

CDR Accreditation Application Form: Unrestricted Level

List of all the questions that may be asked in the full application form for CDR accreditation at the unrestricted level

Warning

This is not a CDR unrestricted accreditation application form. It does not reflect the look and flow of an application made through the online CDR Participant portal.

April 2022

What is the sample application?

This sample application incorporates all the questions that may appear in the full online CDR accreditation application for the unrestricted level, which will be available on the CDR Participant Portal, plus notes on how the online application works. Looking at this sample application before starting an application may be particularly useful if someone else is filling out the application on your behalf.

The online application looks different from this sample as it operates as a series of screens that will guide you through each step.

You will not be asked all questions in the sample application because the CDR Participant Portal tailors the online application to your responses.

Warning

This is a sample application provided for information purposes only and cannot be used to lodge a CDR unrestricted level accreditation application.

The approved form for an application to be an unrestricted level accredited person, for the purposes of section 5.2 of the Competition and Consumer (Consumer Data Right) Rules 2020, is the online application form available via the CDR Participant Portal.

Starting your application

This is an application for [Note: your entity's name will be displayed here] to be accredited as an accredited data recipient, at the unrestricted level, for the CDR. We recommend you read our [CDR Accreditation Guidelines](#) [Note: a link to the CDR Accreditation Guidelines will be provided] before commencing your application as this will aid you in understanding the requirements of accreditation.

You will need to provide some general background information about the applicant to enable us to assess your application, and information to address the following criteria:

- fit and proper person
- information security
- insurance
- internal dispute resolution
- external dispute resolution

You will also need to upload documents in support of your application.

This information is required to assess whether the applicant satisfies the accreditation criteria.

WARNING

It is a serious criminal offence under the Commonwealth Criminal Code to provide false or misleading information. False or misleading information in an application (including a material omission) may also be grounds to revoke any accreditation granted based on that information.

Personal information

Please note that some of the information you provide in your application is 'Personal Information'. The below privacy notice should be read in conjunction with the [ACCC/AER Privacy Policy](#) [Note: a link to the ACCC/AER privacy statement will be provided].

By submitting your application, you acknowledge and accept the following:

- Why we are collecting the information

Information in this application is being collected by us for two purposes:

- as the Data Recipient Accreditor, to assess whether your application satisfies the accreditation criteria in the CDR Rules and
- to facilitate the proper functioning of the CDR system. This may include (but is not limited to) ensuring that the correct information is available through the Register of Accredited Persons and for compliance and enforcement of the CDR regime.

- How we will use the information collected

The information may be shared from time-to-time with other regulators (for example, the Australian Prudential Regulatory Authority, the Australian Securities and Investments Commission, the Australian Financial Complaints Authority and the Information Commissioner) or external consultants engaged by us to assist us with our two purposes stated above.

The information you provide regarding the applicant and the applicant's associated persons will be used to verify the information provided in your application. This could include conducting a police check.

Some of the information will be displayed on a public facing section of the Register of Accredited Persons (such as the company name and Australian Business Name of all CDR participants) while other information will only be available to other CDR participants or only available to us.

- What happens if you do not provide some of the information

All information requested is mandatory, unless otherwise stated. If all mandatory information is not provided, we will not be able to assess your application and your application will be returned to you for completion.

- In general, your information is stored in Australia and will not be disclosed to overseas recipients. However, there are exceptions

We use an external provider to store and collect this information, on servers in Australia, in a secure environment.

The information you provide regarding the applicant and the applicant's associated persons may be shared with overseas regulators and law enforcement to verify the information provided in your application.

Please confirm that you understand and agree with the way the personal information provided in your application will be used and handled, as set out above.

Yes

Note: You must tick yes to proceed with the application

Note: Once you choose to continue from this point an application is generated with its own unique reference number

General background information

Reference number XX

About the applicant

Note: Your application reference number will be displayed on each screen from this point onwards.

We require the following information in order to better understand the applicant and their business.

