be undermined.

Further policy decisions are required on establishing powers to issue pecuniary penalties and creating a framework for liability

In February 2021, Cabinet also agreed in principle:

- that the Authority have the power to issue pecuniary penalties (through a rulings panel) for noncompliance with the Trust Framework’s rules, subject to the development of the rules and the identification of conduct that will be subject to a penalty; and
- to the establishment of a liability framework, subject to the development of the rules and an assessment of the potential risks to users, relying parties and digital identity service providers, as well as the impact on participation.

Should pecuniary penalties be included?

Currently, the digital identity service market is largely unregulated, so there are no enforcement mechanisms available to ensure compliance with best practice standards. Cabinet has agreed to establishing a range of enforcement mechanisms as part of the Trust

Framework – including an in-principle decision to include pecuniary penalties as an enforcement mechanism. The use of enforcement mechanisms is considered pivotal to establishing trust in the Trust Framework by ensuring accredited service providers comply with the rules once accredited. This analysis considers pecuniary penalties as an additional enforcement mechanism, on top of those already agreed. Pecuniary penalties were agreed to in principle by Cabinet with an expectation that the rules would be developed prior to introducing legislation.

As an opt-in regime, those who are not accredited will not be required to comply with the rules and therefore will not be subject to enforcement mechanisms for rule breaches. Digital identity service providers therefore emphasised the need to develop a range of enforcement mechanisms that enable enforcement without disincentivising participation in the Trust Framework and placing undue risks on those who choose to become accredited.

While non-accredited digital identity service providers (and other entities) will not be required to comply with the rules, the Bill does set out offences (agreed by Cabinet), some of which they may be penalised for. Offences outlined in the Bill include:

- knowingly or recklessly representing a provider or service as accredited through the Trust Framework when it is not;
- misusing the trust mark;
- knowingly or recklessly giving false information to the authority in an application for accreditation;
- failing to give key or specified information in an application for accreditation;
- failing to tell the authority of a change to key information or specified information (accredited digital identity service providers or applicants only); or
- obstructing the authority.

A person or organisation may also be subject to enforcement action for wrongdoing under other legislation. For example: if an accredited provider provides a paid issuance credential service to consumers, and the services supplied are not fit for purpose or are not carried out with reasonable care and skill, there might be a cause for action under the Consumer Guarantee Act 1993. Additionally, using, collecting, or sharing a user's information without legal cause to do so (e.g. through the user's authorisation) could be cause for action under the Privacy Act 2020.

What should a liability framework cover?

When enabling the sharing of information, digital identity services can be subject to civil proceedings, where their services (usually as part of a chain of services, including an information provider, sharing or information checking services and relying parties) could produce unreliable identity credentials. In these cases, harm may be caused to a user (e.g. when use of that credential does not allow them to access a service they are eligible for) or a relying party (e.g. when it offers a service to a customer based on a false identity credential). If harm results from reliance on a digital identity service (directly or indirectly), a civil case may be brought against the digital identity service provider to recover damages. Given the complexity of the digital identity sector, the new and evolving nature of the technology, and the variables in the supply chain to creating an identity credential, a digital identity service provider may be subject to uncertainty regarding when it may be found liable for damages.

Currently, it is unclear how digital identity service providers may be held liable for harms resulting from reliance on their services, and the provision of digital identity services carries a potentially significant liability risk as issuing an incorrect identity credential can result in real losses for a user or relying parties. For example, where the information is not properly bound[1] or verified to a person it may be used by a fraudster to access services (e.g. withdrawing a bank loan) from a relying party that they are not entitled to. The average cost of identity fraud is currently estimated at $13,627 per event with each victim having to spend on average 12 hours responding to their incident.

