Australian Government

Consumer Data Right

Supplementary accreditation guidelines: information security

Version 5
December 2022

Table of Contents

1. Introduction

1.1. Consumer Data Right

The Consumer Data Right (CDR) gives consumers the right to require a service provider that holds their personal data (**data holder**) to share that data with another service provider (**accredited data recipient**).

CDR aims to give consumers more access to and control over their personal data. Being able to share data easily and efficiently between service providers will make it easier for consumers to compare and switch between products and services. This will encourage competition between service providers, leading to more innovative products and services and the potential for lower prices.

CDR is being implemented sector by sector. Banking was the first sector to be brought into CDR. The energy sector is the next.

The CDR scheme operates under Part IVD of the *Competition and Consumer Act 2010* (Cth) (the CCA). The CCA sets out the CDR framework, including the subject matter that the CDR Rules may cover. The Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules) set out the obligations that data holders, accredited data recipients and other participating entities must meet to participate in the scheme.

A glossary of common terms is published on the CDR Support Portal. There are also some definitions specific to these guidelines contained in section 9 of this guide.

1.2. Information security obligation

To participate in the CDR, applicants for CDR accreditation and accredited persons must meet and maintain the information security obligation. The information security obligation protects CDR data from:

- misuse, interference and loss
- unauthorised access, modification or disclosure.

Applicants for accreditation must show they have taken the appropriate steps, as set out in the CDR Rules, to keep CDR data secure by providing evidence that they meet the information security obligation. The evidence must be in the form set out in these guidelines.

Once accredited, accredited persons will be required to provide regular reports and attestation statements to show that they continue to comply with the information security obligation.[1]

1.3. These guidelines

These guidelines are intended to assist applicants for accreditation and accredited persons to meet the CDR Rules information security obligation.2

These guidelines are supplementary to the Accreditation guidelines (which provide general information about the CDR scheme) and the CDR Rules.

---

[1] See the default conditions in CDR Rules, rule 5.9 and Schedule 1, clause 2.1.

[2] CDR Rules, rule 5.12(1)(a).

1.4. More information

Prospective applicants can find answers to frequently asked questions (FAQs) about accreditation and applications for accreditation on the CDR Support Portal. If the applicant has a query that is not addressed in the FAQs, they should email ACCC-CDR@accc.gov.au.

2. Meeting the information security obligation

2.1. Steps to meeting the obligation

The steps to meeting the information security obligation are set out in Schedule 2, Part 1, and Schedule 2, Part 2, of the CDR Rules (see Table 1 below).

At the time the applicant submits their application, they must provide evidence that they have taken these steps and that they meet the information security obligation. The type of evidence applicants need to submit will depend on whether they are applying for accreditation at the **unrestricted level** (see section 3 below) or the **sponsored level** (see section 4 below).

The steps and controls in Schedule 2 are the minimum requirements that an entity must meet to satisfy the information security obligation. An accredited person may choose to put in place security greater than minimum requirements or they may be required to do so, depending on the risks to information security their organisation faces and the level of security that will be appropriate to mitigate those risks.

Table 1: Schedule 2 of the CDR Rules: steps to meeting information security obligation

Application to CDR data environment	
Part 1 **(governance requirements for data security)**	**Part 2** **(minimum information security controls to be maintained)**
Step 1: Define and implement security governance in relation to CDR data	Limit the risk of inappropriate or unauthorised access to CDR data environment.
Step 2: Define the boundaries of the CDR data environment	Secure network and systems within CDR data environment.
Step 3: Have and maintain an information security capability	Securely manage information assets over their lifecycle.
Step 4: Implement a formal controls assessment program	Implement formal vulnerability program to identify, track and remediate vulnerabilities within the CDR data environment.
Step 5: Manage and support security incidents	Limit, prevent, detect, and remove malware. Implement formal security training and awareness program for all personnel interacting with CDR data.

3. Unrestricted accreditation – evidence requirements

When applying for accreditation at the unrestricted level, the applicant will need to provide **one** of the following:

- an **assurance report** prepared to ASAE/ISAE/SOC 1 or 2 standard, from a suitably experienced, qualified and independent auditor (see section 3.1). An assurance report from an independent auditor shows that the applicant has robust security practices in place across their CDR data environment
- **ISO 27001 certification**, together with a **reduced scope assurance report** that covers the controls that are not covered by the ISO 27001 certification (see section 3.2)
- **level 1 PCI DSS compliance**, together with a **reduced scope assurance report** that covers the controls that are not covered by the PCI DSS certification (see section 3.3)
- top tier **ATO Digital Service Provider Operational Security Framework compliance** letter of confirmation, together with a **reduced scope assurance report** that covers the controls that are not covered by the ATO Digital Service Provider Operational Framework (see section 3.4).

3.1. Assurance reports

3.1.1. Standards for preparation

An applicant may provide an assurance report prepared in accordance with any of the following standards:

- the Standard on Assurance Engagements (ASAE) 3150 *Assurance Engagement on Controls* (ASAE 3150) (which falls within the ASAE 3000 series of standards)
- the Assurance Reports on Controls at a Service Organisation (ASAE 3402)
- the International Standard on Assurance Engagements (ISAE) 3000 series
- SOC1/SOC2 reports prepared in accordance with applicable Statement on Standards for Attestation Engagements (SSAE) standards.

The assurance report must be:

- a report on the design and implementation of controls as at a particular date or as at a point in time (often referred to as a Type I report)
- in accordance with one of the accepted standards listed above
- a reasonable assurance engagement
- conducted by suitably experienced, qualified and independent auditors who are capable of issuing reports that comply with one of the accepted standards above
- no more than 3 months old at the time of submission of the accreditation application.

It must:

- include a 'description of the system'. For specific details, see the definition of the boundaries of the accredited person's CDR data environment in Schedule 2, clause 1.4
- address all aspects of the information security capability referred to in Schedule 2, clause 1.5
- show how the accredited person will be able to meet the steps in Schedule 2, Part 1

- include a clear description of control requirements, and controls, referred to in Schedule 2, Part 2
- include a description of the types of tests performed and the results of that testing
- use a 'carve-in approach' for controls if the accredited person is using a third-party service provider for one or more aspects of the information security capability (see section 8.2.1).

