Australian Government

Consumer Data Right

Supplementary Accreditation Guidelines

Information Security

Version 3.0

April 2021

Table of Contents

1. Introduction

1.1. Overview

Under Part IVD of the *Competition and Consumer Act 2010 (Cth)* (the Act), the Consumer Data Right (CDR) regime enables consumers to require data holders to share their data with accredited persons.

The Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules) set out how the CDR is to operate[1] including the criteria that the Data Recipient Accreditor (Accreditor) will apply when considering an application for accreditation. Once accredited, an accredited person of CDR data will have ongoing obligations consistent with the criteria.[2]

One obligation for accreditation is the information security obligation.[3] This requires an accredited person to take the steps outlined in Schedule 2 of the CDR Rules. The purpose of this obligation is to protect CDR data from:

(i) misuse, interference and loss

(ii) unauthorised access, modification or disclosure.

These Guidelines aim to provide information and guidance to accreditation applicants and accredited persons to assist them in meeting the information security obligation, and to demonstrate that they satisfy the information security obligation for the purposes of accreditation. These Guidelines are supplementary to the *CDR Accreditation Guidelines* and the CDR Rules.

Answers to frequently asked questions (FAQs) about accreditation and applications for accreditation can be found on the CDR Support Portal. If a query is not addressed in the FAQs, prospective applicants should submit an enquiry on the CDR Support Portal.

1.2. Information security obligation

An accredited person must take the steps outlined at Schedule 2 of the CDR Rules to satisfy the information security obligation.

These steps and controls are the minimum requirements that an entity must meet in order to satisfy the information security criterion to hold accreditation. An accredited person may choose to put in place protection that exceeds these minimum requirements, or may be required to do so to ensure their protection is appropriate and adapted to respond to risks to information security.

The coverage of each Part of Schedule 2 is as follows:

- Part 1: contains provisions about the overarching governance requirements for the security of CDR data.
- Part 2: specifies the minimum information security controls to be maintained by an accredited person as part of its information security capability.

---

1 The Act sets out the CDR framework including the subject matter that the CDR Rules may cover.

2 CDR Rules, rule 5.12.

3 CDR Rules, rule 5.12(1)(a).

Figure 1: Coverage of Schedule 2

Application to CDR Data Environment	
Part 1 (governance)	**Part 2 (control requirements)**
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.

When applying for accreditation, an accreditation applicant will be required to provide evidence in the form set out in these Guidelines to demonstrate that it satisfies the information security obligation. Accredited persons will be required to demonstrate their ongoing compliance with Schedule 2 of the CDR Rules by providing regular assurance reports and attestation statements.[4]

2. Applying for accreditation

Summary

Unrestricted level

When applying for accreditation the following evidence will need to be provided to satisfy the information security obligation. Either:

- an assurance report prepared to ASAE/ISAE/SOC 1 or 2 standard
- ISO 27001 certification, together with a reduced scope assurance report covering the controls that are not covered by the ISO 27001 certification
- level 1 PCI DSS certification, together with a reduced scope assurance report covering the controls that are not covered by the PCI DSS certification
- top tier ATO Digital Service Provider Operational Framework compliance, together with a reduced scope assurance report covering the controls that are not covered by the ATO Digital Service Provider Operational Framework

This evidence must be provided at the time of submitting your accreditation application. Further details of the evidence requirements are set out below.

[4] See the default conditions in rule 5.9 and Schedule 1 sub-clause 2.1 of the CDR Rules.

2.1. Unrestricted level

To be accredited at the unrestricted level, evidence that an accreditation applicant will be able to comply with the information security obligation is required in the form of an assurance report from a suitably experienced, qualified and independent auditor.

We have also sought to leverage existing standards to satisfy the information security obligation where appropriate. Therefore, as an alternative, where an applicant is either ISO 27001 or level 1 PCI DSS certified, or top tier ATO Digital Service Provider Operational Framework compliant they will be able to rely on this evidence together with an assurance report covering the controls that are not covered by their ATO Digital Service Provider Operational Framework letter of confirmation, ISO 27001 or PCI DSS certification, and other evidence addressed in these Guidelines to satisfy the information security obligation.

