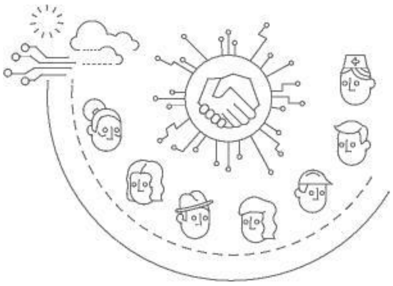
CONSUMER DATA RIGHT (CDR) INFORMATION SECURITY ACCREDITATION



Obtaining assurance on the security of your CDR data environment

Accredited Data Recipient (ADR) applicants must demonstrate the security effectiveness of their people, processes and technology. The key is to demonstrate security, whilst minimising the cost.

Consumer Data Right

Consumer Data Right (CDR) gives individuals and businesses the right to share data with accredited organisations. It is now active in banking, so you may choose to share your banking data to get a better loan offer, or with an app to access a new service. The Energy sector will be next in 2022.

The aim of CDR is to allow individuals and businesses (currently only sole traders, with other businesses going live from 1 November 2021) to have better control over the information that is held on them by organisations (Data Holders). Individuals and businesses can then consent to that information being shared with others (Accredited Data Recipients). Individuals and businesses have control over what data is transferred, and what it can be used for. They can stop the collection of data at any time and ask for it to be deleted if it is no longer needed.

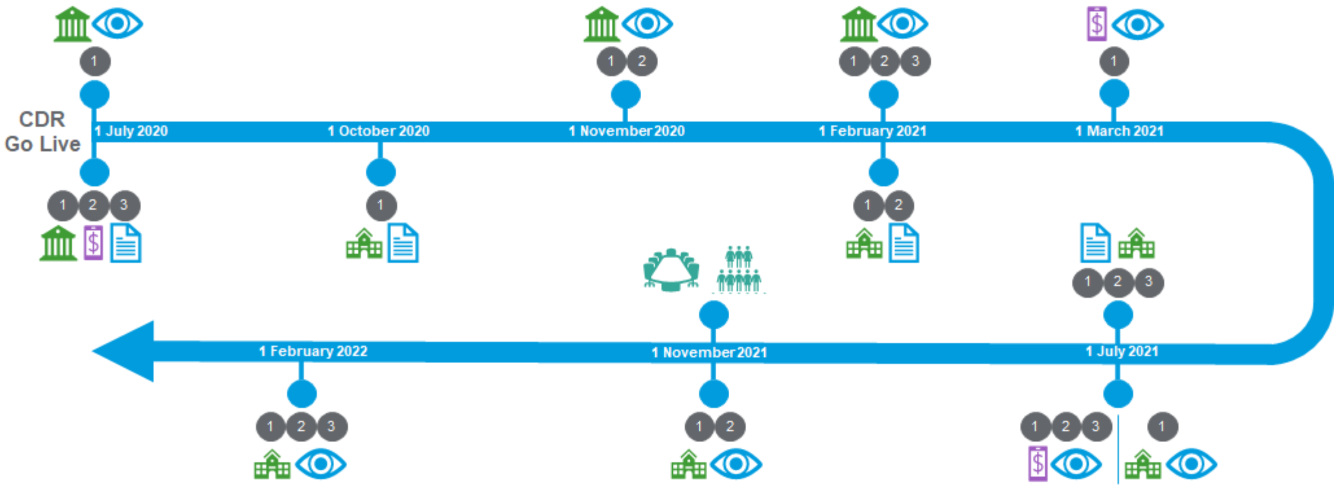
Individuals and businesses can only share their CDR data with Accredited Data Recipients (ADRs). ADR applicants need to develop use cases that are approved as part of the accreditation process, e.g. to help monitor finances, utilities and other services, and compare and switch between different offerings more easily, and obtain an independent information security assurance report.

The roll out of CDR is complex, with different organisations and data types being shared based on an implementation roadmap. For Open Banking, many organisations see July 2021 and November 2021 as the key milestones for achieving their accreditation.

ADR applicants should talk to and work with people who have already been through the accreditation process, to ensure their accreditation is as efficient and economic as possible.