If the assurance report notes an exception in either the design or the implementation of a control, the application should include a response from the applicant's management on:

- the steps it will take to remediate these deviations/exceptions
- the expected timeframe to complete those steps
- the reasonable steps it will take in future to prevent these occurrences.

3.1.2. Assurance reports that cover multiple standards

If the applicant needs to satisfy several different requirements, they can submit assurance reports prepared in accordance with multiple standards. For example, where an applicant has data operations both within and outside of Australia, they may provide a combined assurance report prepared according to both ASAE 3150 and the ISAE 3000 series (or SOC1/SOC2 under SSAE standards).

If an applicant submits an assurance report that is prepared in accordance with multiple standards, the assurance report should clearly specify which standards it has been prepared in accordance with.

3.1.3. Using an existing assurance report

The applicant may use an existing assurance report if it is prepared in accordance with one of the accepted standards in section 3.1.1 and meets the requirements in section 3.2.1.

The applicant can use an existing assurance report that partially covers the controls in Schedule 2 under certain conditions:

- the report must be no more than 12 months old (if the report is on the design, implementation and operating effectiveness of controls over a period of time, often referred as a Type II report).
- if the applicant's existing assurance report is more than 3 months old, they may be required to submit a new assurance report in the initial reporting period instead of an attestation statement, as required under Schedule 1 (see section 5).
- if the existing assurance report only partially covers the required controls in Schedule 2, Part 2 the applicant will need to submit an additional assurance report that covers the remaining controls in Schedule 2 and satisfies the requirements of section 3.1.1.
- if the existing assurance report does not fully explain how all required steps in Schedule 2, Part 1, will be taken, the applicant should submit other documentation that shows how they will take these steps.

See the examples of potential scenario and required treatment below.

If the applicant wants to use an existing assurance report, they should discuss it with the ACCC before they submit their application.

Example 1: Not all required controls are covered by existing assurance report

Beta Products Pty Ltd prepares an annual ASAE 3402 assurance report for its clients. The assurance report relates to the CDR data environment but not all the required Schedule 2 controls are included within the report.

Beta Products will need to identify the controls in Schedule 2, Part 2, that are not covered in its existing assurance report. It will need to prepare a separate assurance report for these remaining controls and show how it takes all the steps in Schedule 2, Part 1.

Beta Products' accreditation application should include both reports.

3.2. ISO 27001 certification

ISO 27001 controls alone do not meet the information security obligation in the CDR Rules. To meet the Schedule 2 requirements, you need to meet both:

- the rules on information security governance in Part 1
- the specific controls in Part 2.

The applicant for unrestricted accreditation may use ISO 27001 certification as partial evidence that they satisfy the information security obligation. The applicant will still need to show they meet the requirements of Schedule 2 for the CDR data environment – especially if the ISO 27001 certification covers specific system(s) rather than the organisation as a whole.

As part of its application the applicant will need to submit an additional reduced scope assurance report (see section 3.2.1) and other evidence set out in Table 2. The assurance report will supplement ISO 27001 certification and will be primarily focused on the information security controls in Schedule 2, Part 2. They will also need to attest that they will be able to comply with the requirements of Schedule 2.

If an applicant intends to use an ISO 27001 certification, they should discuss it with the ACCC before they submit their application.

Table 2: Evidence required when using ISO 27001 certification

Evidence	Details
1. **ISO 27001 information security management system (ISMS) certificate**	The certificate should confirm that the applicant is ISO 27001 certified in the defined scope statement. The applicant must submit: • the original certificate • any recertification certificates (if relevant) to show that continuous recertification has been performed.

Evidence	Details
2. ISMS internal audit report	The internal audit report gives the Accreditor reasonable assurance of the applicant's ISMS implementation. The internal audit report should be no more than 12 months old and cover all of the ISO 27001 clauses and Annexure A controls. If the ISMS internal audit scope only tests some controls, the assurance report should cover the controls not tested. The auditor performing the ISMS internal audit must be objective and impartial. The auditor should not be involved in the design, implementation or operation of the ISMS with the requirement of maintaining the ISO 27001 Lead Auditor qualification. If the internal audit is performed by an external organisation, the person(s) performing the audit should maintain the ISO 27001 Lead Auditor qualification. The applicant's independent auditor could complete both the annual ISMS internal audit report and the assurance report if they are external to the organisation and have no operational responsibilities for the applicant's CDR data environment.
3. Statement of Applicability (SoA)	The SoA must set out the current state of the applicant's environment.
4. Assurance report covering the controls that are not covered by the ISO 27001 certification	See the requirements in section 3.2.1.
5. Attestation	The attestation must show that the applicant will be able to comply with the specific requirements of Schedule 2. This information is requested in the application form.

3.2.1. Assurance report for controls not covered by the ISO 27001 certification

The applicant must submit an assurance report that covers the controls not covered by the ISO 27001 certification. The assurance report must meet the requirements set out in section 3.1.1 but with the following modifications:

- ***Schedule 2, Part 1:*** The assurance report is only required to define the boundaries of the CDR data environment as required by clause 1.4 (Step 2) of Schedule 2, Part 1.
- ***Schedule 2, Part 2***: The assurance report must cover the information security controls set out in Table 3 below. These controls are either not included in ISO 27001 or only partially met.
- ***Other information:*** The assurance report should also include any of the other Schedule 2, Part 2 information security controls that are excluded from an applicant's ISO 27001 certification.