Without clarity as to when a digital identity service provider should be held liable (or when it should be protected), it faces uncertain risks, and users and relying parties will be unclear when they can claim damages against accredited digital identity service providers. Stakeholders from the digital identity sector expressed concern that they may be unduly held liable for losses or harm caused by use of their services despite following best practice rules and standards. Exposure to this risk potentially creates a disincentive to provide digital identity services and it is not clear under existing standards where liability for loss within the digital identity system would lie. Providing assurance to digital identity service providers is viewed as a key incentive for becoming accredited and to following the rules as compliance (or good faith actions) would provide protection from civil liability.

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

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

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

[1] Binding refers to the process of establishing that information relates to the person or organisation claiming it.

Section 2: Option identification and impact analysis

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

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

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

Trust: This option will instil trust in digital identity services and the Trust Framework. In the event an incident undermines trust in the Trust Framework there should be (statutory and non-statutory) processes in place to remediate and restore that trust.

Participation: This option promotes up-take of the Trust Framework, thereby increasing the number of digital identity services following good practice standards and giving consumers more options.

Feasibility: The estimated costs (set-up, ongoing) for government and the wider system are reasonable and practical.

Flexibility: This option is responsive to changes, can reflect the needs of the digital identity service market, and is scalable.

When considering which options to support, more weight is assigned to options that effectively ensure participation in the Trust Framework and can be feasibly implemented. Participation is considered a key driver for the success of the Trust Framework, establishing trust in digital identity services and achieving the objectives outlined above. Additionally, any proposal must be cost-effective and feasible to implement.

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

What scope are you considering options within?

Previous Cabinet decisions on establishing a Trust Framework in legislation (in July 2020 and February 2021) have placed limits on the scope of the decisions being considered. Particularly, this analysis focussed on Cabinet's in-principle decisions:

- that the Authority have the power to issue pecuniary penalties (through a rulings panel) for noncompliance with the Trust Framework's rules, subject to the development of the rules and the identification of conduct that will be subject to a penalty; and
- to establish a liability framework, subject to the development of the rules and an assessment of the potential risks to users, relying parties and digital identity service providers, as well as the impact on participation.

Pecuniary Penalties

The options for pecuniary penalties are whether they should be included in legislation as an enforcement tool, in addition to the enforcement mechanisms already agreed to by Cabinet, or not to include them.

This analysis does not reconsider the decision to include other enforcement mechanisms. In this analysis, pecuniary penalties would be issued by a rulings panel who determine that an accredited digital identity service provider has breached the Trust Framework rules. The provider could be fined up to $10,000 if the rulings panel deems it has broken the rules (this does not have to be determined beyond reasonable doubt). Options to impose pecuniary penalties through a court process have not been analysed in this RIS as it would create prolonged and costly processes, while realising the same outcomes as pecuniary penalties through a rulings panel.

The exclusion of pecuniary penalties in legislation does not restrict the ability of courts to issue pecuniary penalties, for other legislation to be enforced, or for people to seek recourse for civil harm.

Liability

Cabinet has not made any decisions as to the nature of the liability framework. However, the options considered in this analysis are limited to civil liability matters where harm is caused due to reliance on an accredited digital identity service (or outputs from an accredited digital identity service). Options considered in this analysis do not affect users' ability to seek redress for damages, but does provide a framework for when an accredited digital identity service provider can be held liable.

The Department previously considered the option to establish a statutory tort with a form of legal defence so that an accredited service provider would only be liable for losses arising from a failure to comply with the rules when this action was the cause of harm. This option was deemed inappropriate and was not fully analysed following feedback from stakeholders. Stakeholders, including government agencies with valuable information sources, advised that this option would deter them from participating as it would interfere with their ability to mitigate risks contractually (it is common for organisations to manage risk by putting conditions in contracts that put a limit on liability e.g. by capping the amount payable in damages on a breach or restricting the types of loss that are recoverable).

The Department also received legal advice that this approach would impose more stringent liability obligations on digital identity service providers than exist under common law. Principles of negligence require a complainant to establish that a duty of care exists between them and the party that caused harm. It is not currently clear that this would be the case for digital identity service providers. These increased obligations could dissuade organisations from participating in the Trust Framework.