Consumer Data Right Timeline for Open Banking

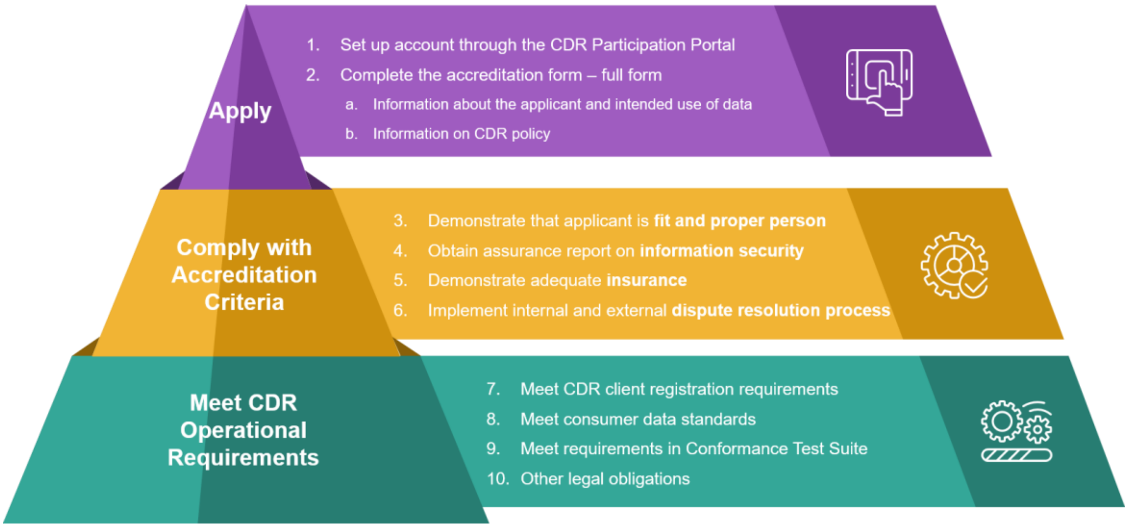
Phase 1	Phase 2	Phase 3	Key
Savings account Call account Term deposit Current account Cheque account Debit card account Transaction account Personal basic account GST or tax account Personal/Business credit card or charge card account	Residential home loan Investment property loan Mortgage offset account Personal loan Joint accounts	Business finance Investment loan Line of credit (personal/business) Overdraft personal/business Asset finance (inc. leases) Cash management account Farm management account Pensioner deeming account Retirement savings account Trust account Foreign currency account Consumer lease	📄 Product reference data 👁 Consumer data requests made by ADRs for account and transaction data 🏛 Initial data holders (NAB, CBA, ANZ, Westpac Branded products) 🏘 Any other relevant ADI and initial data holders for non-primary brand 👥 Direct to consumer data requests made by eligible consumers $ ADRs become reciprocal data holders and are subject to data sharing obligations 🤝 Businesses - non-individual, partnerships, nominated reps and secondary users



Only an organisation that has been accredited can access consented CDR data. An organisation seeking to become an ADR needs to develop and implement their own CDR data environment (the people, processes and technology) to collect, store, process and transmit CDR data securely, some of which can be done with other ADRs and Outsourced Service Providers. This typically requires a new system architecture to be designed and implemented, to ensure that CDR data is appropriately segregated and segmented.

An ADR must comply with safeguards, rules and system requirements that ensure privacy is protected and data is transferred and managed securely. The information security controls described in Schedule 2 of the CDR Rules must be independently audited with an independent assurance report required for the accreditation application. **RSM has completed four CDR information security accreditation assurance reports for ADR applicants, including Frollo and Intuit. RSM's CDR information security accreditation experience is second to none.**

Key steps in CDR accreditation



Apply

1. Set up account through the CDR Participation Portal
2. Complete the accreditation form – full form
   a. Information about the applicant and intended use of data
   b. Information on CDR policy