1. How many full time equivalent employees does the applicant have? *Select a number from the ranges in the list*
2. Please describe the shareholder or ownership structure of the applicant. Include shareholder/owner names, a breakdown of capital and voting rights and detail any close links to other companies:
 - a. Description: *Enter text*
 - b. Number of owners/shareholders: *Select a number from the list*
 - c. Names and shareholdings of top shareholders/owners (include no more than 5)
3. Please provide a clear description of the applicant's current business products/services *Enter text*
4. Can you provide an estimate of the following profitability indicators for the applicant from the last financial year (in AUD):
 - a. Gross revenue *Enter a number*
 - b. Net profit *Enter a number*
 - c. Return on investment *Enter a number*

Document required

Please upload the applicant's financial statement from the last financial year (or latest draft) at the end of the application.

5. Does the applicant hold an Australian Financial Services Licence? Yes No

If yes, please provide the licence number. *Enter a number*

6. Does the applicant hold an Australian Credit Licence? Yes No

If yes, please provide the licence number. *Enter a number*

7. Has the applicant been registered or accredited to participate in a regime similar to the CDR in another country? Yes No

If yes, please provide details about all countries in which the applicant has been registered or accredited to participate in a regime similar to the CDR:

- a. Specify which country the applicant is registered/accredited in. *Choose from a drop down list with option to add*

- b. Provide any relevant registration numbers (if known). *Enter a number*
- c. Provide details of the applicant's use case for that country's regime. *Enter text*

General background information

Reference number XX

Intended use of data

Please provide details about all the products/services the applicant will offer to individual customers/businesses if accredited.

1. What is the name of the product/service the applicant will offer? *Enter text*
2. Under what registered business name (including any relevant number) will the applicant offer the product/service? *Enter text*
3. Does the applicant currently offer the product/service? Yes No
4. Please provide a clear description of the product/service in as much detail as possible. Please also upload a document providing a worked example(s) of how an individual customer/business would use the applicant's product/service(s) at the end of the application. *Enter text*
5. What are the benefits to individual customers/businesses of the product/service? *Enter text*
6. Are there any monetary or non-monetary costs to individual customers/businesses of the product/service? Yes No

 If yes, what are these costs? *Enter text*

 If no, what is the value to the applicant of providing the product/service? *Enter text*
7. Who is the intended target audience of the product/service? *Check box options provided are individuals/business/other (please specify)*
8. How many individual customers/businesses does the applicant intend to service in the first year following accreditation? *Select a number range from the list*
9. How will the CDR data collected be used to provide the product/service? *Enter text*
10. Will the CDR data collected, or data derived from that data (whether de-identified or not), be disclosed to any other party? Yes No

 If yes, please specify how this data will be disclosed? *Enter text*
11. Will the CDR data collected, or data derived from that data (whether de-identified or not), be used for any other purpose?

 If yes, please specify how this data will be used. *Enter text*

Document required

Please upload a document providing a worked example(s) of how an individual customer/business would use the applicant's product/service(s) at the end of the application.

General background information

Reference number XX

Potential reciprocal data holder obligations

ATTENTION

If the applicant generates and holds designated data, upon accreditation as a data recipient, the applicant will also become subject to reciprocal data holder obligations. This means it must also provide an online service that can be used:

- *to make product data requests*
- *by CDR consumers to make consumer data requests directly from the data holder*
- *by accredited data recipients to make consumer data requests on behalf of CDR consumers to the data holder.*

For example, when a non-bank lender is accredited it may become a reciprocal data holder in respect of data it generates and holds for its personal loan products. An accredited person that provides a budgeting app, but does not offer any Phase 1, Phase 2 or Phase 3 products outlined in the relevant sector schedules in the CDR rules, will not be a reciprocal data holder.

The timeframe for when these obligations come into effect is outlined in the relevant sector schedules in the CDR rules. An applicant who becomes a reciprocal data holder will also need to register as a data holder in the CDR participant portal.

A phasing table summarising mandatory data sharing obligations for reciprocal data holders is available on the CDR website.

We encourage applicants with questions or wanting to discuss how these obligations may apply to them to contact the ACCC at ACCC-CDR@acc.gov.au.

What is designated data for the purposes of the CDR?

If the applicant offers or supplies:

a product to a person in connection with one or more of the following activities:

- taking money on deposit (otherwise than as part-payment for identified goods or services)
- making advances of money
- another financial activity prescribed for the purposes of subparagraph (b)(ii) of the definition of banking business in subsection 5(1) of the *Banking Act 1959 (Cth)*, or

a purchased payment facility to a person

data about the product, the use of the product and the user of the product will be designated for the purposes of the CDR.