The independent audit requirement seeks to provide the Accreditor with a level of assurance that the applicant has robust security practices in place across their CDR data environment.

2.1.1. Assurance report

This assurance report must be:

- a report on the design and implementation of controls as at a 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 below
- a reasonable assurance engagement
- conducted by suitably experienced, qualified and independent auditors who are capable of issuing reports in compliance with one of the accepted standards below
- no more than 3 months old at the time of submission of the accreditation application.

The assurance report must:

- include a 'description of the system' which should relate to the definition of the boundaries of the accredited person's CDR data environment as referred to in clause 1.4 of Schedule 2 of the CDR Rules
- address all aspects of the information security capability referred to in clause 1.5 of Schedule 2 of the CDR Rules
- address how the accredited person will be able to meet the steps required by Part 1 of Schedule 2 of the CDR Rules
- include a clear description of control requirements, and controls, referred to in Part 2 of Schedule 2 of the CDR Rules
- include a description of the types of tests performed, and results of that testing
- in circumstances where one or more aspects of the information security capability are, or will be, undertaken by an outsourced service provider use a 'carve-in approach' (see section 6.2.1 of these Guidelines) in respect to such controls.

Where an exception is noted in either the design or implementation of a control, in addition to the report, the applicant should ensure that it includes, in its application, a response from the applicant's management on the steps it intends to take to remediate

these deviations/exceptions and the expected timeframe to complete such steps. It is expected that these responses will include what reasonable steps will be taken to prevent such occurrences in future.

2.1.2. Accepted standards

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)[5] (which falls within the ASAE 3000 series of standards)
- ASAE 3402 Assurance Reports on Controls at a Service Organisation
- 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.

Assurance reports may be issued to satisfy multiple standards in order to satisfy different requirements. 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 SOC 1/SOC 2 under SSAE standards). If an applicant is relying on an assurance report prepared to satisfy multiple standards for the purposes of the CDR, the assurance report should clearly specify which standards it has been prepared in accordance with.

2.1.3. Utilising existing assurance reports

When applying for accreditation, an applicant may seek to use an existing assurance report prepared in accordance with one of the accepted standards listed in section 2.1.2 of these Guidelines. The existing assurance report must meet the requirements outlined in section 2.1.1. However, the Accreditor will generally accept, as part of an accreditation application, an existing assurance report that contains partial coverage over the required controls in Schedule 2 subject to the treatments below:

- is no more than 12 months old (if current report on the design, implementation and operating effectiveness of controls over a period of time)
- if the existing assurance report contains partial coverage over the required controls in Schedule 2, the remaining controls in Schedule 2 of the CDR Rules will need to be assessed in a separate assurance report that satisfies the requirements of section 2.1.1 of these Guidelines. Both assurance reports must be submitted when applying for accreditation
- if the existing assurance report does not fully address how the accredited person takes all required steps in Part 1 of Schedule 2 of the CDR Rules when applying for accreditation, the applicant should submit other documentation that addresses how the accredited person takes these steps.

Examples of potential scenarios and required treatment are provided below.

Where an applicant seeks to rely on an existing assurance report older than three months, the Accreditor may consider a condition that requires the submission of a new assurance report in the initial reporting period instead of an attestation statement, as required under Schedule 1 of the CDR Rules.

---

[5] The ASAE 3150 reporting standard can be found here.

We encourage applicants to discuss the use of an existing assurance report with us prior to submission of their accreditation application.

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

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

Company XYZ will need to identify those controls specified in Part 2 of Schedule 2 of the CDR Rules that are not covered in its existing assurance report and prepare a separate assurance report for these remaining controls, and to address how Company XYZ takes all the steps required by Part 1 of Schedule 2. Company XYZ's accreditation application should include both reports.

2.1.4. Utilising ISO 27001 certification

Where an applicant has an ISO 27001 certification, the applicant may seek to rely on this certification as partial evidence to demonstrate that it satisfies the information security obligation. The Accreditor will accept, as part of an accreditation application, a current ISO 27001 certification together with a reduced scope assurance report and other evidence as specified below. The assurance report is to supplement ISO 27001 certification. It is primarily focused on the information security controls in Part 2 Schedule 2 of the CDR Rules, as ISO 27001 controls alone do not meet the obligations set out by the CDR Rules.