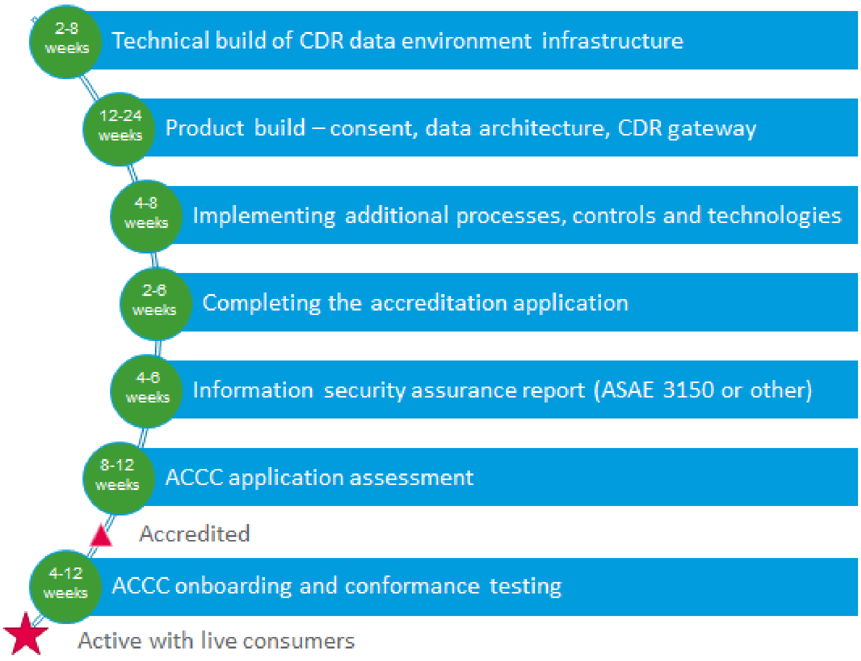
Comply with Accreditation Criteria

3. Demonstrate that applicant is **fit and proper person**
4. Obtain assurance report on **information security**
5. Demonstrate adequate **insurance**
6. Implement internal and external **dispute resolution process**

Meet CDR Operational Requirements

7. Meet CDR client registration requirements
8. Meet consumer data standards
9. Meet requirements in Conformance Test Suite
10. Other legal obligations

It can take approximately six to nine months to become an ADR that is active with live consumers, based on the below estimated timeline (noting that some of the technical build and implementation of processes and technologies can be performed concurrently):



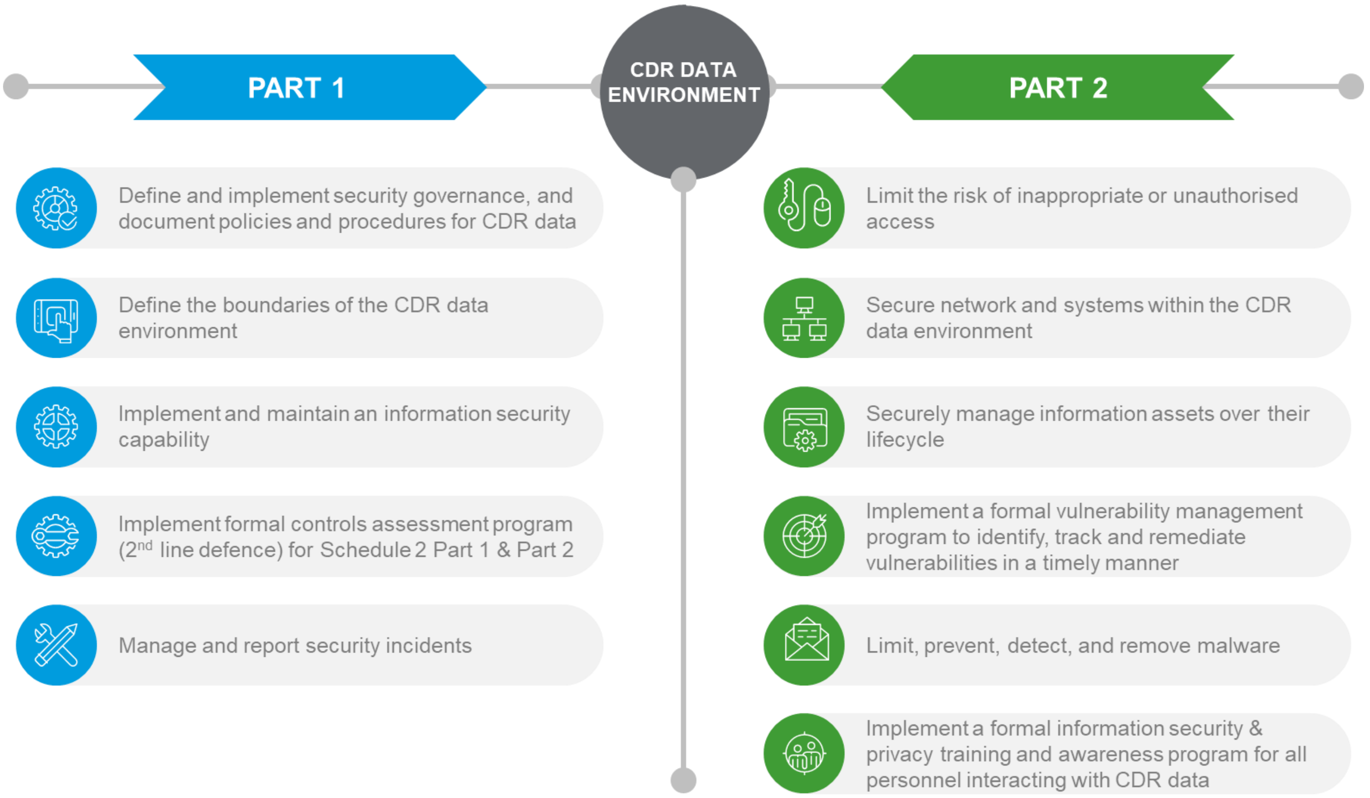
- 2-8 weeks — Technical build of CDR data environment infrastructure
- 12-24 weeks — Product build – consent, data architecture, CDR gateway
- 4-8 weeks — Implementing additional processes, controls and technologies
- 2-6 weeks — Completing the accreditation application
- 4-6 weeks — Information security assurance report (ASAE 3150 or other)
- 8-12 weeks — ACCC application assessment
- Accredited
- 4-12 weeks — ACCC onboarding and conformance testing
- Active with live consumers