Additionally, it is conceivable that an accredited provider might be responsible for incorrect verification of a user's identity or other attributes arising from conduct that does not amount to a breach of the rules. The Trust Framework rules are not intended to provide an absolute guarantee of privacy and security, and limiting the ability of other service providers, relying

parties and individuals to recover damages in these circumstances might undermine public confidence in the Trust Framework.

Immunity from liability for relying parties was considered but has not been analysed as a formal option in this RIS as relying parties are not being regulated under the Digital Identity Services Trust Framework.

Banks and financial institutions were particularly interested in ensuring that reliance on information from accredited digital identity services would meet their anti-money laundering obligations. However, this is out of scope of this Bill and the civil liability framework considered in this RIS.

Additionally, when discussing the user experience in civil proceedings, it was clear that users would often be unable to decipher who was responsible for issuing an incorrect credential given the complex nature of digital identity supply chains and the potentially limited view of users. This issue has not been addressed in this analysis but demonstrates the potential for confusion in the application of liability within the digital identity sector.

Describe and analyse the options

The purpose of the Bill is to address the challenges with the status quo by introducing a set of rules for providers to be accredited in the digital identity system. Accreditation is optional for digital identity service providers who may become accredited to demonstrate compliance. However, their compliance should be monitorable and enforceable to maintain trust in the system. As an opt-in regime, the benefits of, and incentives to join should be weighed against the costs. Without the appropriate incentives, the benefits may not be realised due to lack of participation.

To promote a trusted digital identity system, we are seeking Cabinet agreement for detailed policy proposals on whether to include powers to issue pecuniary penalties for non-compliance and the establishment of a liability framework for accredited digital identity service providers.

Pecuniary Penalties

In this instance, pecuniary penalties are considered as an enforcement option to be imposed by a rulings panel (to be established). If included, they could be issued to accredited digital identity service providers who fail to comply with the Trust Framework's rules (the standards they sign up to and prove they can comply with to become accredited). Enforcing compliance with the Trust Framework will be essential to ensuring the digital identity system remains functional, trustworthy and sustainable, and that its rules and standards are consistently applied.

Cabinet has already agreed that the Accreditation Authority may enforce compliance through issuing private or public warnings/reprimand, imposing additional record-keeping or reporting requirements, making compliance orders, or suspending or revoking accreditation. These enforcement mechanisms are taken as given but the in-principle decision to include pecuniary penalties has not been included in the status quo. These compliance mechanisms do not apply to digital identity service providers who are not accredited under the Trust Framework.

Option 1 – that the power to issue pecuniary penalties is not included in legislation (status quo);

Option 2 – that the Accreditation Authority's rulings panel may issue pecuniary penalties to accredited digital identity service providers for non-compliance with the rules.

Option 1 – no power to issue pecuniary penalties exists (status quo)

Under this option, other enforcement mechanisms would remain, so compliance could still be enforced. However, there would be no power to issue financial penalties for a breach of the rules. Currently, in the unregulated market, these powers do not exist and would not exist for digital identity service providers who are not accredited as they are not required to comply with the rules.

Stakeholders across sectors (representing digital identity service providers, relying parties and users) were supportive of the proposed enforcement mechanisms agreed by Cabinet and mostly felt that applying non-criminal financial penalties within an opt-in regime would be inappropriate. Most stakeholders noted that public warnings, suspension or revoking accreditation would be much more effective tools to ensure compliance as they came with significant reputational costs. Digital identity service providers were particularly supportive of an enforcement regime that enables the Accreditation Authority to work with service providers so they understand how to comply with the rules and are supported to do so, rather than punished for minor or one-off breaches.

