Treasury,

Thank you for the opportunity to respond to the proposed third amendments to the Consumer Data Right Rules.

Table of Contents

[**About AssuranceLab** 2](#_Toc77246457)

[**Executive Summary** 2](#_Toc77246458)

[**Proposed Limited Assurance reports** 4](#_Toc77246459)

**Appendices:**

[Appendix 1 - Background market view 5](#_Toc77246460)

[Appendix 2 - Concerns with the Amendments 6](#_Toc77246461)

[Appendix 3 – Risk-based access considerations 8](#_Toc77246462)

[Appendix 4 – Reasonable and limited assurance 9](#_Toc77246463)

We welcome any questions from Treasury in relation to the contents of this letter, assurance reporting, the state of play with global standards, the maturity of Australia’s cybersecurity ecosystem, or the assurance challenges with the CDR rules that has been hindering its accessibility to date.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Paul WenhamCo-founder & CEOhe/him/his | AssuranceLab |  |  |  |

|  |  |  |
| --- | --- | --- |
|

|  |
| --- |
|  |

 | +61(0) 490 086 000 |
|

|  |
| --- |
|  |

 | paul@assurancelab.com.au |
|

|  |
| --- |
|  |

 | [https://assurancelab.com.au](https://www.assurancelab.com.au/) |
|

|  |
| --- |
|  |

 | Lvl 3/11 York Street, Sydney, Australia |

 |

 |

# **About AssuranceLab**

AssuranceLab is a for-purpose B-Corporation, a Certified Public Practice accounting firm, and a leading provider of information security audits under the System and Organisation Control (‘SOC’) standards. We are the leading provider of SOC 2 reports in ANZ (by # of clients) serving over 60 cloud software providers as annual audit clients across Australia, New Zealand, the US, Ireland, Singapore, The Philippines and Vietnam. AssuranceLab began working with the Consumer Data Right in 2021.

# **Executive Summary**

We understand the CDR legislation is designed to increase competition and improve the products and services offered to Australians. The policy objectives strike a balance between broad participation and accessibility while minimising the information security and privacy risks for Australians’ data.

**Market view**

We recognise the challenges associated with the reasonable assurance reports that have hindered accessibility for the CDR. While those historical observations remain accurate to some degree, it’s important to consider:

* Australia’s cybersecurity maturity trails our US and UK peers (significantly);
* The existing ASAE 3150 assurance reports for Schedule 2, set a more rigorous standard than global ‘benchmarks’ like SOC 2 and ISO 27001;
* That significant uplift in standard is both more challenging and more important in Australia compared to the US and UK where the starting standard is higher;
* It takes time for the ecosystem to build the knowledge, experience, methodologies, capacity, scale, and the confidence that leads to smoother and lower cost accreditation services;
* The path to accreditation is now buoyed by a healthy market of service providers with specialisms in infrastructure and policy implementation, controls assessments, and security and privacy experts on retainers, etc. that can help aspiring ADRs achieve compliance; and
* The accountancy firm market has further to go to streamline the services for accreditation, but there’s a confluence of positive market developments that is rapidly improving this part of the ecosystem.

All of the above takes time to develop and has come a long way in the last 12 months, especially the last three. New access models without a clearly established minimum standard of validating the information security and compliance to Schedule 2 may be a backwards step in the policy objectives of the CDR.

Our background narrative expanding on the above observations is included in [Appendix 1](#_Appendix_1_-).

**Summary of concerns**

With respect to the Sponsor-Affiliate and CDR Representative models:

* There is ambiguity in the minimum standard of compliance validation for Schedule 2 by sponsors and principals for their affiliates and representatives.
* Generally, the data recipient organisations, do not have the qualifications, expertise, experience, systems, and processes, to know what constitutes compliance and to effectively verify compliance to Schedule 2.
* Intermediaries are in a competitive market, competing on their ability to lower the barriers to participation for data recipients. Also being the adjudicator on their customers’ information security practices (one of the highest barriers), raises two conflict of interest concerns:
	+ (1) it puts intermediaries in a position where they may have to choose between protecting consumer interests regarding information security and privacy against onboarding a new customer, and
	+ (2) their competitive proposition is based on the total costs of access, which are lower with reduced rigour of information security validation.
* As it stands, it’s hard for Fintech’s to access cyber liability insurance in Australia’s immature insurance market. That may get worse for all ADRs with liability that extends to third parties in the complex, uncertain arrangements under the new models of access.
* The CDR Representatives and Sponsor-Affiliate models set a significantly different standard of compliance to the unrestricted ADR model, despite in many cases relating to the same information security risks. Independent review by qualified professionals governed by the ASAE standards of professional conduct, independence, and reasonable assurance practices, sets a significantly higher bar than the same Schedule 2 rules without those supporting standards and independent validation. This may create an uneven playing field and a significantly different standard of practice across the CDR ecosystem.