- See the [Consumer Data Right \(Authorised Deposit-Taking Institutions\) Designation 2019](#).

Is the applicant currently a data holder, as defined in the *Competition and Consumer Act 2010 (Cth)*, of any data specified in a designation instrument (**designated data**)?

Yes No

If yes

- a. What types of designated data does the applicant hold? *Enter text*

- b. Under what registered business names (including any relevant number) is the product/service relating to that data being offered to individual customers/businesses? *Enter text*

If no

Does the applicant expect to be a data holder of designated data in the future?

Yes No

Then if yes

- a. Please provide date (if known) from which the applicant expects to hold this data. *Enter number*
- b. What types of designated data does the applicant expect to hold? *Enter text*
- c. Under what registered business names (including any relevant number) will the product/service relating to that data be offered to individual customers/businesses? *Enter text*

Fit and proper person

Associated persons

To be accredited, the applicant must be a fit and proper person to manage CDR data having regard to the fit and proper person criteria. To make this assessment we need to know who the applicant's associated persons are.

An 'associated person' of another person means any of the following:

- (b) a person who:
 - (i) makes or participates in making, or would (if the other person were an accredited person) make or participate in making, decisions that affect the management of CDR data by the other person; or
 - (ii) has, or would have (if the other person were an accredited person), the capacity to significantly affect the other person's management of CDR data;

(b) if the other person is a body corporate—a person who:

- (i) is an associate (within the meaning of the *Corporations Act 2001 (Cth)*) of the other person; or
- (ii) is an associated entity (within the meaning of the *Corporations Act 2001 (Cth)*) of the other person.

See rule 1.7 (1), CDR Rules.

The applicant is [*Note: your entity's name will be displayed here*].

To enable us to know who the applicant's associated persons are please also provide the following details for each of the applicant's associated persons.

1. Is the person an individual or a company? *Choose from individual or company*
2. If the person is
 - a. An individual – please provide:
 - i. Name *Enter first name middle name/s and last name*
 - ii. Any other name the person has previously been known by *Enter first name, middle name and last name*
 - iii. Date of birth *Enter date*
 - iv. Residential address. *Enter address*
 - b. a body corporate – please provide:
 - i. Company name *Enter text*
 - ii. I or registered business number for non-Australian companies *Enter number*
 - iii. Country of registration.
3. If an individual – please provide:
 - i. Email *Enter email*

4. If a body corporate – please provide:
 - i. Registered business address and email *Enter address and email*

5. What is the persons relationship to the applicant? If the person is an individual Identify a specific role (for example a director, company secretary or manager (specify role)). If the person is a company Identify the relationship to the applicant (for example, holding company or subsidiary).
Enter text

Document required

Please upload at the end of the application a current organisational chart and a corporate structure chart (if the applicant is a body corporate) reflecting all associated persons listed above as well as their relationships with the applicant.

Accreditation criteria

Reference number XX

Fit and proper person

Please respond to the questions below on behalf of the applicant.

Each of the applicant's associated persons must also complete a signed declaration addressing each of the fit and proper person criteria. The declaration template can be found on the [CDR resources website](#) and will need to be uploaded at the end of the application.

Questions

The applicant must be fit and a proper person to manage CDR data having regard to the fit and proper person criteria. To enable us to assess this criterion please answer the following questions on behalf of the applicant:

1. In the previous 10 years, has the applicant been convicted of a serious criminal offence against any law of the Commonwealth, or of a State or Territory, or a law of a foreign jurisdiction?
Yes No

A 'serious criminal offence' is defined in Rule 1.9 (2) of the [CDR Rules](#).

If yes, please provide details about all contraventions. *Enter text*

2. In the previous 10 years, has the applicant been convicted of an offence of dishonesty against any law of the Commonwealth, or of a State or Territory, or a law of a foreign jurisdiction?
Yes No

If yes, please provide details about all contraventions. *Enter text*

3. Has the applicant been found to have contravened a law relevant to the management of CDR data or a similar law of a foreign jurisdiction? Yes No

A 'law relevant to the management of CDR data' includes, but is not limited to, any of the following:

- the *Competition and Consumer Act 2010 (Cth)*
- any regulations made for the purposes of the *Competition and Consumer Act 2010 (Cth)*
- the Competition and Consumer (Consumer Data) Rules 2020
- the *Corporations Act 2001 (Cth)*
- the Corporations Regulations 2001
- the *Privacy Act 1988 (Cth)*
- the *Australian Securities and Investment Commission Act 2001 (Cth)*.