Table 3: Controls that require testing when using ISO 27001 certification

#	Information security control	Description
1.	Multi-factor authentication or equivalent control	Multi-factor authentication or equivalent control is required for all access to CDR data.
2.	Restrict administrative privileges	Administrative privileges are granted only on an as needs basis for users to perform their duties and only for the period they are required for. Privileges granted on an ongoing basis are regularly reviewed to confirm their ongoing need.
3.	Role-based access	Role-based access is implemented to limit user access rights to only that necessary for personnel to perform their assigned responsibilities. Role-based access is assigned in accordance with the principle of least necessary privileges and segregation of duties.
4.	Unique IDs	Use of generic, shared and/or default accounts is restricted to those necessary to run a service or a system. Where generic, shared and/or default accounts are used, actions performed using these accounts are monitored and logs are retained.
5.	Password authentication	Strong authentication mechanisms are enforced prior to allowing users to access systems within the CDR data environment, including, but not limited to, general security requirements relating to password complexity, account lockout, password history, and password ageing.
6.	Encryption	Encryption methods are utilised to secure CDR data at rest by encrypting file systems, end-user devices, portable storage media and backup media. Cryptographic keys are securely stored, backed up and retained. Appropriate user authentication controls (consistent with control requirement 1) are in place for access to encryption solutions and cryptographic keys.
7.	Encryption in transit*	Implement robust network security controls to help protect data in transit, including encrypting data in transit and authenticating access to data in accordance with the data standards (if any) and industry best practice; implementing processes to audit data access and use; and implementing processes to verify the identity of communications.

#	Information security control	Description
8.	Firewalls	Firewalls are used to limit traffic from untrusted sources. This could be achieved by implementing a combination of strategies including, but not limited to: a. restricting all access from untrusted networks b. denying all traffic aside from necessary protocols c. restricting access to configuring firewalls, and review configurations on a regular basis.
9.	Server hardening	Processes are in place to harden servers running applications, databases and operating systems in accordance with accepted industry standards.
10.	Data loss prevention	Data loss and leakage prevention mechanisms are implemented to prevent data leaving the CDR data environment, including, but not limited to: a. blocking access to unapproved cloud computing services b. logging and monitoring the recipient, file size and frequency of outbound emails c. email filtering and blocking methods that block emails with CDR data in text and attachments d. blocking data write access to portable storage media.
11.	Web and email content filtering	Solutions are implemented to identify, quarantine and block suspicious content arising from email and the web.
12.	CDR data in non-production environments	CDR data is secured from unauthorised access by masking data, prior to being made available in non-production environments.
13.	Data segregation*	CDR data that is stored or hosted on behalf of an accredited data recipient is segregated from other CDR data to ensure it is accessible only by the accredited data recipient for whom consent was given and remains directly attributable to that accredited data recipient.

* These controls came into effect with the commencement of the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2020 (Accredited Intermediary Rules) on 2 October 2020.

3.3. Level 1 PCI DSS

Level 1 PCI DSS certification alone does not meet the information security obligation in the CDR Rules. To meet the Schedule 2 requirements, you need to meet both:

- the rules on information security governance in Part 1
- the specific controls in Part 2.

The applicant for unrestricted accreditation may use level 1 PCI DSS certification as partial evidence that they satisfy the information security obligation. The applicant will still need

to ensure they meet the requirements of Schedule 2 for their CDR data environment – in particular, where the PCI DSS scope covers specific system(s) rather than the organisation as a whole.

Along with their current level 1 PCI DSS report on compliance, the applicant will need to submit a reduced scope assurance report (see section 3.3.1) and other evidence set out in Table 4 below. The assurance report will supplement the level 1 PCI DSS and will primarily focus on the information security controls in Schedule 2, Part 2. The applicant will also need to attest that they will be able to comply with the requirements of Schedule 2 of the CDR Rules.

If an applicant intends to use level 1 PCI DSS compliance as partial evidence that they satisfy the information security obligation, they should discuss it with the ACCC before they submit their application.

Table 4: Evidence required when using level 1 PCI DSS certification

Evidence	Details
1. **Annual PCI DSS Report on Compliance (ROC)**	The ROC's intention is to provide reasonable assurance of the applicant's PCI DSS implementation to the Accreditor. The ROC should be no more than 12 months old and cover all of the required level 1 controls. If the ROC scope only tests some controls, the assurance report should cover the controls not tested. The auditor performing the ROC must be a Payment Card Industry Qualified Security Advisor and should not be involved in the design, implementation or operation of the ROC. The applicant's independent auditor could complete both the ROC and the assurance report if they are external to the organisation and have no operational responsibilities for the applicant's CDR data environment.
2. **Quarterly Network Scan**	Most recent Quarterly Network Scan as undertaken by a PCI DSS Approved Scan Vendor.
3. **Attestation of Compliance Form**	PCI DSS Attestation of Compliance Form.
4. **Assurance report covering the controls that are not covered by the PCI DSS certification**	As per requirements in section 3.3.1.
5. **Attestation**	Attestation that the applicant will be able to comply with the specific requirements of Schedule 2. This information is requested in the application form.

3.3.1. Assurance report for controls not covered by PCI DSS

The applicant must submit an assurance report that covers the controls not covered by PCI DSS. The report will need to meet the requirements set out in section 3.1.1 but with the following modifications:

- ***Schedule 2, Part 1***: The assurance report is only required to define the boundaries of the CDR data environment as required by clause 1.4 (Step 2) of Schedule 2, Part 1.
- ***Schedule 2, Part 2***: The assurance report is required to cover the information security controls set out in Table 5 below to supplement PCI DSS certification. These controls are either not included in PCI DSS or are only partially met.
- ***Other information***: The assurance report should also include any of the other Schedule 2, Part 2 information security controls excluded from an applicant's ROC.