To minimise the time taken for each step in the process, ADR applicants are encouraged to engage early with subject matter experts who can advise on the most efficient and effective approach. There are managed service providers who can assist with the secure infrastructure build through quick start solutions, technology providers who can provide SaaS products for consent and the CDR gateway, and continuous auditing solutions that can automate testing of some infrastructure controls.

RSM assists ADR applicants with:

- ADR application advisory support
- Security control assessment program or ISO 27001 Lead Auditor internal audit
- Penetration Testing
- Security by Design / Gap Assessment
- Defining CDR data environment boundaries
- Pre-Audit / Readiness Assessment
- Security Assurance Report Audit (ASAE 3150/3402 or SOC 1/2).

What security controls are needed?



PART 1

CDR DATA ENVIRONMENT

PART 2

- Define and implement security governance, and document policies and procedures for CDR data
- Define the boundaries of the CDR data environment
- Implement and maintain an information security capability
- Implement formal controls assessment program (2nd line defence) for Schedule 2 Part 1 & Part 2
- Manage and report security incidents

- Limit the risk of inappropriate or unauthorised access
- Secure network and systems within the CDR data environment
- Securely manage information assets over their lifecycle
- Implement a formal vulnerability management program to identify, track and remediate vulnerabilities in a timely manner
- Limit, prevent, detect, and remove malware
- Implement a formal information security & privacy training and awareness program for all personnel interacting with CDR data

In our experience, ADR applicants focus on Schedule 2 Part 2 but forget about Schedule 2 Part 1 controls which, whilst not difficult, can be time consuming to implement. Our experience completing four CDR information security accreditation assurance reports has enabled us to build up a knowledge bank of guidance and controls in our CDR information security accreditation toolkit from ISO 27001, PCI DSS, SOC 2, CPS 234 and the Australian Government Essential Eight that can be leveraged in your accreditation. Our experience and toolkit are particularly useful for the more difficult CDR requirements around application whitelisting, system hardening and data loss prevention, where compensating controls may be required.

Other Information Security Frameworks

Given CDR will likely require a new system architecture to be built, the scope of any existing assurance reports may not cover the new CDR data environment. The scope needs to be discussed and agreed prior to being used in the accreditation.

Whilst an ISO27001 certification is not sufficient by itself to meet the information security accreditation, we ensure that any previous information security framework investment is leveraged during our assurance process. ISO 27001 is an information security framework, whereas the CDR Schedule 2 controls are based on both information security and data privacy/protection controls, so there are a number of Schedule 2 controls not covered by the ISO 27001 certification. These controls need to be covered by an additional assurance report (ASAE or SOC) to support the ISO 27001 certification.

