CONSUMER DATA RIGHT (CDR) INFORMATION SECURITY ACCREDITATION

Obtaining assurance on the security of your CDR data environment

With CDR going live on 1 July 2020, 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.

What security controls are needed?

The CDR Rules require an organisation applying to become an ADR to meet minimum requirements for protecting CDR data from two broad types of risk: (a) misuse, interference, and loss, and (b) unauthorised access, modification, or disclosure. The CDR Rules outline the controls required to manage these risks in Schedule 2 Part 1 (security governance) and Schedule 2 Part 2 (minimum control requirements). The CDR Rules also require an applicant to document their CDR data environment (the people, processes and technology) in a comprehensive system description.

PART 1

- Define and implement security governance in relation to CDR data
- Define the boundaries of the CDR data environment
- Implement and maintain an information security capability
- Implement a formal controls assessment program for Schedule 2 Part 1 and Part 2
- Manage and report security incidents

SYSTEM DESCRIPTION

PART 2

- 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 training and awareness program for all personnel interacting with CDR data

RSM

The more difficult control requirements relate to implementing application whitelisting, data loss prevention and server hardening to accepted industry standards.

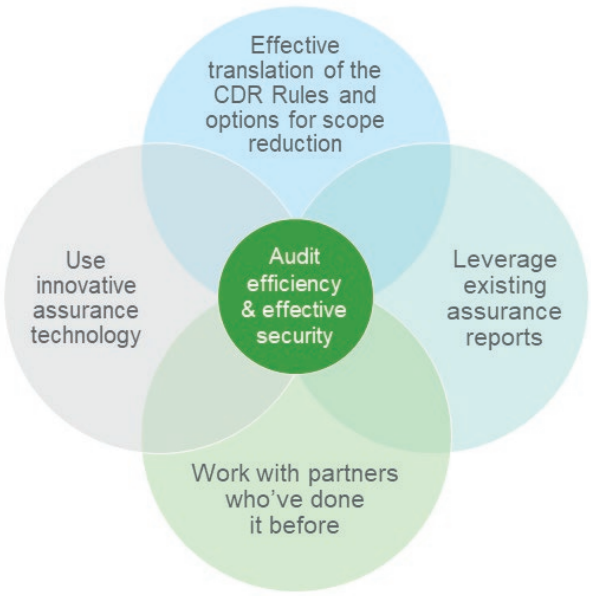
What is required when applying for an accreditation?

To become an ADR, an organisation needs to demonstrate that they have **effectively designed security controls and implemented those controls as designed**. For a non-authorised deposit-taking institution (non-ADI), this requires a "Type I" reasonable assurance report in accordance with the Standard on Assurance Engagements ASAE 3150 — *Assurance Engagements on Controls*, or accepted comparable standards, as identified by the ACCC in the 'CDR - Supplementary accreditation guidelines information security'. A Type I provides assurance on the design and implementation of controls at a date or point in time.

In Australia, these reports can only be prepared by an independent registered auditing firm (CAANZ or CPA) and only a suitably experienced, qualified and independent individual can sign the report as the lead information security assurance practitioner.