As the trust mark is a symbol of compliance with the rules, suspension and cancellation (which would be permanently visible on the public register of accredited service providers) was viewed by sector stakeholders, relying parties and user-representatives as the most useful tool to ensure integrity in the Trust Framework, and to support users to identify trustworthy service providers. It was noted that pecuniary penalties would not have a reputational effect and therefore may not be a preferred approach to maintaining compliance.

Accredited digital identity service providers' actions may lead to harm. This is more likely when they breach the rules. In these circumstances, a user may seek to recover their realised losses through civil proceedings (provided the accredited party did not act in good faith – see below). The use of pecuniary penalties would not provide this compensation for users as penalties would be paid to the Crown.

Option 2 – pecuniary penalties may be issued to accredited digital identity service providers for non-compliance with the Trust Framework rules

If provided for in the Bill, a rulings panel (to be established) would be able to issue pecuniary penalties to accredited digital identity service providers who breach the rules. Penalties could be issued up to the value of $10,000, as determined by the rulings panel. When considering whether to issue a penalty, factors that would need to be considered would include:

- the severity of the breach;
- the impact on others;
- the extent to which the breach was intentional or otherwise;
- past behaviour;
- whether the matter was disclosed to the Authority;

- the amount of time before the breach was resolved; and
- whether the offender benefitted from the breach.

Pecuniary penalties, if included, would provide an additional financial mechanism for the Accreditation Authority to enforce compliance with the rules – improving flexibility in the Accreditation Authority's enforcement decisions. However, it is unclear when the use of pecuniary penalties would be preferred in place of using other enforcement mechanisms, and what conduct they would apply to. This is particularly difficult to identify given that the rules are still in development and have not been publicly consulted on. Additionally, user representatives noted that non-criminal penalties (such as pecuniary penalties) will not deter large actors (such as multi-national corporations).

Some stakeholders indicated that pecuniary penalties (applied variably up to the value of $10,000) would not create a significant reputational (or legal) risk and any large players may not be deterred from non-compliance. However, establishing a higher upper-limit for pecuniary penalties was considered inappropriate as it could disincentivise smaller players in the market from becoming accredited. It has been deemed desirable to encourage both small and big players to become accredited to offer users with a wider range of trusted service options, including NZ owned and operated businesses.

The process for issuing pecuniary penalties would be issued through a rulings panel. While this approach would support more timely decisions than the courts process, it would still involve additional administrative costs. In other compliance-based schemes, pecuniary penalties are rarely used and legal processes can take a year, creating significant costs and pressures on the regulating body. The cost of an equivalent rulings panel for the Electricity Authority is approximately $300,000 per annum. In a small accreditation scheme, this makes the inclusion of pecuniary penalties largely infeasible.

Without creating a strong disincentive to non-compliance, the inclusion of pecuniary penalties creates minimal benefit and the use of other enforcement mechanisms is preferred. It is thought that the threat of accreditation suspension or cancellation is a bigger disincentive to breaching the rules (as identified by consulted digital identity service providers) as the costs to becoming accredited (provisionally estimated to be in the vicinity of $10,000 to $250,000 depending on the complexity of the application) would represent a significant business expense.

To compensate for the lack of financial penalties in this scheme, there will likely be a relatively high barrier to entry with requirements and rules that will ensure those who become accredited do comply with the rules, act in good faith, and support the integrity of the Trust Framework. Additionally, offences under this legislation, or other legislation, would apply to more significant breaches. For example, the misuse and unreasonable sharing of personal information with a third party would be a breach of the Privacy Act 2020.