When applying for accreditation and seeking to rely on ISO 27001 certification the applicant must submit:

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. This should include the original certificate, as well as any recertification certificates (if relevant) to validate that continuous re-certification has been performed.
2. **ISMS internal audit report**	The internal audit report intention is to provide reasonable assurance of the applicant's ISMS implementation to the Accreditor. 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 independent auditor of an applicant could complete both the annual ISMS internal audit report and the assurance report if they are external to the organisation with no operational responsibilities for the applicant's CDR data environment.
3. **Statement of Applicability (SoA)**	Document containing the current state of the applicant's environment.

Evidence	Details
4. Assurance report covering the controls that are not covered by the ISO 27001 certification	As per requirements below.
5. Attestation	Attestation that the applicant will be able to comply with the specific requirements of Schedule 2. Until the accreditation form is updated in the CDR Participant Portal to reflect this, the attestation can take the form of a signed statement from a duly authorised representative from the applicant.

While an applicant may rely on the fact they are ISO 27001 certified as partial evidence of their information security capabilities for the purpose of accreditation at the unrestricted level, the applicant will still need to ensure they meet the requirements of Schedule 2 of the CDR Rules for their CDR data environment – in particular, if the ISO 27001 certification scope covers specific system/s rather than the organisation as a whole. To this end, an attestation that the applicant will be able to comply with the requirements of Schedule 2 of the CDR Rules will also be required in support of an applicant's accreditation application. The requirement to meet Schedule 2 includes meeting both the rules that are focused on information security governance in Part 1, as well as the specific controls at Part 2 of the Schedule.

Assurance report covering the controls that are not covered by the ISO 27001 certification

The assurance report covering the controls that are not covered by the ISO 27001 certification will need to meet the requirements for an assurance report when applying for accreditation as set out in section 2.1.1 of these Guidelines, but with the following modifications:

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

Table 1: Controls requiring testing

#	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.

#	Information security control	Description
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.
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

#	Information security control	Description
		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.

We encourage applicants to discuss reliance on an ISO 27001 certification with us prior to submission of their accreditation application.

2.1.5. Utilising level 1 PCI DSS certification

Where an applicant has a level 1 PCI DSS certification, the applicant may seek to rely on this certification as partial evidence to demonstrate that it satisfies the information security obligation. The Accreditor will accept, as part of an accreditation application, a current level 1 PCI DSS certification together with a reduced scope assurance report and other evidence as specified below. The assurance report is to supplement PCI DSS certification. It is primarily focused on the information security controls in Part 2 Schedule 2 of the CDR Rules, as PCI DSS controls alone do not meet the obligations set out by the CDR Rules.

When applying for accreditation and seeking to rely on level 1 PCI DSS certification the applicant must submit:

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 independent auditor of an applicant could complete both the ROC and the assurance report if they are external to the organisation with no operational responsibilities for the applicant's CDR data environment.

Evidence	Details
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 below.
5. Attestation	Attestation that the applicant will be able to comply with the specific requirements of Schedule 2. Until the accreditation form is updated in the CDR Participant Portal (Participant Portal) to reflect this, the attestation can take the form of a signed statement from a duly authorised representative from the applicant.

While an applicant may rely on the fact they are level 1 PCI DSS certified as partial evidence of their information security capabilities for the purpose of accreditation at the unrestricted level, the applicant will still need to ensure they meet the requirements of Schedule 2 of the CDR Rules for their CDR data environment – in particular, if the PCI DSS certification scope covers specific system/s rather than the organisation as a whole. To this end, an attestation that the applicant will be able to comply with the requirements of Schedule 2 of the CDR Rules will also be required in support of an applicant's accreditation application. The requirement to meet Schedule 2 includes meeting both the rules that are focused on information security governance in Part 1, as well as the specific controls at Part 2 of the Schedule.