See Rule 1.7(1), [CDR Rules](#).

If yes, please provide details about all contraventions. *Enter text*

4. Has the applicant been subject to a determination under paragraph 52(1)(b) or any of paragraphs 52(1A)(a), (b), (c) or (d) of the *Privacy Act 1988 (Cth)*? [Note: a link to paragraph 52(1)(b) and 52(1A) of the *Privacy Act 1988 (Cth)* will be provided] Yes No

If yes, please provide details about all contraventions. *Enter text*

5. Has the applicant, or any of its directors (if the applicant is a body corporate) been disqualified from managing corporations? Yes No

If yes, please provide details about all contraventions. *Enter text*

6. Has the applicant, or any of its directors (if the applicant is a body corporate) been subject to a banning order [Note: a link to section 920B of the *Corporations Act 2001 (Cth)* will be provided]? Yes No

If yes, please provide details about all contraventions. *Enter text*

7. Has the applicant a history of insolvency either in Australia or another jurisdiction? This question only applies if the applicant is a body corporate. Yes No Not Applicable

For example, has the applicant ever entered into liquidation, voluntary administration, or receivership? Insolvency is defined in section 95A of the *Corporations Act 2001 (Cth)* to mean an inability of a person to pay all of their debts as and when they become due.

If yes, please provide details about all insolvency events. *Enter text*

8. Has the applicant a history of bankruptcy either in Australia or another jurisdiction? This question is only applicable if the applicant is an individual. Yes No Not Applicable

For example, has the person ever been declared bankrupt, presented a debtor's petition pursuant to section 55 of the *Bankruptcy Act 1966 (Cth)* or had a creditor's petition presented against them pursuant to the *Bankruptcy Act 1966 (Cth)*.

If yes, please provide details about all bankruptcy events. *Enter text*

9. Has the applicant been subject to a determination made under an external dispute resolution scheme that included a requirement to pay monetary compensation and was at the time the determination was made recognised under the *Privacy Act 1988 (Cth)* or a recognised external dispute resolution scheme? Yes No

The Australian Financial Complaints Authority is the recognised external dispute resolution scheme for the banking sector.

In addition to the Australian Financial Complaints Authority the following external dispute resolution schemes are also currently recognised under the *Privacy Act 1988 (Cth)*:

- i. Energy & Water Ombudsman (NSW) Limited
- ii. Energy and Water Ombudsman Queensland
- iii. Energy and Water Ombudsman (SA)
- iv. Energy and Water Ombudsman (Victoria) Limited
- v. Energy and Water Ombudsman Western Australia
- vi. Public Transport Ombudsman Limited (Victoria)
- vii. Telecommunications Industry Ombudsman Limited
- viii. Tolling Customer Ombudsman
- ix. Credit and Investments Ombudsman
- x. Financial Ombudsman Service.

If yes, please provide details about all determinations. *Enter text*

10. Are there any other matters relevant to our assessment of whether the applicant would be able to comply with the fit and proper person obligation?

For example, but not limited to, whether in Australia or overseas:

- any criminal investigation or proceedings that the applicant is currently the subject
- any investigation or disciplinary action by a professional association where the applicant:
 - is the subject, or
 - has been the subject and an adverse finding was made against them.
- any inquiry or investigation initiated by a government agency where the applicant:
 - is the subject, or
 - has been the subject and an adverse finding was made against them.
- any court proceedings initiated by a government agency where the applicant:
 - is the subject, or
 - has been the subject and an adverse finding was made against them.

Yes No

If yes, provide details of any other matters. *Enter text*

For each associated person, please upload a signed declaration addressing each of the fit and proper person criteria.

Accreditation criteria

Reference number XX

Information security

The applicant must show that, if accredited, it would be able to satisfy the information security obligation set out in rule 5.12(1)(a), CDR Rules. For the unrestricted level, to demonstrate it satisfies the information security obligation the applicant is required to provide either:

- an assurance report prepared in accordance with one of the accepted standards listed in the CDR Supplementary Accreditation Guidelines: Information Security
- acceptable equivalent evidence outlined in the CDR Supplementary Accreditation Guidelines: Information Security.

