Australian Government

Consumer Data Right

Participant Conformance Approach

Version 3.0 – 29 August 2022

Table of figures

References

Table 1: References

#	Title	Location
R1.	AEMO Website	https://aemo.com.au/initiatives/major-programs/cdr-at-aemo
R2.	CDR Compliance and Enforcement Policy	https://www.cdr.gov.au/resources/guides/compliance-and-enforcement-policy
R3.	CDR Consumer Data Standards	https://consumerdatastandardsaustralia.github.io/standards/
R4.	CDR Consumer Experience Guidelines and Standards	https://consumerdatastandardsaustralia.github.io/standards/#consumer-experience
R5.	CDR CTS guidance material	https://www.cdr.gov.au/resources/guides/conformance-test-suite-version-history-and-guidance
R6.	CDR CTS Technical Guidance	https://www.cdr.gov.au/resources/guides/conformance-test-suite-version-history-and-guidance
R7.	CDR On-boarding guide	https://www.cdr.gov.au/sites/default/files/2021-06/CDR-participant-on-boarding-guide_v1-2.pdf
R8.	CDR Rules	https://www.legislation.gov.au/Series/F2020L00094
R9.	CDR Service Management Portal	https://cdrservicemanagement.atlassian.net/servicedesk
R10.	CDR Service Management Portal User Guide	https://www.cdr.gov.au/resources/user-guides/cdr-service-management-portal-user-guide
R11.	CDR Support Portal	https://www.cdr.gov.au/resources/guides/conformance-test-suite-version-history-and-guidance
R12.	CDR Test Documentation Repository	https://github.com/ConsumerDataStandardsAustralia/standards-testing
R13.	CDR Website	https://www.cdr.gov.au/
R14.	Data Holder User Journey	https://www.cdr.gov.au/for-providers/data-holder-user-journey
R15.	Data Recipient User Journey	https://www.cdr.gov.au/for-providers/data-recipient-user-journey
R16.	OpenID Conformance Suite	https://openid.net/certification/about-conformance-suite/
R17.	Participant On-boarding Guide	https://www.cdr.gov.au/resources/guides/participant-on-boarding-guide
R18.	Participant Tooling Mock Solutions	https://www.cdr.gov.au/for-providers/participant-tooling
R19.	CDR Sandbox	https://www.cdr.gov.au/for-providers/participant-tooling/consumer-data-right-sandbox
R20.	Postman Collection	https://github.com/ConsumerDataStandardsAustralia/dsb-schema-tools
R21.	CDR Performance Dashboard	https://www.cdr.gov.au/performance

1. Introduction

A critical element of the Consumer Data Right (CDR) ecosystem is the successful operation of all participants' technology solutions. This Participant Conformance Approach (PCA) provides guidelines for participants who are seeking to enter the ecosystem (new participants) and participants who are already part of the ecosystem (active participants). It outlines mandatory and voluntary activities that improve conformance to the CDR rules and CDR standards throughout three broad phases of a participant's technology lifecycle:

1. Development and testing of participants' CDR solutions
2. Activation on the CDR Register
3. Ongoing operations and conformance

Further information relating to a participant's user journey can be found via the Data Holder User Journey and the Data Recipient User Journey pages on the CDR website.

New and active participants are expected to ensure their solution correctly incorporates the relevant CDR scope and follow an established testing process in conjunction with formal software release and risk management practices. This could include activities such as unit, system, and integration testing as well as user acceptance testing (UAT), performance testing, penetration testing and where applicable testing with secondary data holders. Internal testing is expected to be completed prior to testing against the ACCC's Conformance Test Suite (CTS).

In addition, active participants should perform regression testing on previously tested code to ensure no defects have been introduced and to be confident that their CDR solution operates as intended.

The ACCC is currently the Accreditation Registrar (the Registrar) for CDR. Part of the Registrar's functions include requesting an Accredited Person or a Data Holder to do specified things (rule 5.30(c)) in order for the Registrar to perform its function to maintain the security, integrity and stability of the Register of Accredited Persons and associated database (herein the Register) (rule 5.30(b)). In this context, this means that the CDR Registrar may request information and evidence from participants on their internal testing and outcomes.

The ACCC is also responsible for monitoring compliance and enforcement of the CDR regulatory obligations and expects that participant solutions continue to incorporate the correct release scope as per the CDR rules and standards. Further information on CDR's Compliance and Enforcement Policy can be found on the CDR website.