To leverage an existing ISO27001 certification the organisation also needs to have an additional internal audit report that has been performed by an ISO 27001 Lead Auditor covering all the ISO27001 controls. Even if ISO 27001 certified, where the organisation does not already have an annual internal audit by an ISO 27001 Lead Auditor a standalone ASAE 3150 is likely the most cost effective way to obtain a CDR information security assurance report for accreditation.

Should you wish to leverage your ISO 27001 certification, but require an internal audit, RSM has ISO 27001 Lead Auditors to complete the ISMS internal audit report. It is likely that leveraging the ISO 27001 certification will be more cost effective for the ongoing assurance reports required every two years from accreditation.

If the organisation has an existing SOC 2 (or ASAE 3402) report, the control activities in the report will need to be mapped to the specific CDR requirements to identify where controls need to be covered by an additional assurance report. This could be a SOC 2+CDR assurance report to ensure the differences between the Trust Services Criteria and the CDR Rules are addressed, or a separate limited scope ASAE 3150 report. If obtaining a SOC 2 report for the first time this will be more expensive than a standalone ASAE 3150, but there are additional benefits in then having the SOC 2 report for other purposes. The cost benefit and time required needs to be carefully considered. As a member of the RSM international network, we also prepare reports under the AICPA SOC for Service Organisations: Trust Services Criteria (SOC 2).

Boundaries of the CDR data environment scope

This is where we spend a large amount of our time, and where many organisations need support. **CDR data also includes data derived from 'raw' CDR data**. The CDR data environment involves identifying the people, processes, technology and infrastructure that manages, secures, stores or otherwise interacts with CDR data. The CDR Rules therefore apply to all system components included in or connected to the CDR data environment, including system components indirectly connected, impacting the configuration or security, or providing security services to the CDR data environment.

We describe CDR data as being toxic, contaminating any derived data or connected systems with the CDR Rules. As no guidance on the boundary scope has been provided by the ACCC, we leverage the guidance provided by the PCI Security Standards Council for scoping a cardholder data environment and apply similar themes to the scope of the CDR data environment.

If CDR data has not been de-identified per *The De-Identification Decision-Making Framework* published by the Office of the Information Commissioner and Data61, the Schedule 2 information security controls apply. Our current understanding of this means that tokenisation or using any identifier does not reduce the scope of information security compliance, as it still allows the data to be linked to personally identifiable information.

The CDR data environment includes outsourced service providers (OSPs) provided CDR data. If the data has not been de-identified the OSP needs to comply with and demonstrate that it complies with the Schedule 2 information security controls. This is a carve-in audit approach that will increase the audit costs if the OSP is not accredited. Any other organisations that provide services to the CDR data environment, but cannot access CDR data, are third party providers.

To understand how the CDR data environment boundary impacts your accreditation, discuss it early with someone who knows the CDR Rules and the information security requirements.

ENGAGEMENT APPROACH

To become an ADR, an organisation needs to demonstrate that they have effectively designed security controls and implemented those controls as designed. We refer to the assurance report as a transparency report, providing visibility on control effectiveness. Our experience shows it is very hard to get an unqualified report due to the specific wording of some of the CDR control requirements, but a qualified report does not prevent the organisation from becoming accredited.

Our engagement includes our CDR information security accreditation toolkit, which has been developed and successfully used during the previous CDR information security engagements that we have performed. Our experience shows that initial investment in the Security by Design and Pre-audit / Readiness Assessment phases more than pays for itself in cost savings when completing the CDR information security assurance report, both in ensuring controls are fit for purpose, reduced auditor fees for the final Assurance Audit, and less resources required by you during the audit.

Engagement Phase	
Security by Design / Gap Assessment (optional)	The security by design review assesses whether the proposed design of the information security controls for the CDR data environment will result in compliance with the CDR Rules. This includes assessing whether the scope identified for the CDR data environment is appropriate and will minimise the size of the compliance requirements.
Pre-audit / Readiness (optional)	The readiness assessment approach assesses whether you have identified, implemented and documented the required controls to meet Schedule 2 Part 1 and Part 2. Whilst no detailed testing is performed, the high-level desktop review determines whether the organisation is likely to comply with the requirements to design controls effectively and implement controls as designed.
Assurance Audit and Reporting (required)	• Perform a preliminary review of the control environment • Evaluate the reasonableness of the control objectives • Evaluate the completeness, accuracy and presentation of the System Description of your CDR data environment, against the controls implemented • Evaluate the design of specific controls by assessing the risks that threaten the achievement of the control objectives and evaluating whether the controls described can address those risks and achieve the related objectives • Perform tests of controls to ascertain whether the degree of compliance with controls is sufficient to provide reasonable assurance that the controls have been implemented as designed and achieve their objectives. We will produce a final signed SOC 2 / ASAE 3150 report on the results of our testing.