Each of these factors may increase the security and privacy risks for consumer data. These concerns are explained further in [Appendix 2](#_Appendix_2_-).

**Proposed solution**

We recommend Treasury introduces a **limited** assurance report under ASAE 3150 for Affiliates and CDR Representatives. This sets a consistent, minimum standard with independent validation that may be about 75% less cost and time as the existing reasonable assurance reports. This independent validation provides the checks and balances that ensures information security and privacy standards are upheld across the entire CDR ecosystem to balance the CDR policy objectives.

To further improve accessibility, we would recommend considering this approach to also apply for smaller, less complex data recipients with a lower volume of data processing. In these cases, the accessibility challenges are most significant, and the inherent information security risk is lower (likelihood and impact of data breaches are lower). This would enable smaller and earlier stage companies to get started using CDR data with a level of assurance commensurate with the related information security risks. This risk-based consideration is explained further in [Appendix 3](#_Appendix_4_–).

# **Proposed Limited Assurance reports**

The Consumer Data Right rules currently requires a *reasonable assurance* engagement for accreditation. The definitions from ASAE 3150 are included in [Appendix 4](#_Appendix_3_–) for reasonable and limited assurance engagements. Audit files for an ASAE 3150 Type 1 engagement (for accreditation) need to contain evidence of each control, the testing procedures performed, and the control characteristics validated to prove the controls were suitably designed and placed into operation. Covering ~60-80 control activities in this way requires significant information collection, documentation, audit review, queries, edits, quality review and reporting work by audit firms; driving cost and time for both parties.

The proposed self-attestations could be validated through a *limited assurance* engagement under ASAE 3150. Limited assurance engagements require significantly less work by audit firms. There is flexibility for Treasury to define what is a “meaningful” level of assurance in this context, and the way it would work in practice.

As one example, the data recipients may prepare their self-attestation for the limited assurance review (or engage a service provider to help them with that). The limited assurance review could be conducted through audit firm walkthroughs to verify the controls without the full audit procedures of a reasonable assurance engagement. This may include only reporting by exception if any cases of non-compliance or control weaknesses were observed. The independence, expertise, experience and rigour of supporting standards, would provide a substantially higher level of assurance than a self-attestation on its own, without the high costs and time commitments of the existing reasonable assurance reports. We anticipate this approach would be up to 75% lower cost and time involved compared to the median costs and time of the existing reasonable assurance reporting.

# **Appendix 1 - Background market view**

From May to July 2020, AssuranceLab spoke with over 20 founders and businesses that were considering accreditation under the Consumer Data Right. Almost universally, the feedback was that accreditation was not viable. It was either cost prohibitive, didn’t support the business case to pursue a new product/feature/service, or that continuing to obtain data directly from ADI relationships or screen scraping was more viable.

In August 2020, we held a workshop with the ACCC accreditation team, expressing our concerns about the rigorous standard for accreditation and how that would limit the uptake accordingly. That feedback was well received by the ACCC. We have continued to liaise with the ACCC since, finding that what initially seemed like a “black-and-white” set of rigorous requirements, did allow for judgement and flexibility by audit firms like ourselves. We cautiously observed as the practice evolved and early ADRs became accredited. We decided in 2021 to enter the market, at the point we were confident we could viably offer these services.

We now see the market evolving at a fast pace with several complementary developments in progress. Accounting firms are hiring additional team members, developing their knowledge and expertise in the area of CDR, and refining their audit approaches to be more scalable and effective. With each new ADR engaging in an ASAE 3150 audit, and the increased interest of new ADR candidates, the economies of scale are improving. Audit firms are increasingly prepared to invest in CDR and prioritise this area of their business. Speaking of AssuranceLab specifically, we have developed internal and external practice guides, mapping tables between common cloud infrastructure and software to the CDR requirements, formed partnerships with complementary service providers, built a new audit tool for a seamless agile audit process, and we have recently secured new team members and are continuing to hire others. These developments in AssuranceLab and the broader audit firm market are all leading towards smoother and lower cost accreditations for aspiring ADRs.

# **Appendix 2 - Concerns with the Amendments**

Most of the proposed updates in the third amendment have been received positively by AssuranceLab and our associates. The main concern we want to highlight is the potential to undermine the quality and integrity of information security and privacy in the CDR Representative and Sponsor-Affiliate access models.

Our experience in the market gives us an insight into the global drivers behind assurance reports, which is, that questionnaires, self-assessments, attestations and independent reviews by organisations without specialism and expertise, are inadequate for validating information security practices of third parties. It’s recognised by large global enterprises that these practices to manage outsourced service providers without an independent validation by suitably qualified auditors, are not reliable. This is the major driver behind standards like SOC 2 and ISO 270001.