2. Support Available for Development and Testing of Participant CDR Solutions

During the development and testing phases, new and active participants have access to a range of tools and support to assist with ongoing development and implementation of solutions that conforms to the CDR rules and standards. Benefits of using these support tools can include reduced development costs, expedited development speed, and the ability to identify defects earlier in the development cycle.

Although not discussed in this document, there are a range of commercial providers who also offer paid services to assist participants meet their compliance obligations, as well as platform-as-a-service services for CDR.

2.1 Solutions & Support Provided by the ACCC

2.1.1 Participant Tooling Mock Solutions

The ACCC has been working on ways to help CDR participants understand the CDR ecosystem's technical requirements, as well as develop and maintain solutions that can operate effectively within the ecosystem.

As the first step in the participant tooling journey, the ACCC has built a series of free, open-source mock solutions covering the CDR Register, Data Holder and Data Recipient. A separate mock Energy Data Holder is also available to support rollout of CDR into the Energy sector.

The source code can be used by the community during development and testing of their CDR solutions and allows the end user to test the various interactions by changing input values, executing and viewing the expected response. The Mock Data Recipient requires a Mock Register and a Mock Data Holder to completely mimic the CDR Ecosystem. Participants can swap out any of the Mock Data Holder and Mock Data Recipient solutions with their own solution. The mock solutions are constantly updated as the CDR rules and standards continue to evolve.

2.1.2 CDR Sandbox

The ACCC hosted CDR Sandbox is a free tool that builds on the work of the participant tooling mock solutions by enhancing the capability available to participants and their vendors to develop and perform end to end testing of their own solutions in a sandbox environment.

The sandbox facilitates participants discovering and connecting with each other to test their solutions in a 'production-like' environment. It also allows participants to test against hosted versions of the mock solutions.

It provides the following features to new and existing participants:

- Ability for participants to use their own seed data to perform end-to-end testing against the participant tooling mock solutions or interact directly with other participants to exchange test data.
- Management portal to assist participants with the integration and management of their own solutions within the environment.

- Revised versions of the mock solutions compatible with the latest rules and standards, which have been updated to include the energy sector.

2.2 External Support & Solutions

2.2.1 DSB Test Documentation Repository

The Data Standards Body (DSB) maintains a CDR Test Documentation repository of Test Cases and Assertions that describe the way the standards can be tested. These are logically grouped into Suites and Scenarios for each Sector and API to validate an API against the Consumer Data Standards.

The aim is to provide the community with a resource they can use to create their own test suites to verify a CDR implementation aligns with the standards. It consolidates many references within the standards, including normative references, that apply to a single API, to help people interpret and understand the standards.

This repository will continue to be expanded to cover test cases for all resource APIs for Banking and Energy in addition to Common and Admin. Energy is the current priority given approaching obligation dates. The DSB anticipates this documentation, in time, will also reference DSBs postman collection to validate schemas.

2.2.2 FAPI open-source testing tools

The Consumer Data Right uses the Financial-grade API (FAPI) profile, which is a secure profile of OpenID Connect, OAuth 2 and other standards that facilitates financial and other transactions requiring higher security and non-repudiation.

The OpenID Foundation is a non-profit international standardisation organisation specialising in the standardisation of internet identity and API access management, and hosts an open-source Conformance Suite that covers OpenID connect and FAPI test plans for the Australian CDR. This suite covers an extensive range of FAPI scenarios that the ACCC's Conformance Test Suite is not designed to cover.

Please note, the ACCC does not require Participants to become FAPI certified officially via the OpenID Foundation's certification scheme. The OpenID Foundation is an external provider and is not affiliated with the ACCC.

2.2.3 AEMO's integrated test environment for Energy Data Holders

The Energy Sector utilises a Shared Responsibility (SR) data model, meaning when a data holder receives a request for SR data, they are required to obtain that data from the secondary data holder before providing the data back to the accredited data recipient. The Australian Energy Market Operator (AEMO) is the designated secondary data holder holding SR data for the energy sector.

To assist with testing the connection between energy retailers (as the primary data holders) and AEMO (as the secondary data holder), AEMO will make testing available for Data Holders.

Further information on AEMO's role in CDR as well as how to access the test environment can be found on AEMO's website.

It is recommended for participants to complete testing with AEMO prior to commencing CTS.