Multi-Criteria Analysis

	Option 1 – No pecuniary penalties (status quo)	Option 2 – Can issue pecuniary penalties for non-compliance
Principles	**0** This option promotes accreditation and does not impose penalties. Other enforcement mechanisms are considered more people-centred and less punitive.	**-** A punitive approach to non-compliance was considered to be undesirable by stakeholders as it is not people-centred (it is punitive rather than restorative).
Trust	**0** Does not provide additional financial penalties within an opt-in regime. However, existing enforcement mechanisms (e.g. compliance orders, suspension or cancellation of accreditation) should enable compliance.	**0** Promotes compliance due to risk of financial penalties, and gives users confidence that service providers will be punished if they don't comply. However, pecuniary penalties will not deter big players from breaching rules and could deter smaller providers from applying for accreditation thereby reducing the overall trustworthiness of the digital identity sector.
Participation	**0** Does not provide a disincentive from becoming accredited and participating in the Trust Framework.	**-** Financial penalties that apply only to those who choose to become accredited were identified as a significant deterrent for service providers considering becoming accredited.
Feasibility	**0** Will not require any cost to administer (rulings panel will not be established).	**-** Will be costly and onerous to administer - the cost of an equivalent rulings panel is approximately $300,000 per annum. It was also considered impractical to establish penalties for rules that have not yet been set.
Flexibility	**0** The Accreditation Authority maintains a range of enforcement mechanisms.	**+** Pecuniary penalties would add an extra option for the Accreditation Authority to enforce compliance with the rules, improving the flexibility of the enforcement scheme.
Overall assessment	**0** This option is preferred as it is cheaper, retains a good range of compliance tools and does not disincentivise participation.	**--** This option is not preferred as it is too costly and provides limited benefit to the Trust Framework (including users). While it would provide an additional enforcement mechanism to promote compliance, the other enforcement mechanisms are considered sufficient.

Conclusions

Option one (not including pecuniary penalties) is preferred as the current enforcement mechanisms provide sufficient compliance assurance. Pecuniary penalties would not fill a gap in the enforcement regime and therefore the marginal benefits of including them are outweighed by the costs of their administration. Pecuniary penalties applied in an opt-in regime are considered to be a potentially significant disincentive for digital identity service providers becoming accredited.

Summarise the costs and benefits of your preferred option

Affected groups	Comment	Impact
Additional costs of the preferred option		
Regulated groups	Not subject to pecuniary penalties. Their risk of financial penalty is therefore unchanged from the status quo.	None
Regulators	Not responsible for administering pecuniary penalties and therefore do not have to establish a rulings panel to review pecuniary penalty decisions.	None
Other groups (e.g. wider government, users etc.)	Users and relying parties are not (and would not have been) subject to pecuniary penalties. They may still seek civil redress for harm if caused by a providers actions.	None
Total monetised costs	N/A	None
Non-monetised costs	N/A	None
Additional benefits of the preferred option		
Regulated groups	Accredited digital identity service providers face reduced risk of being financially penalised and are assured that the enforcement regime will not be punitive but focusses on promoting compliance. This should incentivise accreditation and compliance.	Low
Regulators	Reduced costs of administering the enforcement regime as a rulings panel is no longer needed. This also improves the efficiency of the enforcement decision-making process.	Low
Other groups (e.g. wider government, users etc.)	By incentivising uptake, users and relying parties should have more accredited digital identity services to choose from. However, this group is not directly affected.	None/Low

Total monetised benefits	Reduced costs by not requiring a rulings panel and reducing the risk of financial penalties for accredited parties.	Low
Non-monetised benefits	Improved uptake due to lower risks to becoming accredited.	Low

Liability

Digital identity service providers have an interest in clearly understanding the risk of legal liability that flows from their participation in the Trust Framework, and how they may mitigate this risk. This RIS considers the circumstances where accredited digital identity service providers should (or shouldn't) be liable for harm resulting from the use of their services.

Options for the liability framework considered in this analysis include:

- **Option 1** – no liability protections (status quo);
- **Option 2** – immunity from liability for accredited service providers strictly complying with the rules;
- **Option 3** – immunity from liability for accredited service providers acting in good faith.

Option 1 – No immunity from liability (status quo)

Without liability protections, in cases where civil proceedings are brought against an accredited service provider, they may be held liable for damages that were not caused by their actions, and instead were the result of other actors in a supply chain over which it had no control. For example, a digital identity service provider may issue an incorrect credential by sharing information which had been verified or bound by another digital identity service provider who failed to comply with the rules.