Table 5: Controls that require testing when using level 1 PCI DSS certification

#	Information security control	Description
1.	Application whitelisting	Download of executables and installation of software on infrastructure and end-user devices (including on bring-your-own-device (BYOD) systems) is restricted to authorised software only.
2.	Data segregation	CDR data that is stored or hosted on behalf of an accredited data recipient is segregated from other CDR data to ensure it is accessible only by the accredited data recipient for whom consent was given and remains directly attributable to that accredited data recipient.
3.	Encryption in transit*	Implement robust network security controls to help protect data in transit, including encrypting data in transit and authenticating access to data in accordance with the data standards (if any) and industry best practice; implementing processes to audit data access and use; and implementing processes to verify the identity of communications.
4.	End-user devices	End-user devices, including BYOD systems, are hardened in accordance with accepted industry standards.
5.	Information asset lifecycle (as it relates to CDR data)	The accredited data recipient must document and implement processes that relate to the management of CDR data over its lifecycle, including an information lifecycle classification and handling policy (which must address the confidentiality and sensitivity of CDR data) and processes relating to CDR data backup, retention and, in accordance with rules 7.12 and 7.13, deletion and de-identification.
6.	CDR data in non-production environments	CDR data is secured from unauthorised access by masking data, prior to being made available in non-production environments.

#	Information security control	Description
7.	Data loss prevention	Data loss and leakage prevention mechanisms are implemented to prevent data leaving the CDR data environment, including but not limited to: a. blocking access to unapproved cloud computing services b. logging and monitoring the recipient, file size and frequency of outbound emails c. email filtering and blocking methods that block emails with CDR data in text and attachments d. blocking data write access to portable storage media.

* These controls came into effect with the commencement of the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2020 (Accredited Intermediary Rules) on 2 October 2020.

3.4. Top tier ATO Digital Service Provider Operational Security Framework

ATO Digital Service Provider Operational Security Framework compliance alone does not meet the information security obligation in the CDR Rules. To meet the Schedule 2 requirements of the CDR Rules, you need to meet both:

- the rules on information security governance in Part 1
- the specific controls in Part 2.

The applicant for unrestricted accreditation may use their top tier ATO Digital Service Provider Operational Security Framework letter of confirmation as partial evidence that they satisfy the information security obligation. The applicant will still need to show they meet the requirements of Schedule 2 for their CDR data environment – especially if the ATO Digital Service Provider Operational Security Framework scope covers specific system(s) rather than the organisation as a whole.

The applicant will need to submit a reduced scope assurance report (see section 3.4.1) and other evidence set out in Table 6. The assurance report will supplement the top tier ATO Digital Service Provider Operational Security Framework and will be primarily focused on the information security controls in Schedule 2, Part 2. The applicant will also need to attest that they will be able to comply with the requirements of Schedule 2.

If an applicant intends to use their top tier ATO Digital Service Provider Operational Security Framework, they should discuss it with the ACCC before they submit their application.

Table 6: Evidence required when using top tier ATO Digital Service Provider Operational Security Framework compliance

Evidence	Details
1. **ATO Digital Service Provider (DSP) Operational Security Framework letter of confirmation**	The most recent written confirmation from the ATO that the applicant is compliant against the ATO DSP Operational Security Framework. The confirmation gives the Accreditor reasonable assurance of the applicant's ATO DSP Operational Security Framework implementation. This confirmation should be issued by the ATO and be no more than 12 months old. It must include the applicant's legal name and recognise it is meeting the requirements for products and services controlled by the DSP with greater than 10,000 taxation or superannuation client records. The scope of the ATO DSP Operational Security Framework and its partial reliance on ISO 27001 certification only covers some of the required controls set out by the CDR Rules. Therefore, an assurance report should be provided to cover the other controls not tested.
2. **Assurance report covering the controls that are not covered by the ATO DSP Operational Security Framework**	As per requirements in section 3.4.1.
3. **Attestation**	Attestation that the applicant will be able to comply with the specific requirements of Schedule 2.

3.4.1. Assurance report for controls not covered by the ATO Digital Service Provider Operational Framework

The applicant must submit an assurance report to cover the controls not covered by the ATO Digital Service Provider Operational Security Framework. The report will need to meet the requirements set out in section 3.1.1 but with the following modifications:

- ***Schedule 2, Part 1***: The assurance report is only required to define the boundaries of the CDR data environment as required by clause 1.4 (Step 2) of Schedule 2, Part 1.
- ***Schedule 2, Part 2***: The assurance report is required to cover the information security controls set out in Table 7 to supplement the ATO Digital Service Provider Operational Security Framework. These controls are either not included in the ATO Digital Service Provider Operational Security Framework or only partially met.
- ***Other information***: The assurance report should also include any of the other Schedule 2, Part 2 information security controls excluded from an applicant's ATO Digital Service Provider Operational Security Framework.

Table 7: Controls that require testing when using top tier ATO Digital Service Provider Operational Security Framework

#	Information security control	Description
1.	Restrict administrative privileges	Administrative privileges are granted only on an as needs basis for users to perform their duties and only for the period they are required for. Privileges granted on an ongoing basis are regularly reviewed to confirm their ongoing need.
2.	Role-based access	Role-based access is implemented to limit user access rights to only that necessary for personnel to perform their assigned responsibilities. Role-based access is assigned in accordance with the principle of least necessary privileges and segregation of duties.
3.	Unique IDs	Use of generic, shared and/or default accounts is restricted to those necessary to run a service or a system. Where generic, shared and/or default accounts are used, actions performed using these accounts are monitored and logs are retained.
4.	Password authentication	Strong authentication mechanisms are enforced prior to allowing users to access systems within the CDR data environment, including, but not limited to, general security requirements relating to password complexity, account lockout, password history, and password ageing.
5.	Firewalls	Firewalls are used to limit traffic from untrusted sources. This could be achieved by implementing a combination of strategies including, but not limited to: a. restricting all access from untrusted networks b. denying all traffic aside from necessary protocols c. restricting access to configuring firewalls, and review configurations on a regular basis.
6.	Server hardening	Processes are in place to harden servers running applications, databases and operating systems in accordance with accepted industry standards.

#	Information security control	Description
7.	Data loss prevention	Data loss and leakage prevention mechanisms are implemented to prevent data leaving the CDR data environment, including, but not limited to: a. blocking access to unapproved cloud computing services b. logging and monitoring the recipient, file size and frequency of outbound emails c. email filtering and blocking methods that block emails with CDR data in text and attachments d. blocking data write access to portable storage media.
8.	Web and email content filtering	Solutions are implemented to identify, quarantine and block suspicious content arising from email and the web.
9.	CDR data in non-production environments	CDR data is secured from unauthorised access by masking data, prior to being made available in non-production environments.
10.	Data segregation*	CDR data that is stored or hosted on behalf of an accredited data recipient is segregated from other CDR data to ensure it is accessible only by the accredited data recipient for whom consent was given and remains directly attributable to that accredited data recipient.