3. Activation on the CDR Register

Activation is the final step prior to participating in the CDR ecosystem. The Conformance Test Suite (CTS) is a key input into activation requests and on-going security and stability of the ecosystem. After the completion of CTS, the Registrar may request additional evidence of a participants' internal test results as part of the activation process. One of the final steps in the on-boarding process requires participants to provide an attestation confirming they have completed appropriate internal testing and their solution is ready to enter the ecosystem. The attestation applies for each Data Holder brand and Accredited Data Recipient software product.

3.1 CTS introduction

The CTS is a final checkpoint for participants of key elements of a participant's solution before activation. Each new participant (additional Data Holder brands and Accredited Data Recipient software products) must complete the CTS before they can be made active on the CDR Register.

The primary focus of the CTS is to provide the ACCC as the Registrar, performing its function to maintain the security, integrity, and stability of the Register, with a level of confidence that:

- a participant has delivered to the security standard required for CDR
- a participant can share consumer data in the CDR ecosystem without significant disruption
- key capabilities have been built, unless an exemption has been granted

The CTS is designed to verify a limited subset of standards alignment against security profile and consent components as well as other high-risk areas. The CTS does not test the connection between a primary data holder and a secondary data holder under the Shared Responsibility Datasets model as used by the Energy sector, please refer to the AEMO integration environment for Shared Responsibility DH testing.

While CTS conforms to the CDR standards, its role is not to validate a participant's solution is fully compliant with those standards. Participants are accountable for compliance with the CDR Standards and must address any alignment issues prior to commencing CTS testing. Many of the tools described in Section 2 of this document can be used to assist a participant's full conformance with the CDR Standards during development and testing.

The CTS will continue to evolve and further test scenarios will be added as ecosystem requirements change. The execution of CTS is not a one-time event for a participant; it is expected that active participants will complete the new test scenarios. This is described in more detail in section 4.1.

Additional guidance material relating to the CTS include:

- CTS guidance material for Data Holders and Data Recipients.
- An up-to-date list of the available test scenarios on the CDR website

An overview of CTS test plan versions on the CDR website, which includes the test plan release date, an overview of the different test scenarios, and the high-level scenario changes between different versions.

3.2 CTS for new participants

The conformance testing for new participants who are not yet on the register is based on the following:

- Participant solutions should be production-ready and internal testing completed by the participant before CTS testing commences.
- New participants must confirm the technical conformance of their production-ready solution using a range of test scenarios targeting a limited subset of high-risk areas by completing test scenarios through the CTS as part of the on-boarding process. This and all other on-boarding requirements are explained in more detail in the Participant On-boarding Guide.
- New participants should be testing against the version of the CDR Standards based on their planned activation date. This means that, depending on a participant's planned activation date, a participant might be assigned a new test plan version.
- New participants will need to complete all relevant CTS tests within the assigned test plan, as well as the other on-boarding steps, which are outlined in the Participant On-boarding Guide, before the activation assessment can be sent to the Registrar to make a decision if the participant can be made active on the Register. The Registrar may request further evidence of conformance. If a participant is unable to execute all applicable tests (e.g. if certain tests are not relevant for an Accredited Data Recipient offering or the participant has an active exemption), they are required to inform the ACCC, as outlined in the CTS guidance material.

Figure 1 outlines the high-level steps for internal participant testing in relation to conformance testing activity, and the sequence of the CTS in relation to when new participants can commence live data sharing. CTS conformance testing is step 7 of the on-boarding process for new participants as outlined in the Participant On-boarding Guide.

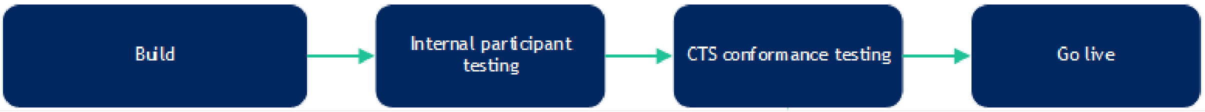


Figure 1: Internal participant testing in relation to conformance testing

Internal participant testing for new participants can be conducted prior to and in parallel to Steps 1 to 6 of the On-boarding process.

! Note

Passing all CTS tests does not guarantee compliance with the rules [R5] and Consumer Data Standards [R3] obligations.

Participants who are preparing to meet a compliance milestone should allow sufficient time in their plans to execute CTS. While the CTS can be completed in a few hours, the duration required to execute CTS is participant dependent, it is not unusual for completion of CTS to take between 4 and 8 weeks

4. Ongoing Operations and Conformance

Fostering an ongoing culture of conformance is critical to achieving the objectives of the CDR. Consumers must be confident that the CDR system works as intended and that the regulatory framework put in place will protect their interests. Consumers should be able to trust that there is ongoing monitoring and assurance of CDR participants' conformance with the relevant CDR rules and standards s.