ENGAGEMENT METHODOLOGY

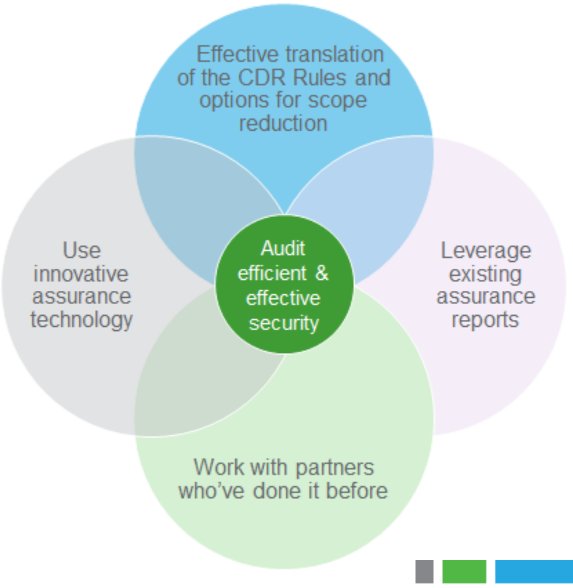
The following table outlines the key phases that would be performed as part of the assurance process:

SCOPE & SYSTEM DESCRIPTION	SCHEDULE 2 PART 1 OF CDR RULES	SCHEDULE 2 PART 2 OF CDR RULES
Determine whether appropriate boundaries for the CDR data environment have been implemented and appropriate system descriptions have been developed Understand the CDR data environment and documentation, such as ▪ Description of the services ▪ System architecture and component diagram ▪ Network architecture ▪ Data flows diagrams ▪ Use of network segmentation, tokenisation, de-identification, anonymisation and pseudonymisation ▪ Third party and outsourced service providers (OSPs)	**Determine the implementation of security governance in relation to CDR data** ▪ Determine the implementation of security governance in relation to CDR data ▪ Determine implementation and maintenance of an information security capability ▪ Determine the effectiveness of the information security controls testing/assessment program ▪ Review the management and reporting of security incidents	**Assess compliance to mandatory information security controls** ▪ Determine your ability to meet all mandatory control requirements outlined in the CDR ▪ Assess any industry standards or frameworks that you have existing accreditation for, to determine whether they address mandatory control requirements

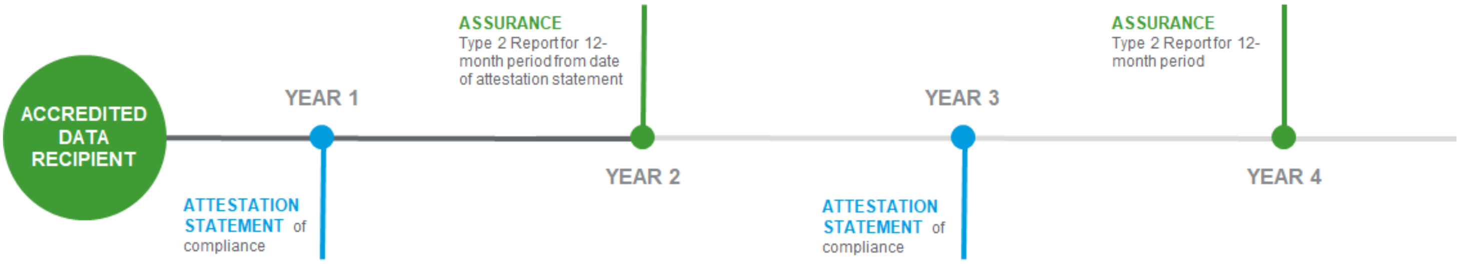
Lessons from previous CDR information security accreditations