Without protections, the compliant digital identity service provider may end up sharing civil liability for harm that was not caused by its actions. Furthermore, liability will be determined by the courts or through a dispute resolution process, so even if an accredited participant is able to establish it is not liable, this will still often involve a lengthy, expensive and uncertain legal process. While this provides users with the normal legal path to compensation for damages, it can mean that these damages are partially paid by a provider who is not at fault or who has complied with best practice standards (the Trust Framework rules).

Stakeholders from the digital identity sector expressed concern that without certainty regarding liability, accreditation would not provide them with assurance against risks and so the potential costs of accreditation may be perceived to outweigh the benefits. Failure to promote accreditation is considered detrimental to the Trust Framework's sustainability, leading to unrealised benefits for users and relying parties.

Option 2 – immunity for accredited digital identity service providers complying with the rules

Under option 2, accredited digital identity services complying with the rules would not be held liable for damage caused by the use of their services when they comply with the rules. To be

eligible for immunity from civil liability, the accredited service provider must be strictly complying with the Trust Framework rules for the transaction in question.

Stakeholders from the digital identity sector (and other sectors) supported immunity provisions for compliance with the rules but noted that there may be circumstances where their non-compliance with the rules may expose them to liability even if it did not contribute to any harms caused by the use of their services (for example, not following procedural requirements such as having processes to identify and deal with security incidents). Under this option, 'good faith actors' would be open to potentially significant liability risks when operating within the Trust Framework. Digital identity service providers indicated that they would therefore be disincentivised from becoming accredited.

Any option to limit immunity has the potential to limit opportunities for users and relying parties to recoup losses. In cases where a digital identity service provider has complied with the rules, it has been deemed unlikely that it will be the cause of harm and that actions by another party in the supply chain or reckless or careless behaviour on the part of the user (e.g. sharing their username and password with another person) is likely the cause of harm. In these cases, other responsible parties in the supply chain may be found liable for the harm caused to users or relying parties.

The exclusion of liability is tied only to compliance with the rules, suggesting that non-compliance with the rules will leave accredited service providers open to liability in cases against them for civil harm. This incentivises accredited service providers to comply. Non-compliance is also punishable through the Accreditation Authority's enforcement mechanisms.

Option 3 – immunity for accredited digital identity service providers acting in good faith where their behaviour does not amount to gross negligence

Under option 3, accredited digital identity service providers would not be liable for damages caused as a result of the use of their services when they are acting in good faith to follow the rules, and where their actions do not amount to gross negligence. This provision would not require strict compliance with all rules when carrying out the transaction in question. However, it would demand that the accredited service provider was trying to do so in good faith.

Within the digital identity system, it is possible that a service provider may be unable to strictly comply with the Trust Framework rules for a specific transaction, despite their good intentions and their proven ability to do so. In this case, while the accredited service provider in question would not be liable for harm caused, their failure to comply with the rules would still be enforceable through the enforcement mechanisms available to the Accreditation Authority.

Stakeholders from the digital identity sector were supportive of this option as a means to protect accredited digital identity service providers who act in good faith. They emphasised that this would be a key incentive to becoming accredited and for accredited providers to comply with the rules (or to pursue compliance in good faith).

Public sector agencies that hold valuable personal information (such as driver licences, passports, income information, educational qualifications etc.) noted that they would only seek accreditation if they could be sure that their good faith actions would not leave them vulnerable to civil liability proceedings. This was of particular concern for agencies who collect self-asserted information, as they cannot always be certain of its accuracy. Agencies may not therefore choose to become accredited and their information sources would not be recognised as trusted within the digital identity system. This would significantly diminish value in the system and leave significant benefits unrealised.