For further detail about the information security obligation and how an applicant is required to satisfy this obligation see Schedule 2, CDR Rules and the [CDR Supplementary Accreditation Guidelines: Information Security](#) [Note: a link to the CDR Supplementary Accreditation Guidelines: Information Security will be provided].

Assurance reports must be conducted by a suitably qualified and independent auditor who is capable of issuing a report in compliance with an accepted standard. Assurance reports must be:

- 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).
- prepared in accordance with one of the following accepted standards:
 - the Australian Standard on Assurance Engagements (ASAE) 3150 *Assurance Engagement on Controls* (ASAE 3150)
 - the ASAE 3402 *Assurance Reports on Controls at a Service Organisation*
 - International Standard on Assurance Engagements (ISAE) 3000 series
 - SOC1/SOC2 reports prepared in accordance with applicable Statement on Standards for Attestation Engagements (SSAE) standards.
- a reasonable assurance engagement. A reasonable assurance engagement (as opposed to a limited assurance engagement) is an assurance engagement in which the assurance practitioner reduces engagement risk to an acceptably low level in the circumstances of the engagement as the basis for the assurance practitioner's conclusion. The assurance practitioner's conclusion is expressed in a form that conveys the assurance practitioner's opinion on the outcome of the measurement or evaluation of the underlying subject matter against criteria.

Applicants may also partially rely on ISO 27001 certification, level 1 PCI DSS compliance or top tier Australian Tax Office's Digital Service Provider Operational Framework compliance to satisfy the information security obligation by submitting the acceptable equivalent evidence outlined in sections 2.1.4 – 2.1.6 of the CDR Supplementary Accreditation Guidelines: Information Security. For further detail about what the assurance report or equivalent evidence must encompass and who is qualified to undertake an audit, see the [CDR Supplementary Accreditation Guidelines: Information Security and the Controls Guidance](#) [Note: a link to the Controls Guidance will be provided].

Does the applicant meet the information security obligation by having one of:

- an independent auditor's assurance report on its ability to satisfy the information security obligation?

- a current ISO 27001 certification together with a reduced scope assurance report on its ability to satisfy the information security obligation?
- level 1 PCI DSS compliance together with a reduced scope assurance report on its ability to satisfy the information security obligation?
- top tier Australian Tax Office’s Digital Service Providers Operational Security Framework compliance together with a reduced scope assurance report on its ability to satisfy the information security obligation?

If relying on independent auditor’s assurance report

1. Name of auditor? *Enter text*
2. Please outline the auditor’s qualifications and previous experience in preparing equivalent assurance reports. *Enter text*
3. Date of assurance report? *Enter date*
4. Was the assurance report prepared in accordance with an accepted standard listed in the CDR Supplementary Accreditation Guidelines: Information Security?
Yes No
5. Is the assurance report 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)? Yes No
6. Is the assurance a reasonable assurance engagement? Yes No
7. Has the applicant’s senior management approved and commented on the assurance report?
Yes No
8. Does the assurance report describe the applicant’s information security governance framework? Yes No
9. Does the assurance report include a detailed description of the system clause 1.4 of Schedule 2 to the CDR Rules? Yes No

A description of the system is a definition of the people, processes, technology and controls in place to manage CDR data prepared in accordance with international auditing standards. The description of the system should relate to the applicant’s CDR Data Environment as defined in Schedule 2, [CDR Rules](#).

10. If accredited, does the applicant presently intend that it would rely on any outsourced service provider(s) or third party provider(s) to meet any control requirements referred to in Schedule 2, Part 2 of the CDR Rules? Yes No

Then if yes

Does the assurance report adopt a carve-in approach to relevant controls performed by any outsourced service provider(s)/third party provider(s)? Yes No

11. Does the assurance report identify any controls where exceptions were noted in the design or implementation of the control? Yes No

If yes, please provide details about each control where exceptions were noted in the design or implementation of the control

- a. Control name? *Enter text*
- b. Please detail the exception. *Enter text*
- c. Please detail the steps being taken to remediate the exception. *Enter text*

Document required

Please upload the assurance report at the end of the application.