- **Work with a partner who has done it before to effectively translate the CDR Rules.** The information security obligation under CDR Rules is broad whilst also containing CDR-specific control expectations. The complexity around the compliance criteria requires a thoughtful discussion to clarify what is expected. Each minimum control requirement contains multiple controls and the mapping to ISO 27001, SOC 2 Trust Services Criteria and PCI DSS contained in the 'CDR - Accreditation controls guidance' workbook, is incomplete. Options for reducing the scope of your CDR data environment include network segmentation and de-identification. The information security accreditation process can be complex and expensive, but it does not need to cost the +$70k quoted by some audit firms.
- **Leverage related assurance programs.** From the onset, determine the extent and limits of existing assurance reports (SOC 1, SOC 2, ASAE 3402, ISAE 3000) and programs (ISO/IEC 27001, PCI DSS) to unlock audit efficiencies whilst meeting CDR criteria. This includes assurance reports from third party providers like AWS, Microsoft Azure and Google Cloud Platform, that need to be mapped into the CDR information security assurance report.
- **Use innovative assurance technology solutions.** Modern technology systems are complex and the security controls to secure them are just as complex. Leveraging security governance software and continuous assurance solutions can reduce the cost of the initial information security accreditation slightly, and significantly reduce the cost of the ongoing assurance report.

To realise these benefits, we recommend a robust initial gap assessment for the proposed design of the CDR data environment, and/or an assessment of the initial implementation in advance of the expected audit.


Effective translation of the CDR Rules and options for scope reduction
Use innovative assurance technology
Audit efficient & effective security
Leverage existing assurance reports
Work with partners who've done it before

What are the ongoing requirements?


ACCREDITED DATA RECIPIENT
YEAR 1
ATTESTATION STATEMENT of compliance
ASSURANCE Type 2 Report for 12-month period from date of attestation statement
YEAR 2
YEAR 3
ATTESTATION STATEMENT of compliance
ASSURANCE Type 2 Report for 12-month period
YEAR 4

Once accredited, the ADR organisation (both non-ADIs and ADIs) will need to provide:

- An attestation statement of compliance to the ACCC at the end of the first year of being accredited and every other year thereafter (i.e., end of 1st year, 3rd year, 5th year, and so on)
- A "Type 2" assurance report covering (a) the 12-month period from the date of submission of the first attestation and (b) every two-year period thereafter (i.e., 2nd year, 4th year, 6th year, and so on), where the period covered is a minimum of 12 months within the relevant two-year period

A "Type II" reasonable assurance report involves a sample to be tested over the period to demonstrate that the ADR has **effectively designed security controls, implemented those controls as designed and that those controls have been operating effectively since accreditation**.

The Type II assurance report is significantly more onerous than the Type I report. Any organisation becoming an ADR needs to understand the ongoing costs to maintain accreditation and how assurance technology can assist in reducing the costs.

Is there more to CDR assurance than just compliance?

Many of the CDR control requirements encompass a scope beyond the CDR data environment, with 15 of the Part 2 controls having an enterprise-wide reach. This is on top of the Part 1 controls which are already, by their nature, enterprise-level controls.

For organisations applying for accreditation, compliance to the CDR information security requirements also provides substantial visibility into the strength of the enterprise information security program. This also enables organisations to better quantify the value that can be obtained on top of CDR compliance and the implementation of controls that align to other information security frameworks like ISO 27001 and CPS 234.

Taking the CDR Rules' ongoing information security reporting obligations into consideration, this focus on value makes a stronger case for integrating information security and assurance programs throughout the organisation.

About RSM

RSM is uniquely placed in Australian professional services as a national partnership with over 150 Partners and Principals and over 1,200 staff operating out of 30 offices throughout Australia. Throughout our history, we have strived to deliver highly personalised services to each client – a principle that has pioneered our success over 95 years ago. We have repeatedly won national awards for the quality of our client service, most recently in March 2020 when we won the **Financial Review Client Choice Award for Best Accounting & Consulting Services firm (Revenue > $200m)**.

RSM in Australia is CREST accredited for penetration testing and our Cyber Security and Privacy Risk team assists organisations in evaluating control requirements against various frameworks, including Consumer Data Right (CDR), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS), Center for Internet Security (CIS), Cloud Security Alliance (CSA), and the Australian Government Information Security Manual and Strategies to Mitigate Cyber Security Incidents.

The CDR information security accreditation process is complex. If you want to discuss your accreditation with one of our experienced team members, please get in touch with:

Darren Booth National Head of Security & Privacy Risk Services
E: darren.booth@rsm.com.au **T:** +613 9286 8158