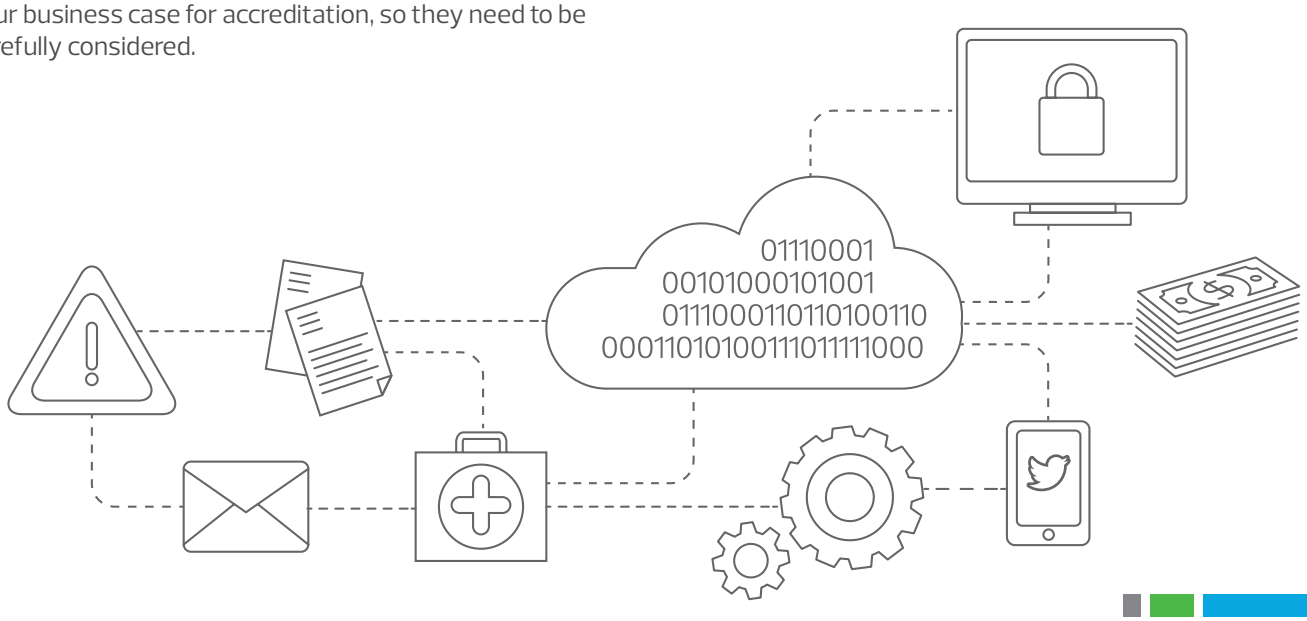
Lessons from previous CDR information security accreditations

- **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, tokenisation, de-identification, anonymisation and pseudonymisation. This process can be complex, expensive and reduce the effectiveness of your business case for accreditation, so they need to be carefully considered.



- Leverage related assurance programs. From the onset, determine the extent and limits of existing assurance reports (SOC 2, ASAE 3402, ISAE 300) 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, or an assessment of the initial implementation in advance of the expected audit.



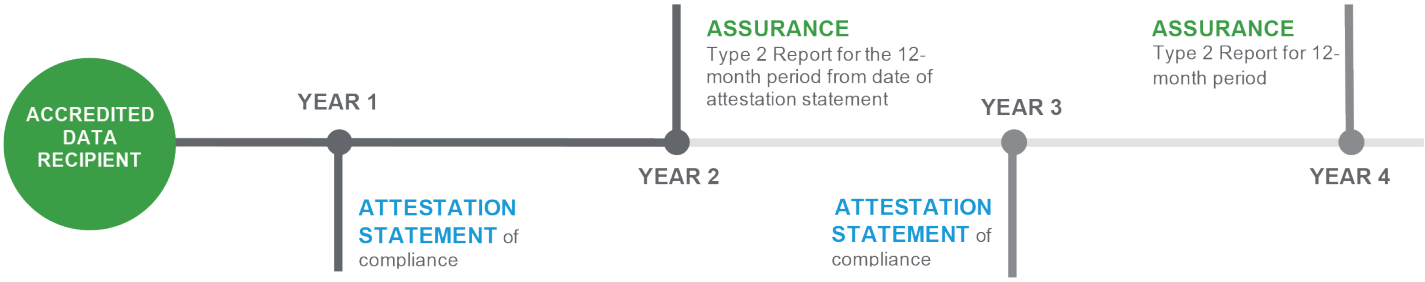
RSM

Time frames

The accreditation applicant can submit their application on the ACCC Consumer Data Right (CDR) Register and Accreditation Application Platform (RAAP) without having the information security assurance report completed. Given that the ACCC say that any ADR application will take approximately three months to approve (providing time to test the consent management system, check insurances and the CDR Policy, and complete the conformance tests), this gives the applicant time to obtain the information security assurance report.

Based on our experience of completing two CDR information security assurance reports, the process will take between 4–12 weeks. A robust initial gap assessment prior to the audit will ensure that this process is at the lower end of this time frame.

What are the ongoing requirements?



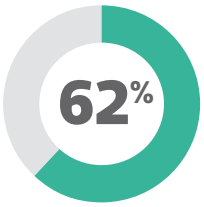
Once accredited, the organisation will need to provide:

- 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?



15 of 24 Part 2 Controls are typically implemented at the enterprise-level

Many of the CDR control requirements encompass a scope beyond the CDR data environment. 15 of the 24 Part 2 controls have 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.

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.

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