Assurance report covering the controls that are not covered by the PCI DSS certification

The assurance report covering the controls that are not covered by the PCI DSS certification will need to meet the requirements for an assurance report when applying for accreditation as set out in section 2.1.1 of these Guidelines, but with the following modifications:

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

Table 2: Controls requiring testing

#	Information security control	Description
1.	Application whitelisting	Download of executables and installation of software on infrastructure and end-user devices (including on BYOD devices) 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 bring-your-own-device (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.
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.

We encourage applicants to discuss reliance on a level 1 PCI DSS certification with us prior to submission of their accreditation application.

2.1.6. Utilising top tier ATO Digital Service Provider Operational Framework

Where an applicant is compliant to the top tier ATO Digital Service Provider Operational Framework, the applicant may seek to rely on this compliance as partial evidence to demonstrate that it satisfies the information security obligation. The Accreditor will accept, as part of an accreditation application, a current top tier ATO Digital Service Provider Operational Framework letter of confirmation together with a reduced scope assurance report and other evidence as specified below. The assurance report is to supplement the top tier ATO Digital Service Provider Operational Framework. It is primarily focused on the information security controls in Part 2 Schedule 2 of the CDR Rules, as the ATO Digital Service Provider Operational Framework controls alone do not meet the obligations set out by the CDR Rules.

When applying for accreditation and seeking to rely on top tier ATO Digital Service Provider Operational Framework the applicant must submit:

Evidence	Details
1. **ATO Digital Service Provider Operational Framework letter of confirmation**	The most recent written confirmation from the ATO that the applicant is compliant against the ATO Framework (certified). The intention of the confirmation is to provide reasonable assurance of the applicant's ATO Framework implementation to the Accreditor. This confirmation should be issued by the ATO, be no more than 12 months old, and must include the applicants legal name and recognise it is meeting the requirements for products and services controlled by the Digital Service Provider with greater than 10,000 taxation or superannuation client records As the scope of the ATO Digital Service Provider Operational Framework and its partial reliance on ISO 27001 certification only covers some of the required controls set out by the CDR Rules, 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 Framework certification**	As per requirements below.
3. **Attestation**	Attestation that the applicant will be able to comply with the specific requirements of Schedule 2. Until the accreditation form is updated in the Participant Portal to reflect this, the attestation can take the form of a signed statement from a duly authorised representative from the applicant.

While an applicant may rely on the fact they are compliant to the top tier ATO Digital Service Provider Operational Framework as partial evidence of their information security capabilities for the purpose of accreditation at the unrestricted level, the applicant will still need to ensure they meet the requirements of Schedule 2 of the CDR Rules for their CDR data environment – in particular, if the ATO Digital Service Provider Operational Framework scope covers specific system/s rather than the organisation as a whole. To this end, an attestation that the applicant will be able to comply with the requirements of Schedule 2 of the CDR Rules will also be required in support of an applicant's accreditation application. The requirement to meet Schedule 2 includes meeting both the

rules that are focused on information security governance in Part 1, as well as the specific controls at Part 2 of the Schedule.

Assurance report covering the controls that are not covered by the ATO Digital Service Provider Operational Framework

The assurance report covering the controls that are not covered by the ATO Digital Service Provider Operational Framework will need to meet the requirements for an assurance report when applying for accreditation as set out in section 2.1.1 of these Guidelines, but with the following modifications:

- in terms of Part 1 of Schedule 2, it is only required to define the boundaries of the CDR data environment as required by clause 1.4 (Step 2) of Part 1 of Schedule 2 of the CDR Rules
- it is required to cover the Part 2 of Schedule 2 information security controls set out in table 3 below to supplement the ATO Digital Service Provider Operational Framework. These controls are either not included in the ATO Digital Service Provider Operational Framework or only partially met
- the assurance report should also include any of the other Part 2 of Schedule 2 information security controls excluded from an applicant's ATO Digital Service Provider Operational Framework.

Table 3: Controls requiring testing

#	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

#	Information security control	Description
		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.
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.

We encourage applicants to discuss reliance on a top tier ATO Digital Service Provider Operational Framework with us prior to submission of their accreditation application.