The ACCC is committed to driving a high level of ongoing compliance within the CDR system and will use the most appropriate tools available to us to achieve our continuing compliance objectives. This is particularly important as the CDR is rolled out more broadly.

4.1 CTS for active participants

The ACCC may require participants who are already active in the CDR ecosystem to retest against CTS in response to changing ecosystem requirements. In some instances, this will be voluntary and in others retesting will be mandated as outlined below.

4.1.1 Voluntary testing

The CTS will be readily accessible for active participants to use on a voluntary basis. Access to CTS can be requested via the participant portal by requesting a new PKI test certificate. The ACCC encourages active participants to retest through the latest version of the CTS:

- If they make a significant change to their solution/technology
  - Participants are strongly encouraged to retest through the CTS prior to the production release of the changes to their solution / technology / use case. This is to ensure the interactions of the solution within the CDR ecosystem continue to work as expected and to reduce critical points of failure.
- When there is a significant change in the CDR rules or CDR standards
  - Participants are strongly encouraged to revisit CTS before a change in the rules or standards comes into effect. This is to ensure that active participants remain in sync with new participants joining the ecosystem. The ACCC intends to announce changes to CTS resulting from changes to the rules and standards at least 4 months before new rules or standards come into force and intends to make new CTS scenarios available for testing 3 months prior to this date.
- Active participants who wish to revisit CTS after activation will be allocated to the latest available test plan that includes future changes to the rules or standards or the version prior to that one if they wish to test against the latest current obligations in the ecosystem.
- Even if there is no material impact to the CTS, regular retesting through the latest version of CTS can be an effective form of regression testing areas covered by CTS. The ACCC encourages participants to revisit CTS at least once every 12 months.

Figure 2 outlines the anticipated sequence of a participant's internal testing in relation to the CTS, when active participants update their solution.

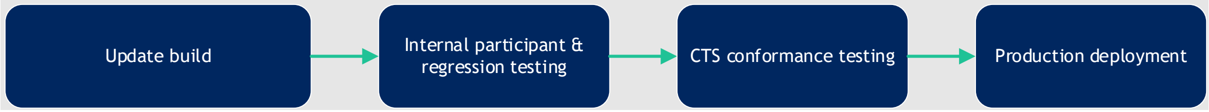


Figure 2: Active participants - update in participant solution

4.1.2 Mandatory testing

Under certain circumstances, the Registrar may mandate active participants to retest their solution through the CTS, to reduce broader risks in the ecosystem. Examples that might form part of the consideration for such a request could include, but are not limited to:

- the stability of the ecosystem (e.g. due to information security concerns)
- volume and severity of incidents in the ecosystem

Figure 3 outlines the anticipated sequence for conformance testing in relation to production deployments when active participants are notified of ACCC expectations regarding retest.

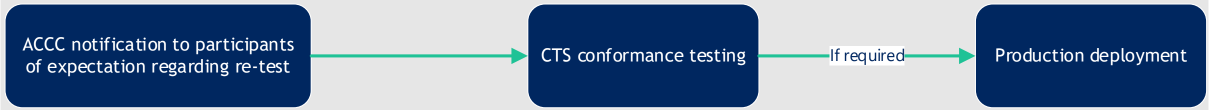

ACCC notification to participants of expectation regarding re-test
CTS conformance testing
If required
Production deployment

Figure 3: Active participants - retest as requested by the ACCC

4.1.3 Updates to CTS test plans and test plan retirement

The CTS plays a key role in ensuring the interactions of a participant solution against the Register interactions are working as expected and to reduce critical points of failure. The CTS will evolve over time in response to changing ecosystem requirements. This may result in new test plans and scenarios being introduced. An up-to-date list of test plans and scenarios are available on the CDR website.

The ACCC intends to announce major CTS releases 4 months in advance and publish any new test cases 3 months prior to the date the changes will take effect. Note that in some circumstances (e.g. if required to maintain the integrity, security and stability of the CDR Register) scenarios might be added closer to the date new rules and standards are effective.

The ACCC strongly recommends and may mandate active participants retest through CTS in conjunction with the introduction of any new rules or standards to reduce critical points of failure. New participants will be allocated to the test plan that is most relevant to their projected activation date.