* These controls came into effect with the commencement of the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2020 (Accredited Intermediary Rules) on 2 October 2020.

4. Sponsored accreditation – evidence requirements

Sponsored accreditation applicants are not required to provide an independent third-party assurance report to demonstrate that they satisfy the information security obligation.

Instead, where an applicant has, or will have, an arrangement with an unrestricted accredited person (their sponsor), the applicant may apply for accreditation at the sponsored level and use the **self-assessment and attestation form** to show that they satisfy the information security obligation.

4.1. Self-assessment and attestation form

Applicants for accreditation at the sponsored level will need to provide a completed self-assessment and attestation form covering the information security obligation. The template form can be found on the CDR Resources webpage.

The self-assessment and attestation form shows the applicant how to perform an assessment to confirm they meet their information security obligation for their CDR data environment. The form has 3 sections:

- Description of Systems – applicant and proposed sponsor details (if applicable)
- CDR Data Environment – compliance with the information security governance requirements set out in Schedule 2, Part 1
- CDR Controls Questionnaire – testing of the design and implementation of the CDR information security controls set out in Schedule 2, Part 2.

Applicants must complete all 3 sections to demonstrate they satisfy the information security obligation.

The CDR Controls Questionnaire covers the design and implementation for each control as at a date or point in time. People who are applying for sponsored accreditation should only complete sheet C3A in the CDR Controls Questionnaire. They will complete sheet C3B, which covers operating effectiveness, after accreditation when providing reports to meet ongoing compliance requirements (see section 5).

The self-assessment and attestation form must:

- be signed off by the applicant's Chief Executive Officer; Chief Information Officer; Chief Risk Officer; Chief Information Security Officer; Chief Auditor; or other company officer/manager with a similar level of seniority
- show that the information security controls have been designed and implemented as at a date or as at a point in time
- be no more than 3 months old at the time of submission of the accreditation application.

Applicants may seek assistance from appropriate professionals (including their sponsor/proposed sponsor) when completing the form.

5. Ongoing information security reporting obligations

To comply with the default conditions of accreditation,[3] accredited persons must provide:

- an **attestation statement** at the end of the ***first reporting period*** after being accredited and then every alternate year after that (at the end of Year 1, Year 3, Year 5 and so on)[4]
- **ongoing assurance reports** that cover one-year periods starting from the day after the end of the first reporting period, and every second reporting period thereafter (Year 2, Year 4, Year 6 and so on).

The type of ongoing assurance report depends on the level of accreditation (see section 5.2).

The reporting period for an accredited person will be either a financial year or a calendar year. The Accreditor will determine which period is appropriate, but applicants are able to nominate the preferred period in the accreditation application form.

Ongoing information security reporting obligations do not apply to persons with streamlined accreditation.

5.1. Attestation statement

For both the unrestricted and sponsored level, the attestation statement must:

- be an attestation by management in the form of the 'responsible party's statement', as laid out in ASAE 3150
- include details of changes, if any, to the CDR data environment since the previous assurance report was required to be submitted to the Accreditor.

There is no need for an external party to provide assurance for the attestation statement.

5.2. Ongoing assurance reports

5.2.1. Unrestricted accreditation

An assurance report for maintaining accreditation must comply with the requirements when applying for accreditation set out at section 3.1.1 or section 3.1.2 (depending how the information security obligation is demonstrated). The report must:

- be a report on the design, implementation and operating effectiveness of controls over a period of time (often referred to as a Type II report)
- cover the relevant reporting period, which is a minimum of 12 months.

ISO 27001 certification

Where an accredited person is relying upon ISO 27001 certification as partial evidence to demonstrate that it satisfies the information security obligation, they must also provide to the Accreditor an ISO 27001 annual surveillance audit report, by a Joint Accreditation System of Australia and New Zealand (JAS-ANZ) accredited body, which verifies that the

---

[3] Under Schedule 1 of the CDR Rules.

[4] If an accreditation decision takes effect within 3 months before the end of the reporting period, the first reporting period will end on the last day of the following reporting period.

accredited person's information security management system is still operational and effective. This should be no older than 12 months from the original ISO 27001 certification, ISO 27001 recertification or previous surveillance audit.

Level 1 PCI DSS compliance

Where an accredited person is relying upon level 1 PCI DSS compliance as partial evidence to demonstrate that it satisfies the information security obligation, it must also provide to the Accreditor the most recent:

- Attestation of Compliance Form
- Quarterly Network Scan, undertaken by a PCI DSS Approved Scan Vendor
- Report on Compliance, undertaken by a Payment Card Industry Qualified Security Advisor.

Top tier ATO Digital Service Provider Operational Security Framework compliance

Where an accredited person is relying upon top tier ATO Digital Service Provider Operational Security Framework compliance as partial evidence to demonstrate that it satisfies the information security obligation, it must also provide to the Accreditor the most recent written confirmation from the ATO that it is compliant against the ATO Digital Service Provider Operational Security Framework.

5.2.2. Sponsored accreditation

To meet ongoing information security reporting obligations, sponsored level accredited persons must complete the self-assessment and attestation form, including:

- sheet C1 – Description of Systems
- sheet C2 – CDR Environment
- sheet C3A – CDR Questionnaire on Design and Implementation
- sheet C3B – CDR Questionnaire on Operating Effectiveness. This sets out what is required to demonstrate operating effectiveness of each control. It is an assessment of how the control operates over a period of time.

The self-assessment and attestation form must:

- be signed off by the applicant's Chief Executive Officer; Chief Information Officer; Chief Risk Officer; Chief Information Security Officer; Chief Auditor; or other company officer/manager with a similar level of seniority
- demonstrate the design, implementation *and* operating effectiveness of controls over a period of time
- cover the relevant reporting period – a minimum of 12 months.