3. Ongoing information security reporting obligations

3.1. Unrestricted level

In order to comply with the default conditions of accreditation, under Schedule 1 of the CDR Rules, accredited persons are required to provide:

- an attestation statement at the end of the first reporting period of being accredited, and every alternate year thereafter (i.e. at the end of Year 1, Year 3, Year 5, and so on)[6]
- an assurance report to cover a one-year period starting from the day after the end of the first reporting period, and every second reporting period thereafter (i.e. Year 2, Year 4, Year 6, and so on).

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

The reporting period for an accredited person will be either a financial year or a calendar year, as determined for the accredited person by the Accreditor.

3.1.1. Attestation statement

The attestation statement must:

- meet the criteria for '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.

3.1.2. Ongoing assurance reports

An assurance report for the purposes of maintaining accreditation will be consistent with the requirements of the CDR Rules if it complies with the requirements for when applying for accreditation set out at section 2.1.1 or 2.1.2 (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, being a minimum of 12 months.

Where an accredited person is relying upon ISO 27001 certification as partial evidence to demonstrate that it satisfies the information security obligation, it 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 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.

Where an accredited person is relying upon level 1 PCI DSS certification as partial evidence to demonstrate that it satisfies the information security obligation, it must also provide to the Accreditor both the most recent Attestation of Compliance Form, Quarterly Network Scan undertaken by a PCI DSS Approved Scan Vendor and ROC undertaken by a Payment Card Industry Qualified Security Advisor.

Where an accredited person is relying upon top tier ATO Framework certification 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 Framework.

3.2. Acceptable auditors

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

ASAE 3150 contains a concept of the 'lead assurance practitioner', who maintains overall responsibility for the assurance engagement, including quality and alignment with certain standards and codes of ethics. 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.

3.3. Controls Guidance

The details of how a suitably experienced, qualified and independent auditor may perform an audit of the information security obligation, in relation to the CDR data environment, are set out in the *CDR Information Security Controls Guidance* (Controls Guidance).

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

The Controls Guidance does not aim to be prescriptive in the methodology by which an assessment should be performed. Further, it does not reflect the level of detail and complete set of elements that an auditor may require in order to complete their work and obtain assurance under the accepted standards. An auditor utilising this template will need to use their own professional judgement in determining whether it 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.

4. Part 1—Steps for Privacy Safeguard 12

Part 1 of Schedule 2 of the CDR Rules sets out the steps regarding the information security of CDR data.

Information security of CDR data refers to an accredited person's capability to manage the security of its CDR data environment in practice through the implementation and operation of an information security governance framework and underlying processes and controls which enable the accredited person to meet the mandatory steps under Part 1 of Schedule 2 of the CDR Rules.

This section summarises what is required by these steps and provides guidance on how accredited data recipients may implement them.

4.1. Step 1: Define and implement security governance in relation to CDR data

4.1.1. Information security governance framework

The CDR Rules require an accredited person to establish a formal information security governance framework for managing information security risks relating to its CDR data, including setting out the policies, procedures, roles and responsibilities required to facilitate the oversight and management of CDR data.

An accredited person may leverage their existing information security governance structure where this will cover their CDR data environment. An accredited person may utilise 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).

4.1.2. Roles and responsibilities

An accredited person must define roles and responsibilities for managing information security of CDR data, including 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, it is expected that the security governance structures (for example, committees and forums) in place will include membership from across key business areas.

4.1.3. 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,[7] and compliance with the policy monitored. The information security policy should document the various security areas managed by the accredited person.

4.1.4. 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 are required at least every 12 months, or sooner upon either of the following occurring:

- 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, such as the introduction of a new system, the migration of data onto new infrastructure, introduction of a new outsourced service provider, or a change to the terms and conditions of the services provided by an existing outsourced service provider.

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

Assessing and defining the boundaries of the CDR data environment involves identifying the people, processes, technology and infrastructure that manages, secures, stores or otherwise interacts with CDR data. The CDR data environment may include infrastructure owned by, and management provided by, an outsourced service provider or third party. An accredited person must document its CDR data environment and may do so through a detailed data flow diagram, or through a written statement.

---

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

Documentation must be reviewed and updated as soon as practicable upon the accredited person becoming 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.

