Submission by

AI Forum
New Zealand
Te Kāhui Atamai Iahiko o Aotearoa

to the

Department of Internal Affairs

on the

Digital Identity Services Trust Framework Phase Two Regulations

1 September 2025

Background

The AI Forum of New Zealand is a not-for-profit organisation that brings together industry, academia, and government to advance the responsible and inclusive adoption of artificial intelligence (AI) across Aotearoa. We welcome the opportunity to provide feedback on the Digital Identity Services Trust Framework Phase Two Regulations developed by the Department of Internal Affairs.

Summary of Recommendations

The AI Forum supports the Department's preferred options across all three areas. We recommend adopting a standardised accreditation renewal pathway as the baseline, complemented by proportionate oversight and continuous monitoring; implementing a five-level assurance model with explicit fairness, inclusivity, and interoperability values; and shifting reporting dates while piloting structured, machine-readable submissions. These changes align with ISO/IEC 42001:2023 principles and comparable international frameworks (Australia, UK, EU), reduce unnecessary burden on low-risk and SME providers, and enhance trust and accountability through targeted transparency.

Detailed Feedback

1. Accreditation Renewal

Questions - Standardised approach

1.1. Have you identified any risks with this standardised option? If so, what are your concerns?

We acknowledge the benefits of a standardised renewal pathway, particularly in offering certainty to providers. The primary risk we observe, however, is that repeating comprehensive evaluations every three years may create compliance for compliance's sake, rather than yielding fresh assurance about a provider's trustworthiness. Independent audits in security, privacy, and identity management are resource-intensive. For larger organisations this is manageable, but for SMEs, which the Government is seeking to encourage into the digital economy, these obligations may present a material barrier to entry or continuation in the Framework.

A further concern is that a fixed three-year cycle may not reflect material changes in risk that arise between renewals. Internationally, regulators are increasingly supplementing periodic reviews with continuous monitoring tools. For example, the UK Financial Conduct Authority uses RegTech systems to detect emerging risks between formal audits. If New Zealand adopts a purely standardised three-year model, there is a risk that the Trust Framework Authority is left blind to significant developments occurring in the interim.

In short, while we support the certainty of the standardised approach, it should be complemented by proportionality measures for smaller providers and by mechanisms for interim oversight between renewal periods.

International standards are increasingly moving away from static review cycles. For example, ISO/IEC 42001:2023 – the world's first AI management systems standard – is built on principles of continuous monitoring, corrective action, and risk-based governance. Embedding such principles into accreditation renewal would help ensure the Trust Framework does not become a compliance exercise but remains a living system that reflects providers' ongoing governance maturity.

It is also worth noting that repeating comprehensive evaluations is burdensome even for large organisations, when considered alongside their wider compliance activities. The cumulative effect of multiple regulatory obligations can become significant.

1.2. Do you think that this option would provide an appropriate level of rigour in the accreditation renewal process? If not, what do you think we have missed?

Yes, the standardised option provides a consistent baseline of rigour. It ensures all providers are assessed against the same criteria and helps to maintain confidence in the Framework. However, we caution that rigour should not be measured purely by the weight of documentation.

What matters is whether the process generates reliable, timely and actionable insight. For example, requiring providers to submit structured, machine-readable compliance data would enable the Trust Framework Authority to detect issues more rapidly and make oversight less reliant on retrospective reviews. This is increasingly the norm in international practice. Australia's *Digital ID Act 2024* tailors accreditation obligations to provider scale and service type, balancing assurance with proportionality. A similar approach in New Zealand would allow the system to remain rigorous without discouraging smaller, innovative entrants.

Questions - Risk-based approach

1.3. Have you identified any risks with this risk-based option? If so, what are your concerns?

A purely risk-based model carries a number of risks. The most significant is inconsistency: different providers may face different requirements, which could create perceptions of unequal treatment and lead to challenge. Without a robust and transparent methodology for risk assessment, trust in the Authority's decisions may be undermined.

Another risk is the resourcing impact on the regulator. Developing bespoke assessments for every renewal application would require specialist expertise and greater administrative capacity. This may reduce the Authority's ability to focus resources on the highest-risk areas.

While oversight mechanisms are outlined, the regulations provide limited detail on enforcement actions for non-compliance or how accountability will be maintained consistently across providers. Clarity on enforcement is important to sustain trust.

1.4. Do you think that this option would be simple to comply with? If not, what do you think we have missed?

We do not believe that a purely risk-based model would be simpler to comply with. For some providers, particularly those assessed as low-risk, the burden may reduce. However, the unpredictability of the process introduces uncertainty, making it difficult for providers to plan. This uncertainty may deter investment or discourage new entrants from seeking accreditation.

Simplicity is best achieved by combining a standardised baseline with proportionate additional requirements where a provider's risk profile justifies it. This "hybrid" model provides clarity to providers while allowing the Authority flexibility where required.

Questions on this section

1.5. Do you agree with our preferred option?

Yes. We agree that a standardised approach is the most appropriate foundation. It ensures consistency across providers, gives the sector clarity on expectations, and maintains fairness in application.

1.6. Should the Department consider an alternative option to those proposed?

Yes. We recommend a hybrid option that combines a standardised baseline with targeted risk-based oversight. This would enable the Authority to focus more intensive scrutiny on higher-risk providers while maintaining certainty for all. Such approaches are common in other regulated sectors, including financial services, and provide a balanced way of managing risk.