5.3. Acceptable auditors

Assurance reports must be completed by suitably experienced, qualified and independent auditors who are capable of issuing reports in compliance with one of the accepted standards.

ASAE 3150 provides a definition for 'lead assurance practitioner'. A 'lead assurance practitioner' is someone who maintains overall responsibility for the assurance

engagement, including quality and alignment with certain standards and codes of ethics.[5] The lead assurance practitioner is the person responsible for signing and issuing the assurance report. The lead assurance practitioner should maintain adequate experience and qualifications to meet the required standard of quality in assurance reporting.

Details for acceptable auditors for other accepted standards are set out in section 3.1.

[5] See ASAE 3150, which contains this concept.

6. Steps to secure CDR data

Schedule 2, Part 1, sets out the steps for the information security of CDR data.

Information security of CDR data refers to an accredited person's ability to manage the security of its CDR data environment in practice. The accredited person must manage its CDR data by implementing and operating an information security governance framework and underlying processes and controls that enable them to meet the mandatory steps under Schedule 2, Part 1.

This section summarises what is required for these steps and provides guidance on how accredited persons may implement them.

6.1. Step 1: Define and implement security governance for CDR data

6.1.1. Information security governance framework

Under the CDR Rules, an accredited person must establish a formal information security governance framework for managing information security risks relating to its CDR data. This includes setting out the policies, procedures, roles and responsibilities needed to oversee and manage CDR data.

An accredited person may use their existing information security governance structure where this will cover their CDR data environment. They may use existing frameworks, requirements and models in developing their information security governance framework and defining security areas (for example, ISO 27001, NIST, CSF, PCI DSS, and CPS 234). Security areas are commonly employed in maintaining the security of data (for example, access security and network security).

6.1.2. Roles and responsibilities

An accredited person must define roles and responsibilities for managing information security of CDR data. This will include the specific responsibilities of senior management, who typically have ultimate responsibility for the management of information security. Where an organisation's CDR data environment is large or complex, its security governance structures (for example, committees and forums) should include membership from across key business areas.

6.1.3. Information security policy

An accredited person must have and maintain an information security policy. The information security policy must set out:

- the accredited person's information security risk posture – that is, the exposure and potential for harm to an entity's information assets from security threats and how the entity plans to address these
- the exposure and potential for harm from security threats
- how the information security practices and procedures, and its information security controls, are designed, implemented and operated to mitigate those risks.

The information security policy should be enforceable,[6] and compliance with the policy must be monitored. The information security policy should document the various security areas that the accredited person manages.

6.1.4. Review of appropriateness

An accredited person must ensure its information security governance framework, including the definition and assignment of roles and responsibilities, remains up to date and fit for purpose. Updates must be completed at least every 12 months. They will be needed sooner if there are:

- material changes to its CDR data environment, or
- material changes to both the extent and nature of threats to its CDR data environment.

A 'material change' is one that significantly changes the scope of the CDR data environment – for example:

- the introduction of a new system
- the migration of data onto new infrastructure
- the introduction of a new third-party service provider
- a change to the terms and conditions of the services provided by an existing third-party service provider.

6.2. Step 2: Define the boundaries of the CDR data environment

As part of the assurance report, the applicant or accredited person must document a 'description of the system' in accordance with international auditing standards. In other words, the accredited person must assess and define the boundaries of the CDR data environment. This will include defining the people, processes, technology and controls in place to manage CDR data. The CDR data environment may include infrastructure owned by, and management provided by, a third-party service provider.

ASAE 3150 clearly defines what a 'description of system' means;[7] what elements it should cover;[8] and what a suitably experienced, qualified and independent auditor should assess to determine if the description is complete and accurate in all respects.[9] ASAE 3150 also includes an example of what a description of the system looks like.[10]

The CDR data environment can be documented using a detailed data flow diagram or through a written statement. A description of the system that has been reviewed by a suitably experienced, qualified and independent auditor will be an appropriate way to document the CDR data environment.

Documentation must be reviewed and updated as soon as practicable after the accredited person becomes aware of material changes to the extent and nature of threats to its CDR data environment or, where no such changes occur, on an annual basis.

---

[6] ' Enforceable' here means both internally and externally enforceable and includes provisions to deal with breaches to the policy. 'Internally' means the policy is enforceable against an accredited person's employees and internal departments. 'Externally' means the policy, or parts thereof, is enforceable against the accredited person's third parties and vendors through mechanisms such as contractual requirements and ongoing third-party monitoring processes.

[7] ASAE 3150, section 17(J).

[8] ASAE 3150, section 51.

[9] Paragraph A86 and multiple other references throughout ASAE 3150.

[10] ASAE 3150, Appendix 7, 'Example Responsible Party's Statement on Controls and System Description'.

In general, it is good practice for an accredited person to limit the size of its CDR data environment to the extent practicable. This may be achieved by:

- segregating the environment from other systems
- minimising the number of people interacting with CDR data
- limiting the number of systems hosting, processing or accessing CDR data
- minimising the use of third-party service providers interacting with CDR data.

By limiting the size of the CDR data environment, the attack surface is decreased and, as a result, it is likely that the security of CDR data will increase.

6.3. Step 3: Implement and maintain an information security capability

An accredited person must have and maintain an information security capability that:

- is appropriate and adapted to respond to risks to information, having regard to the factors in clause 1.5(1)(b) (Step 3) of Schedule 2, Part 1
- complies with the controls specified in Schedule 2, Part 2, with regard to systems within the CDR data environment.

An accredited person's information security capability includes its ability to manage the security of its CDR data environment by:

- implementing and operating sufficiently designed processes and controls
- using appropriate technology, equipment and infrastructure
- involving suitably experienced persons.

It may include steps or processes undertaken by third-party service providers.