While this option establishes a limit on users' ability to recover damages from 'good faith actors', it does not restrict their ability to recover damages from those acting in bad faith or who have been grossly negligent.[2] The exclusion of liability in this option is tied to good faith intentions, suggesting that accredited service providers will be open to liability in cases against them for civil harm where they have not acted in good faith. It also incentivises accredited service providers to make a good faith effort to comply with the rules, and to undertake due diligence.

There is a risk that limiting liability to cases of demonstrable bad faith or gross negligence could affect trust in the Trust Framework if a circumstance arises where users or relying parties end up suffering harm due to a provider error and cannot seek recompense for it in civil court. However, this risk is mitigated by two factors.

Firstly, the complaints process will allow users and participants to make complaints to the Accreditation Authority. Non-compliance is still punishable through the Accreditation Authority's enforcement mechanisms, meaning that while strict non-compliance may not lead to civil liability, it may be enforced through other mechanisms. Parties that repeatedly show an inability to comply with the rules would likely be suspended or even have their accreditation cancelled. Furthermore, serious non-compliance with the rules may amount to a criminal offence under other legislation (such as the Privacy Act 2020) and accredited providers would therefore be criminally liable.

Secondly, the accreditation process will be designed to ensure that accredited service providers have the knowledge and capability necessary to ensure compliance with the rules. In this way, the accreditation process will ensure that the risk of 'good faith' actors violating the rules in a way that creates risks for users and relying parties is minimised.

[2] The High Court held that gross negligence "is a degree of negligence where whatever duty of care may be involved has not been met by a significant margin."

Multi-Criteria Analysis

	Option 1 – No immunity (status quo)	Option 2 – Immunity for accredited providers complying with rules	Option 3 – Immunity for accredited providers acting in good faith
Principles	**0** Has a people-centred approach as pathways to recoup damages are left open.	**0** This may limit users' ability to recoup damages. However, it does ensure accredited providers are not held unduly liable for damages, making it sustainable.	**-** This option is not as people-centred as the others as it may limit users' ability to recoup losses.
Trust	**0** Promotes users' ability to recover losses.	**0** Promotes compliance with the rules but users may not be able to recoup damages in all cases.	**0** Promotes good faith actions but users may not be able to recoup damages in all cases.
Participation	**0** Digital identity service providers indicated that they would be hesitant to join without knowing the liability implications. Public sector agencies would be unlikely to participate, diminishing value in the system.	**+** Digital identity service providers supported protection from liability when following the rules but noted that non-compliance may not always be their fault.	**++** Digital identity service providers (including public sector agencies) supported this option as it reflected a protection for 'good actors' and encouraged them to join while still promoting compliance and good faith actions.
Feasibility	**0** Without liability protections for accredited service providers, they will face uncertainty and may be subject to undue risk.	**0** Accredited digital identity service providers must strictly comply with the rules or face potential liability for consequential damages.	**0** Provides more flexible protection for accredited providers acting in good faith.
Flexibility	**0** The status quo provides uncertainty for digital identity service providers but does not tie liability to strict compliance with the rules.	0 Demands strict compliance with the rules, even if the provider is unaware of the rule breach (or unable to control it).	**+** Provides flexibility for accredited service providers acting in good faith who may be unaware (or may not have control of) potential rule breaches.
Overall assessment	**0** This option is not preferred as it does not promote participation, and it creates the potential for undue risk and uncertainty for accredited digital identity service providers.	**+** This option is not preferred as its lack of flexibility does not properly incentivise participation, therefore diminishing value in the system.	**++** This option is preferred as it is more flexible than option 2 and promotes participation. However, it does not empower users to recover potential losses in civil court.

Conclusions

Option 3 (extending immunity from liability for accredited service providers acting in good faith) is preferred as it provides the most assurance for accredited service providers acting in good faith and promotes accreditation within the digital identity system. This approach maintains accountability for 'bad actors' and sets an expectation that providers not complying with the rules and acting with gross negligence will be liable for the harm they cause.