We expect the following adverse outcomes from the proposed models that have ADRs and self-attestations replacing the need for assurance reports.

**i) Sponsors are incentivised to lower the standard**

Potential sponsors and principals, e.g. Intermediaries, compete on lowering the barriers to access. This power to sponsor their potential customers, offers a new way to compete by lowering the barriers to entry, including the rigour of information security requirements that takes significant time and resources from those ADRs. In a competitive market, this incentive and opportunity may create a race to the bottom on the standard of practice.

**ii) ADRs are not qualified to confirm compliance**

The slow start and high fees for accreditations are in part due to the time it has taken for accountancy firms to learn the rules and requirements, and develop their audit practices to meet the standards. The new models are effectively replacing the role of these firms with the expectation that sponsors, principals and/or the ADRs and representatives perform the equivalent compliance validation role. These businesses generally do not have the experience, expertise, systems, or processes to perform this role effectively.

**iii) Inconsistency and an uneven playing field across the CDR ecosystem**

Assurance reports under ASAE 3150 are supported by hundreds of pages of guidance, professional and ethical conduct standards, subject to quality review schemes by CA ANZ, and decades of live practice. By contrast, a self-assessment or validation of compliance by an ADR is vague and leads to different interpretations and standards. That will create inconsistency and an uneven playing field across the CDR ecosystem.

**iv) Independent audits are important to the standard of practice**

In our experience, every Type 1 audit and report we have completed (SOC 1, SOC 2, & ASAE 3150), has surfaced control design and implementation issues that were remediated upon our identification of those. In most cases, these businesses had completed self-assessments prior to our engagement. Many of those clients have served the Big4 Australian banks or other large global enterprise and have been subject to vendor audits previously. Even still we identified significant control gaps that required remediation to achieve the SOC 2 standard, which is less stringent than CDR Schedule 2. Experience, expertise, clearly defined standards and complete independence in the review process are important influences on the standard of practice.

# **Appendix 3 – Risk-based access considerations**

The inherent level of information security and privacy risk for using CDR data may consider the following three factors:

* **Organisation size**Smaller organisations, while sometimes perceived as riskier due to the higher financial and operational risks, generally have a lower inherent information security risk. This is due to the lower volume of people in contact with the data, a higher level of seniority / higher ratio of senior personnel, and less dispersed responsibilities including those for information security.
* **Breadth and complexity of system components**There is a significantly different risk profile comparing hundreds of legacy systems in a bank, compared to a simple modern cloud infrastructure and software environment. The latter centralises the data for fewer locations and exposure, applies best practices tools and configurations by default “out-of-the-box”, simplifies the monitoring, and leverages best practices provided by cloud service providers under the shared responsibility model for security.
* **Volume of data handling**A lower volume of data reduces the magnitude of impact from potential security breaches or failures.

A benefit of these drivers is they align to where the accessibility challenges of the CDR are most prevalent. The costs and time involved are more prohibitive for smaller businesses that would naturally fall into the lower tiers of each of the above. We recommend treasury considers allowing a limited assurance report per the above proposal for organisations where all three of the above are “low”. This may change over time with the ongoing assurance requirement every two years. This can be uplifted as needed to a reasonable assurance engagement based on the volume, scope of systems, or organisation size, increasing beyond defined thresholds.

# **Appendix 4 – Reasonable and limited assurance**

**ASAE 3150, Definitions (Ref: Para. 17(jj) and 17(bb)):**

***Reasonable assurance engagement―****An assurance engagement in which the assurance practitioner reduces engagement risk to an acceptably low level in the circumstances of the engagement as the basis for the assurance practitioner’s conclusion. The assurance practitioner’s conclusion is expressed in a form that conveys the assurance practitioner’s opinion on the outcome of the measurement or evaluation of the underlying subject matter against criteria.*

***Limited assurance engagement―****An assurance engagement in which the assurance practitioner reduces engagement risk to a level that is acceptable in the circumstances of the engagement, but where that risk is greater than for a reasonable assurance engagement, as the basis for expressing a conclusion in a form that conveys whether, based on the procedures performed and evidence obtained, a matter(s) has come to the assurance practitioner’s attention to cause the assurance practitioner to believe the subject matter information or subject matter is materially misstated. The nature, timing and extent of procedures performed in a limited assurance engagement is limited compared with that necessary in a reasonable assurance engagement but is planned to obtain a level of assurance that is, in the assurance practitioner’s professional judgement, meaningful. To be meaningful, the level of assurance obtained by the assurance practitioner is likely to enhance the intended users’ confidence about the subject matter information or subject matter to a degree that is clearly more than inconsequential.*