An accredited person must review and adjust its information security capability in response to material changes to both the extent and nature of threats to its CDR data environment. These changes could result from the development of new applications, migration to new infrastructure, or engagement of a new third-party service provider. The accredited person must conduct this review annually, even if no material changes have occurred.

6.4. Step 4: Implement a formal controls assessment program

An accredited person must implement a testing program to review and assess the effectiveness of its information security capability. The factors they must consider for the testing program are set out in clause 1.5(1)(b) (Step 3) of Schedule 2, Part 1.

For example, the accredited person must test the effectiveness of information security controls. They may use a testing process that includes independent audits and/or control self-assessments, in which the assessor:

- identifies and assigns the associated control owner
- assesses the effectiveness of those controls, noting any deviations from expected operation
- identifies steps for improving controls

- logs and tracks the deviations and remediation measures and reports them to senior management.[11]

This testing must be carried out at an appropriate frequency and be appropriately extensive. It must take into account the matters in clause 1.6(1)(b) (Step 4) of Schedule 2, Part 1.

An accredited person must review their testing program if there are material changes to the extent and nature of threats to its CDR data environment or the boundaries of its CDR data environment. However, they must carry out the testing at least annually regardless of whether there are any changes.

The form of the test and assessment will determine the level of independence and professional skills that the tester should have. For example, audits should be performed in line with generally accepted practices for independence and skill. Control self-assessments should be performed by persons with suitable knowledge and understanding of the controls and their expected operations (technical expertise) but independent from the day-to-day performance and administration of the control to promote impartiality. Well-known standards, such as Center for Internet Security Critical Security Controls (CIS CSC) and National Institute of Standards and Technology (NIST) SP800-53, provide detailed guidance on the performance of security controls for information systems. An accredited person may use this guidance when developing a testing program.

6.5. Step 5: Manage and report security incidents

6.5.1. General guidance

An accredited person must have formal plans, procedures and practices in place for responding to a security incident. For example, they must have methods for:

- identifying, classifying and rating the incident
- managing the incident through its lifecycle
- following appropriate escalation channels
- reporting to relevant authorities where necessary
- conducting post-incident review.

To maintain and ensure the efficacy of these procedures and achieve a base level of preparedness, an accredited person must perform periodic testing – for example, by doing tabletop exercises or interactive simulations.

This testing should occur at least annually. It should occur more regularly where there have been material changes to the accredited person's CDR data environment that would lead to changes in the plans, procedures or practices of responding to a security incident.

6.5.2. CDR data security response plans

An accredited person must have procedures and practices in place to detect, record and respond to information security incidents in a timely manner.

The accredited person must create and maintain data security response plans that detail their response to information security incidents that they consider could plausibly occur.

[11] CDR Rules, Schedule 2, Part 1, rule 1.6(3).

For their CDR data security response plans, accredited persons should refer to the Office of the Australian Information Commissioner (OAIC) guidance on the reporting of notifiable data breaches. Accredited persons should also report all security incidents, even minor ones, to the Australian Cyber Security Centre (ACSC).

Security incidents may include, but are not limited to:

- system compromises that directly/indirectly impact the CDR data environment
- receipt of malicious emails
- unauthorised attempts to gain access to the CDR data environment
- unauthorised scanning of systems and networks
- denial of services
- data exposure, theft or leaks.

Reports to the ACSC can be made through the ACSC's online cybercrime and incident reporting tool.

7. Information security controls

The accredited person must implement certain mandatory controls, set out in Schedule 2, Part 2, across their CDR data environment.

7.1. Control requirements and controls

To be accredited, an applicant will need to demonstrate that, if accredited, it would be able to meet all control requirements. The evidence required to demonstrate this is set out in section 3.

An applicant can still be accredited (potentially with conditions) if there are deviations in the effectiveness of individual controls, as long as the Accreditor believes that the applicant would, if accredited, be able to meet all control requirements.

Accredited persons must maintain information related to controls (such as logs of critical events) for a period of 6 years (CDR rules, rule 9.3(2)(l)). This information should be stored for at least 90 days in a readily accessible storage media. Information older than 90 days can be archived to less expensive storage media, as long as the information is still accessible if it is required in future (for example, for incidents or investigations).

7.2. Controls guidance

The *CDR Information Security Controls Guidance* (Controls Guidance) sets out how a suitably experienced, qualified and independent auditor may perform an audit of the information security obligation for the CDR data environment.

The Controls Guidance includes mapping of controls from Schedule 2, Part 2, against corresponding controls from industry-accepted standards and frameworks (namely, ISO 27001, PCI DSS, and the Trust Service Principles). It also contains a template which is a sample of how an auditor may capture information and details of audit fieldwork and testing.

The Controls Guidance does not give a prescriptive methodology that must be used when performing an assessment. Also, it does not reflect the level of detail and complete set of elements that an auditor may require to complete their work and obtain assurance under the accepted standards. The auditor will need to use their own professional judgement to decide whether this template is fit for purpose given the specific requirements of the entity they are auditing.

Accredited persons may also wish to use the Controls Guidance to conduct their own internal assessment of their ongoing compliance with the information security obligation. Similarly, applicants for or persons with the sponsored level of accreditation may wish to refer to the Controls Guidance when completing the self-assessment and attestation form (see section 4.1).

7.3. Industry standards

When assessing required controls, the auditor may be able to recognise the accredited person's certification against industry standards or frameworks where they adequately address relevant parts of the requirements. They may also recognise third-party service providers' certification against industry standards (for example, cloud providers).

‘Accepted industry standards’ are a set of criteria for the standard processes and operations in that specific field. These are the generally accepted requirements followed by the members of an industry. They are not fixed and are expected to evolve as circumstances change.

The Controls Guidance, under the controls mapping tab, provides guidance on how each of the controls defined under the CDR Rules for information security relates to common frameworks and standards for information security.

8. Guidance on third-party service providers

8.1. General guidance

An accredited person may use a third-party service provider to assist in providing goods or services to a CDR consumer. An accredited person at the unrestricted level may also engage an outsourced service provider to collect CDR data from a data holder.