A new test plan could be released when minor changes to existing scenarios are required or as new scenarios are added. Participants will be notified when a new test plan is published.

While new test plans are created in response to changing ecosystem requirements, older test plans will retire over time. Until the date new rules and standards are in force, two test plans will be available:

- A test plan that supports future changes to the ecosystem prior to the new compliance date
- A test plan that reflects the current state of the ecosystem. Participants can be allocated to this plan only prior to the future compliance date.

! Note

When new rules come into force the old test plan will be retired once the last participant allocated to this plan completes CTS or 3 months after the compliance date. This is to ensure that new participants test scenarios that are relevant to the rules and active participants remain in sync with new participants joining the ecosystem.

4.2 Get Metrics API

The Get Metrics API as defined by the CDR standards is a binding data standard that allows the ACCC to obtain operational statistics from Data holders on the operation of their CDR implementation and provides insight into how the CDR ecosystem is operating. This includes monitoring average response times and the availability of the Data holders' systems in line with the non-functional requirements (NFRs) of the CDR system.

Data holders are required to make the Get Metrics API available for ACCC to call from the date of each brand activation on the Register and must ensure the data returned in response to this API call is complete and accurate. Subsets of the Get Metrics Data is published via the CDR Performance Dashboard.

4.3 Rule 9.4 reporting

Rule 9.4 of the CDR rules requires data holders and accredited data recipients to submit 6-monthly reports to the ACCC and the Office of the Australian Information Commissioner (OAIC). Participants are to submit reports to the ACCC and the OAIC within 30 days of the end of each reporting period, which are 1 January to 30 June and 1 July to 31 December of each year.

A data holder is required to prepare a report which sets out the number (if any) of product data requests, direct-to-consumer data requests, and consumer data requests made via Accredited Data Recipients. The report also requires a summary of CDR complaint data and the number of times the data holder has refused to disclose data, including the rule and standard relied upon for the refusal.

A secondary data holder is required to prepare a report which sets out the number of requests for Shared Responsibility data from the primary data holder, and the number of times the secondary data holder has refused to disclose data, including the rule and standard relied upon for the refusal.

An accredited data recipient is required to prepare a report which summarises CDR complaint data and sets out the number of consumer data requests the Accredited Data Recipient made during the period, the proportion of CDR consumers who opted to delete their data, information about any new goods or services offered using CDR data, and information about disclosures of trusted insights, trusted advisors and any sponsors or affiliate arrangements.

Additionally, an Accredited Data Recipient that is also a CDR principal must submit a report under rule 9.4(2A) for each of its CDR representatives.

Both the ACCC and the OAIC can publish these reports or require an Accredited Data Recipient to publish its report on its website. The ACCC or OAIC may audit a CDR participant's compliance with their obligations under the *Competition and Consumer Act 2010*, the CDR rules and the CDR standards and may request a CDR participant to provide copies of records required to be kept and maintained under the CDR rules.