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 through a combination of the following:

- segregation of 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 outsourced service providers interacting with CDR data.

Limiting the size of the CDR data environment is likely to increase the security of CDR data due to a decreased attack surface.

As part of the assurance report, the accredited person will be required to document a 'description of the system' in accordance with international auditing standards. This will include defining the people, processes, technology and controls in place to manage CDR data. For example, ASAE 3150 clearly defines what a 'description of system' means,[8] what elements it should cover,[9] what a suitably experienced, qualified and independent auditor should assess for determining if the description is complete and accurate in all respects,[10] and includes an example of what a description of the system looks like.[11] Where this description has been reviewed by a suitably experienced, qualified and independent auditor, it is expected that it will be sufficient for the purposes of documenting the CDR data environment.

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

An accredited person's information security capability includes its ability to manage the security of its CDR data environment through the implementation and operation of sufficiently designed processes and controls, the use of appropriate technology, equipment and infrastructure, and the involvement of suitably experienced persons. It may include steps or processes undertaken by outsourced service providers or third party infrastructure owners.

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 Part 1 of Schedule 2 of the CDR Rules, and
- complies with the controls specified in Part 2 of Schedule 2 of the CDR Rules to systems within the CDR data environment.

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. Such changes could result from the development of new applications,

[8] Section 17(J) of ASAE 3150.

[9] Section 51 of ASAE 3150.

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

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

migration to new infrastructure, or engagement of a new outsourced provider. Where no such material changes occur, this review must be undertaken annually.

4.4. 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 having regard to the factors set out in clause 1.5(1)(b) (Step 3) of Part 1 of Schedule 2 of the CDR Rules.

For example, in respect of testing the effectiveness of information security controls, a testing process may include independent audits and/or control self-assessments, in which the assessor identifies and assigns the associated control owner, assesses the effectiveness of those controls with respect to any deviations from expected operation, and identifies steps for improving controls. These deviations and remediation measures should be logged, tracked and reported to senior management.[12]

The testing program must require testing at a frequency and to an extent that is appropriate having regard to the matters set out at clause 1.6(1)(b) (Step 4) of Part 1 of Schedule 2 of the CDR Rules.

An accredited person must review its testing program in response to material changes to the extent and nature of threats to its CDR data environment, or the boundaries of its CDR data environment, or where no such changes occur, at least annually.

The expected level of independence and professional skills required for the performance of this testing is dependent upon the form of the test and assessment. 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, and may be applied by the accredited person in its development of a testing program.

4.5. Step 5: Manage and report security incidents

4.5.1. General guidance

An accredited person must have formal plans, procedures and practices in place for responding to a security incident, including methods for identifying, classifying and rating the incident, managing the incident through its lifecycle, following appropriate escalation channels, reporting to relevant authorities where necessary, and post-incident review.

As part of maintaining and ensuring the efficacy of these procedures, an accredited person must perform periodic testing, such as through tabletop exercises or interactive simulations to achieve a base level of preparedness. This testing should occur at least annually, and 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.

[12] CDR Rules, Schedule 2, Part 1, clause 1.6(3).

4.5.2. 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 plans to respond to information security incidents that it considers could plausibly occur.

For their CDR data security response plans, accredited persons should refer to the guidance published by the Office of the Australian Information Commissioner (OAIC) on the reporting of notifiable data breaches.[13] Accredited persons should also report all security incidents, even those of minor nature to the Australian Cyber Security Centre (ACSC). For example, such incidents may include, but are not limited to:

- system compromises that directly/ indirectly impact the CDR data environment
- receiving 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.[14]

5. Information security controls

The controls defined in Part 2 of Schedule 2 of the CDR Rules provide mandatory controls to be implemented across an accredited person's CDR data environment.

5.1. Control requirements and controls

In order to be accredited, an applicant will need to demonstrate that it would, if accredited, be able to meet all control requirements. The evidence required to demonstrate this is set out at section 2 of these Guidelines.

Deviations in the effectiveness of individual controls will not in and of itself preclude the Accreditor granting accreditation (potentially with conditions) provided it was of the view that the applicant would, if accredited, be able to meet all control requirements.