An accredited person may choose to use third-party service providers such as:

- data centres and backup providers
- SaaS (Software as a service) providers
- PaaS (Platform as a service) providers
- cloud-based service providers.

The CDR Rules do not prohibit an accredited person from storing CDR data on infrastructure owned by third parties. However, the accredited person must still meet all of the obligations and requirements set out in legislation and the CDR Rules.

An accredited person may also be liable for the use or disclosure of CDR data by outsourced service providers or certain other recipients of that data.[12] Therefore, accredited persons should consider carefully the terms on which they disclose any CDR data to outsourced service providers. The CDR Rules set out various requirements for a CDR outsourcing arrangement.[13]

8.2. Application of third-party service providers to Schedule 2

8.2.1. Using a 'carve-in' approach to assurance reporting

Where controls requirements under Schedule 2 are performed by a third-party service provider, the auditor will be required to perform the audit procedures and issue an assurance report using the 'carve-in' approach.[14]

Under the carve-in approach, the auditor may extend the audit fieldwork to include controls at the third-party service provider that relate to the management of the accredited person's CDR data environment.

An alternative carve-in method is to use existing third-party assurance reports provided by the third-party service provider. This alternative should only be used where the controls within such reports relate to the management of the accredited person's CDR data environment.

8.2.2. Assessment of controls performed by third-party service provider

If a control defined in Schedule 2, Part 2 is or will be performed by a third-party service provider, an accredited person must assess this as part of their formal controls assessment program.

---

12 CDR Rules, rule 7.6(2).

13 See CDR Rules, rule 1.10.

14 Where an applicant or accredited person is relying on ISO 27001 certification to satisfy their information security obligation, the carve-in approach must be taken for those controls covered by the reduced scope assurance report.

This includes assessments before on-boarding a new third-party service provider (during the due diligence phase), as well as periodic assessments in line with the inherent risk of the third-party service provider in regard to the security of the accredited person's CDR data environment.

The accredited person may use a combination of security questionnaires, formal control assessments, site visits or third-party assurance reports (for example, SOC2, ASAE 3402 or other comparable standards) in performing these assessments.

An accredited person relying on information security control testing that the third-party service provider has provided – for example, general use third-party assurance reports – must assess whether the extent and frequency of controls testing directly relate to the management of the accredited person's CDR data.

The accredited person must also ensure that the controls tested align to the control requirements defined in Schedule 2, Part 2 where the performance of a control is outsourced.

8.2.3. Security incidents at a third-party service provider

Where a security incident related to the CDR data environment occurs at a third-party service provider – for example, because of deficiencies in controls operated by the provider – the accredited person is accountable for this breach. Therefore, the accredited person will be responsible for ensuring the breach is reported in compliance with clause 1.7 (Step 5) of Schedule 2, Part 1 and other relevant legislation, including the *Privacy Act 1988* (Cth).

To ensure they comply with the CDR Rules, the accredited person should include clauses for mandatory reporting of any security incident occurring to the CDR data environment within the service contract.

9. Glossary

Shortened form	Extended form
accredited person	a person who has satisfied the Data Recipient Accreditor that it meets the criteria for accreditation specified in the CDR Rules and has been accredited by the Accreditor
ACSC	Australian Cyber Security Centre
ACCC	Australian Competition and Consumer Commission
ATO	Australian Taxation Office
the Act	*Competition and Consumer Act 2010 (Cth)*
AUASB	Australian Auditing and Standards Board
ASAE	Australian Standard on Assurance Engagements
ASAE 3150	Australian Standard on Assurance Engagements (ASAE) 3150 *Assurance Engagement on Controls* standard
ASAE 3402	Australian Standard on Assurance Engagements (ASAE) 3402 *Assurance Reports on Controls at a Service Organisation*
Controls Guidance	the CDR Information Security Controls Guidance accompanying these Guidelines
CDR	Consumer Data Right
CDR data	specific information for the relevant designated sector. See section 56AI(1) of the Act.
CDR data environment	the information technology systems used for, and processes that relate to, the management of CDR data
CDR Rules	Competition and Consumer (Consumer Data Right) Rules 2020
CIS CSC	Center for Internet Security Critical Security Controls
CPS 234	Australian Prudential Regulation Authority Cross-industry Prudential Standard 234 – Information Security
data holder	a holder of CDR data

Shortened form	Extended form
description of the system	a definition of the people, processes, technology and controls in place to manage CDR data prepared in accordance with international auditing standards
information security capability	the accredited person's ability to manage the security of their CDR data environment in practice through the implementation and operation of processes, including allocating adequate budget and resources, and providing for management oversight
information security governance framework	the policies, processes, roles and responsibilities required to facilitate the oversight and management of information security
information security obligation	the requirement to take the steps outlined in Schedule 2 of the CDR Rules as detailed in rule 5.12(1)(a) of the CDR Rules
information security policy	a formal document that defines the mandatory requirements for managing information security at the organisation
ISAE	International Standard on Assurance Engagements
ISO 27001	International Organisation for Standardisation 27001 – Information Security Management Systems
NIST CSF	National Institute for Standards and Technology – Cyber Security Framework
NIST SP800-53	National Institute for Standards and Technology – Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations
OAIC	Office of the Australian Information Commissioner
outsourced service provider	a provider: • who collects CDR data from a CDR participant on behalf of a principal under a CDR outsourcing arrangement, and/or • to whom a principal discloses CDR data under a CDR outsourcing arrangement for the purpose of the provider providing goods or services to the principal See rule 1.10 of the CDR Rules
PaaS	platform as a service
PCI DSS	Payment Card Industry Data Security Standard
ROC	PCI DSS annual Report on Compliance

Shortened form	Extended form
SaaS	software as a service
senior management	an accredited person's directors, and any person who is an associated person of an accredited person that is a body corporate
SOC	System and Organization Control
SSAE	Statement on Standards for Attestation Engagements
third-party service provider	a provider engaged by the applicant to perform tasks, handle operations or provide services which manage, secure, store or otherwise interact with CDR data. This also includes outsourced service providers (see above definition).