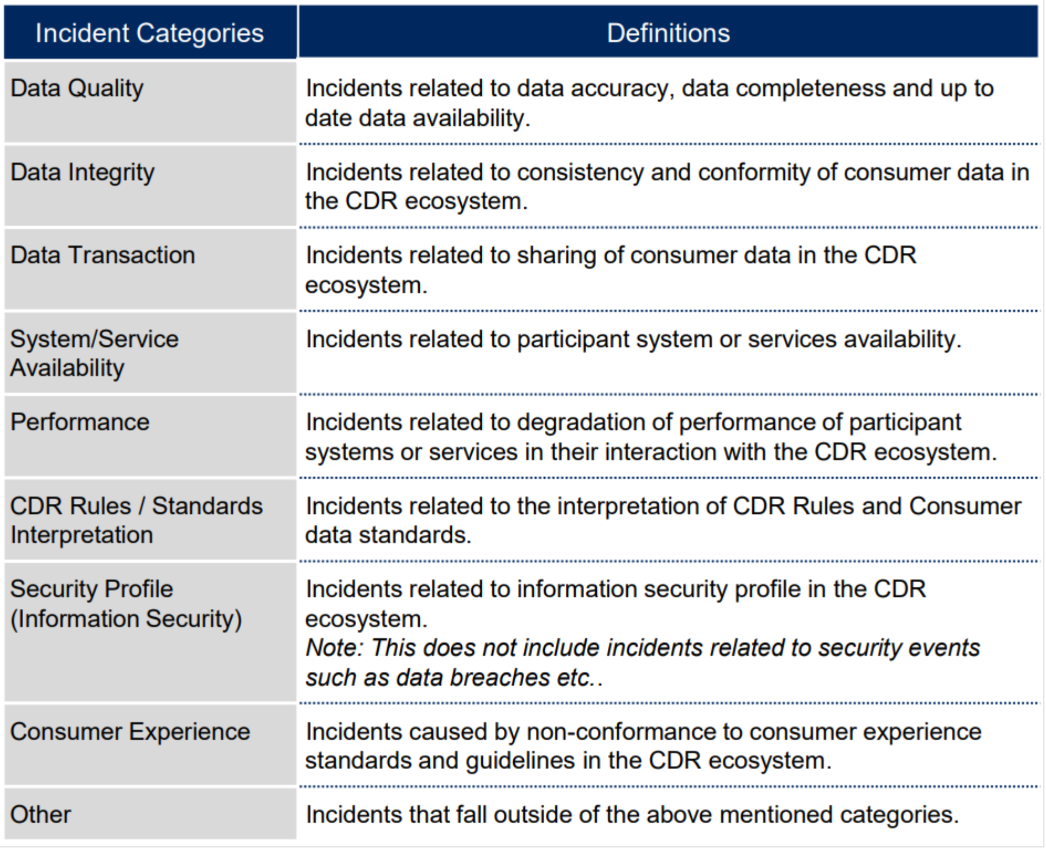
Reports are to be submitted via the CDR Participant Portal, or in a form as approved by the ACCC. Further resources to assist with submission of rule 9.4 reporting is available, including:

- Examples and templates of Rule 9.4 reports
- The CDR Participant Portal user guide

4.4 Technical Operations Service Management Portal

The CDR Service Management Portal is provided by the ACCC for CDR participants to communicate technical incidents between each other, or with the ACCC CDR Technical Operations team. It is an important tool for enabling participants to communicate with one another and to ensure incidents are identified, assessed, and resolved in an efficient and timely manner.

The table below outlines the various incident categories that can be reported and triaged between participants.



Incident Categories	Definitions
Data Quality	Incidents related to data accuracy, data completeness and up to date data availability.
Data Integrity	Incidents related to consistency and conformity of consumer data in the CDR ecosystem.
Data Transaction	Incidents related to sharing of consumer data in the CDR ecosystem.
System/Service Availability	Incidents related to participant system or services availability.
Performance	Incidents related to degradation of performance of participant systems or services in their interaction with the CDR ecosystem.
CDR Rules / Standards Interpretation	Incidents related to the interpretation of CDR Rules and Consumer data standards.
Security Profile (Information Security)	Incidents related to information security profile in the CDR ecosystem. *Note: This does not include incidents related to security events such as data breaches etc..*
Consumer Experience	Incidents caused by non-conformance to consumer experience standards and guidelines in the CDR ecosystem.
Other	Incidents that fall outside of the above mentioned categories.

The CDR Technical Operations team undertake a 'monitoring' approach on technical incidents raised between participants in order to mediate, advise or support the process of technical incidents between participants being efficiently progressed through to resolution. Further information can be found in the CDR Service Management Portal User Guide.

Appendix A: Terminology

Shortened Form	Extended Form
ACCC	Australian Competition and Consumer Commission
AEMO	Australian Energy Market Operator
CDR	Consumer Data Right
CDR rules	Competition and Consumer (Consumer Data Right) Rules 2020
CDR standards	Consumer Data Standards
CTS	Conformance Test Suite
Data holder (DH)	A Legal Entity (participant) that is a data holder subject to CDR data sharing obligations (data sharing obligations) under the CDR Rules.
DSB	Data Standards Body
Accredited data recipient (ADR)	A Legal Entity (participant) who has been granted accreditation by the DR Accreditor and is able to receive CDR data.
Participant	In this context, a participant is an entity that has been accredited (data recipient) or registered (data holder) and is preparing or currently undertaking on-boarding in order to participate in the CDR system
New participant	A participant entering the CDR ecosystem for the first time
Active participant	A participant already part of the CDR ecosystem
CDR Registrar	The person or entity appointed as the Accreditation Registrar under the CDR legislation, currently the ACCC.
Mock Register	A simulation of the production CDR Register
Mock Data Holder	A simulation of a data holder
Mock Data Recipient	A simulation of a data recipient
SR	Shared Responsibility