Information related to controls (such as logs of critical events, etc.) should be retained for a period of 6 years in accordance with rule 9.3(2)(l) of the CDR Rules. 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, so long as the information is still accessible if it is required in future (for example, for incidents or investigations).

---

[13] Guidance on notifiable data breach reporting is available at: http://www.oaic.gov.au/privacy/notifiable-data-breaches/.

[14] The ACSC reporting tool is available at: https://www.cyber.gov.au/report.

5.2. Industry standards

When assessing required controls, industry standards or frameworks that an accredited person has an existing certification against, may be able to be recognised by an auditor to the extent they adequately address relevant parts of the requirements. This recognition of controls will also apply to the extent that accredited persons will use outsourced service providers who are certified against industry standards (e.g. cloud providers). The term 'accepted industry standards' refers to a set of criteria relating to the standard processes and operations in that specific field. These are the generally accepted requirements followed by the members belonging to an industry. These 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 relate to common frameworks and standards for information security.

6. Guidance on outsourced service providers

6.1. General guidance

An accredited person may use an outsourced service provider to assist in providing goods or services to a CDR consumer. An accredited person may also use another accredited person as an outsourced service provider to collect CDR data from a data holder.

An accredited person may choose to use outsourced 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.

An accredited person may be liable for the use or disclosure of CDR data by outsourced service providers, or certain other recipients of that data, by virtue of rule 7.6(2) of the CDR Rules. Accordingly, accredited persons should consider carefully the terms on which they disclose any CDR data to outsourced service providers.

The CDR Rules do not preclude an accredited person from storing CDR data on infrastructure owned by third parties. However, the fact that an accredited person uses infrastructure owned by a third party to store CDR data does not have the effect of removing the obligations and requirements on the accredited person in respect of that data that arise by virtue of legislation or the CDR Rules.

The extent to which a third party has access to data may be relevant to determining whether that data has been disclosed to such party for the purposes of the CDR Rules.

Outsourced service providers who are not collecting CDR data on behalf of an accredited person are not precluded by the CDR Rules from subcontracting. However, the CDR Rules specify various requirements in respect of a CDR outsourcing arrangement (see rule 1.10 of the CDR Rules).

6.2. Application of outsourcing to Part 1 of Schedule 2

6.2.1. Treatment in assurance reporting

Where controls requirements under Schedule 2 of the CDR Rules are performed by an outsourced service provider, the auditor will be required to perform the audit procedures and issue an assurance report using the 'carve-in' approach.[15]

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

An alternative carve-in method is to utilise existing third party assurance reports provided by the outsourced 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.

6.2.2. Assessment of controls performed by an outsourced service provider

Where a control defined in Part 2 of Schedule 2 of the CDR Rules is or will be performed by an outsourced service provider, an accredited person must assess these as part of their formal controls assessment program. This includes assessments prior to on-boarding a new outsourced service provider (during the due diligence phase), as well as periodic assessments in line with the inherent risk of the outsourced service provider in regards 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.

Where an accredited person is reliant on information security control testing provided by the outsourced service provider, such as general use third-party assurance reports, the accredited person must assess whether the extent and frequency of controls testing directly relate to the management of the accredited person's CDR data. Further, the accredited person must ensure that the controls tested align to the control requirements defined in Part 2 of Schedule 2 of the CDR Rules where the performance of a control is outsourced.

6.2.3. Security incidents at an outsourced service provider

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

In order to ensure compliance 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.

[15] In circumstances where an applicant or accredited person is relying on ISO 27001 certification to satisfy their information security obligation, the carve-in approach is required to be taken for those controls covered by the reduced scope assurance report.

Glossary

Shortened form	Extended form
accredited person	an accredited person is 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	CDR data is specific information for the relevant designated sector. See section 56AI(1) of the Act. For the banking sector this is set out in Schedule 3 of the CDR Rules.
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
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

Shortened form	Extended form
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 person to whom an accredited person discloses CDR data under a CDR outsourcing arrangement
PaaS	Platform as a service
PCI DSS	Payment Card Industry Data Security Standard
ROC	PCI DSS annual Report on Compliance
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