Summarise the costs and benefits of your preferred option

Affected groups	**Comment**:	**Impact**
Additional costs of the preferred option compared to taking no action		
Regulated groups	Protects accredited digital identity service providers acting in good faith. However, it does indicate that those not acting in good faith will be held liable for actions that lead to harm.	None
Regulators	This option provides some clarity for court proceedings and disputes processes. However, it is not a complete liability framework outlining how liability would be applied in all instances.	Low
Other groups (e.g. wider government, users etc.)	Relying parties or users are less likely to pass on the costs of damages to accredited digital identity service providers. This could create risks for them, but this will be determined by the courts (or disputes processes).	Low
Total monetised costs	Potential that users and relying parties will not be able to recoup consequential damages from good faith actors. However, they should be able to recoup these damages from responsible parties (e.g. non-accredited digital identity service providers or accredited digital identity service providers not acting in good faith).	Low
Non-monetised costs	None.	None
Additional benefits of the preferred option compared to taking no action		
Regulated groups	Increased assurance that they will not face undue risk when acting in good faith. This will reduce risks/costs for good actors and incentivise accreditation and compliance.	Low
Regulators	Will benefit from more clarity in the application of liability, reducing civil cases against accredited digital identity service providers and supporting demand for accreditation services, and thus an effective Trust Framework.	Low
Other groups (e.g. wider government, users etc.)	Potentially more accredited digital identity services to choose from as more become accredited.	Low
Total monetised benefits	Reduced legal costs and financial risk for accredited digital identity service providers.	Low
Non-monetised benefits	Improved certainty and better uptake, improving the effectiveness of the Trust Framework.	Low

Section 3: Implementing the preferred option

How will it be implemented?

The Accreditation Authority will be responsible for administering and enforcing the Trust Framework, and will therefore administer the enforcement mechanisms included in the Bill (which will not include pecuniary penalties). Cabinet agreed in July 2020 that the Accreditation Authority will sit within a public service department (to be determined by the Prime Minister).

The Rules Development Programme – set up within the Department of Internal Affairs – is currently designing the 'rules' for the Trust Framework. These rules are being developed alongside stakeholders and Māori, including the Data Iwi Leaders Group, relevant functional leads within government, digital identity service providers, banks and financial institutions, and other subject matter experts. The rules will determine the requirements for becoming accredited and will therefore determine what the Accreditation Authority is enforcing. The rules will at least cover privacy, security, identification management, information and data management, and sharing and facilitation requirements.

When the rules development programme has finished developing the rules, the Board will take responsibility for governance of the rules and the Trust Framework. The Board – which will be hosted by a public service department and appointed by the host Chief Executive – will be responsible for:

- recommending changes to the Trust Framework's rules and regulations to the Minister (in consultation with Māori, the Office of the Privacy Commissioner, accredited digital identity service providers, and other stakeholders);
- undertaking education and publishing guidance for potential users, relying parties, and digital identity service providers;
- monitoring the effectiveness of the Trust Framework (including the enforcement regime and liability framework).

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

The liability framework does not include any specific implementation requirements as it will be realised through civil court proceedings.

Monitoring, Evaluation, and Review

Once established, the Trust Framework will be monitored by the Board to ensure it is functional and effective. This will be a core function of the Board who is also responsible for recommending changes to the Trust Framework. In monitoring the performance of the Trust Framework, the Board will consider the effectiveness of the enforcement regime and liability framework. The Board will also work with accredited providers to better understand how the regime is affecting trust in the digital identity system.

While the Board will hold an oversight and advisory function for the Trust Framework, the Minister for the Digital Economy and Communications will hold responsibility for the Trust Framework and this legislation.

The Bill also provides a statutory requirement for the Board's host department to review of the Board's operations two years after commencement of the Act. The review will include an assessment of the effectiveness of the Board in carrying out its functions and will consider the viability of other governance arrangements. The department will also review the complaints and disputes processes two years after enactment, and will review these processes at five yearly intervals.

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