1.7. Do you have any additional comments to provide on this part of the document?

We encourage the Department to explore the use of automation and RegTech to support accreditation renewal. Continuous compliance monitoring, structured data reporting, and AI-assisted audit trails would allow oversight to scale efficiently while reducing the administrative burden on providers. This would align New Zealand with emerging international practice and future-proof the Framework.

- Encourage the Authority to focus resources on high-risk providers, reducing unnecessary burden on those assessed as low-risk.
- Consider commissioning a cost–benefit analysis comparing the standardised, hybrid, and risk-based models. Such analysis could quantify the economic impact on SMEs and strengthen the case for proportionality.
- Explore financial support mechanisms or grants to help SMEs meet compliance requirements.
- Investigate "sandbox" environments to allow start-ups to test compliance affordably before full accreditation.
- Advocate for transparency mechanisms, such as publishing audit summaries or trust scores, to enhance accountability and public confidence.

2. Levels of Assurance

Questions

2.1. What are your views on defining levels of assurance in regulations? Are there any risks to doing this?

We strongly support the inclusion of levels of assurance in regulation. This will provide clarity for providers and users, and enable relying parties to make better-informed decisions. It will also align the Trust Framework more closely with international regimes, supporting interoperability.

The principal risk is that levels become overly rigid or outdated. The regulatory framework must be able to adapt as technology develops, particularly in areas such as biometrics and decentralised identity. Another risk is that heavy reliance on biometric binding could have unintended exclusionary effects. International studies have demonstrated that biometric systems may perform unevenly across demographic groups, particularly for Māori, Pacific peoples, older adults, and those with disabilities. This could undermine public trust.

2.2. Are there other assurance values that should be added to regulations?

Yes. In addition to information and binding assurance, we recommend that fairness, inclusivity and interoperability are explicitly recognised as assurance values. This would require providers to test for bias in biometric systems, demonstrate accessibility of services, and design with international standards in mind. The UK Digital Identity & Attributes Trust Framework has incorporated inclusion monitoring, while the OECD AI Principles emphasise fairness and human rights. Embedding such values into regulation would strengthen trust and align New Zealand with leading practice.

The relevance of international standards is clear here. ISO/IEC 42001:2023 requires organisations to actively identify and mitigate risks such as bias, fairness, and accessibility in the design and operation of AI systems. Aligning the Framework's assurance values with these obligations would future-proof New Zealand's system and strengthen its interoperability with other jurisdictions.

2.3. Do you agree with our preferred option?

Yes. We agree with the Department's preference for five levels of assurance. This provides greater granularity, especially by distinguishing between "standard" and "standard plus". The additional category allows biometrics to be recognised without forcing all providers to adopt them.

2.4. What are your views on these approaches?

We consider the five-level model more flexible and internationally aligned. The four-level model increases the baseline by making biometric binding mandatory at "standard", but risks excluding providers unable to meet biometric requirements. This could lead to more services being classified as "basic", which may reduce confidence in the Framework overall.

2.5. Is it useful for standard and standard plus to be separated?

Yes. Separating "standard" and "standard plus" is useful. It provides a clearer pathway for providers wishing to incorporate biometrics, while maintaining an alternative for those who cannot. It also aligns more closely with Australia's Identity Proofing standards, enhancing the potential for interoperability.

2.6. Do you have any additional comments to provide on this part of the document?

We recommend that the levels of assurance are reviewed periodically, for example every three years, to ensure they remain aligned with technological developments and international frameworks such as the EU's eIDAS 2.0. This will ensure that New Zealand's framework remains relevant and globally interoperable.

3. Amending Reporting Dates

Questions

3.1. Do you agree with our approach?

Yes. We agree that moving reporting dates to March and September will reduce administrative burden on providers, as it avoids the peak periods of the calendar year and government financial year-end. This is a pragmatic adjustment that supports compliance.

3.2. Do you have any concerns with changing the reporting dates?

We have no concerns with the proposed changes. However, the opportunity could be taken to modernise reporting beyond simple date adjustments. Internationally, regulators are beginning to require machine-readable compliance reports, which enable more efficient analysis and reduce duplication. Singapore and Canada have both moved towards structured reporting formats to support digital governance.

We therefore recommend that the Department pilot structured compliance submissions (for example in XML or JSON) alongside the new reporting dates. This would reduce administrative costs in the long term and help the Trust Framework Authority manage oversight more effectively.

Reporting obligations should not be tied only to static deadlines. ISO/IEC 42001:2023 highlights the value of continuous documentation and monitoring of governance controls. Moving towards structured, machine-readable reporting would align with this international direction, supporting both efficiency and transparency.

Conclusion

As the AI Forum is engaged in international standards development, including through representation on ISO/IEC JTC 1/SC 42 and the development of ISO/IEC 42001:2023, we see clear opportunities for New Zealand to align the Trust Framework with global practice. This will ensure the Framework remains relevant, resilient, and interoperable with partner economies, while also reinforcing New Zealand's leadership in responsible AI and digital identity governance.

Thank you for the opportunity to provide feedback on the consultation document. We are happy to engage further to discuss our submission and provide any further assistance.

If you have any further queries, please do not hesitate to contact us.

Yours sincerely,

Madeline Newman
Executive Director
AI Forum New Zealand
E| madeline.newman@aiforum.org.nz **P|** +64 21 274 9778

Craig Pattison

Craig Pattison
Executive Member
AI Forum New Zealand
Head of Delegation for NZ Mirror Committee JTC 1 SC 42 – International Standard for Artificial Intelligence
COO at Capability Collective Ltd
E| craig.pattison@capabilitycollective.co.nz **P|** +64 21 0827 1515