If relying on ISO 27001 certification

1. Date of ISO 27001 information security management system certificate? *Enter date*
2. Does the ISO 27001 information security management certificate confirm that the applicant is certified in the defined scope statement? Yes No
3. Does the ISO 27001 information security management certificate include the original certificate as well as any recertification certificates (if applicable) to validate that continuous recertification has been performed? Yes No
4. Does the applicant have an information security management system (ISMS) internal audit report which provides reasonable assurance of the applicant's ISMS implementation? Yes No
5. Name of auditor of the information security management system internal audit report? *Enter text*
6. Does the auditor of the information security management system internal audit report hold an ISO 27001 Lead Auditor qualification? Yes No
7. Date of information security management system internal audit report? *Enter date*
8. Does the applicant have a statement of applicability describing the current state of its environment? Yes No
9. Does the applicant have an accompanying reduced scope assurance report? Yes No

10. Name of auditor of reduced scope assurance report? *Enter text*
11. Please outline the auditor's qualifications and previous experience in preparing equivalent assurance reports. *Enter text*
12. Date of reduced scope assurance report? *Enter date*
13. Was the reduced scope assurance report prepared in accordance with an accepted standard listed in the CDR Supplementary Accreditation Guidelines: Information Security?
Yes No
14. Is the reduced scope assurance report 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)?
Yes No
15. Is the reduced scope assurance a reasonable assurance engagement? Yes No
16. Has the applicant's senior management approved and commented on the reduced scope assurance report? Yes No
17. Does the reduced scope assurance report describe the applicant's information security governance framework? Yes No
18. Does the reduced scope assurance report include a detailed description of the system clause 1.4 of Schedule 2 to the CDR Rules? Yes No

A description of the system is a definition of the people, processes, technology and controls in place to manage CDR data prepared in accordance with international auditing standards. The description of the system should relate to the applicant's CDR Data Environment as defined in Schedule 2, [CDR Rules](#).

19. Does the applicant attest that it complies with the requirements of Schedule 2 to the CDR Rules for its CDR data environment? Yes No
20. If accredited, does the applicant presently intend that it would rely on any outsourced service provider(s)/third party provider(s) to meet any control requirements referred to in Schedule 2, Part 2 of the CDR Rules? Yes No

Then if yes

- a. Does the reduced scope assurance report adopt a carve-in approach to relevant controls performed by any outsourced service provider(s)/third party provider(s)?
Yes No

21. Does the reduced scope assurance report identify any controls where exceptions were noted in the design or implementation of the control? Yes No

Then if yes

- a. How many controls were exceptions noted for? *Enter number*
- b. For each control, please provide details where exceptions were noted in the design or implementation of the control
- c. Control name? *Enter text*
- d. Please detail the exception. *Enter text*
- e. Please detail the steps being taken to remediate the exception. *Enter text*

Document required

At the end of the application please upload:

- ISO 27001 information security management system certificate
- information security management system internal audit report
- statement of applicability describing the current state of the applicant's environment
- reduced scope assurance report

If relying on level 1 PCI DSS compliance:

1. Date of latest annual PCI DSS Report on Compliance? *Enter date*
2. Does the latest annual PCI DSS Report on Compliance cover all of the required level 1 controls? Yes No
3. Name of auditor of the latest annual PCI DSS Report on Compliance? *Enter text*
4. Is the auditor of the latest annual PCI DSS Report on Compliance a Payment Card Industry Qualified Security Advisor? Yes No
5. Date of latest Quarterly Network Scan as undertaken by a PCI DSS Approved Scan Vendor? *Enter date*
6. Name of PCI DSS Approved Scan Vendor who undertook the latest Quarterly Network Scan? *Enter text*
7. Does the applicant have an accompanying reduced scope assurance report? Yes No
 - a. Name of auditor of reduced scope assurance report? *Enter text*
 - b. Please outline the auditor's qualifications and previous experience in preparing equivalent assurance reports. *Enter text*
 - c. Date of reduced scope assurance report? *Enter date*
 - d. Was the reduced scope assurance report prepared in accordance with an accepted standard listed in the CDR Supplementary Accreditation Guidelines: Information Security? Yes No
 - e. Is the reduced scope assurance report 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)? Yes No

- f. Is the reduced scope assurance a reasonable assurance engagement?
Yes No
- g. Has the applicant's senior management approved and commented on the reduced scope assurance report? Yes No
- h. Does the reduced scope assurance report describe the applicant's information security governance framework? Yes No
- i. Does the reduced scope assurance report include a detailed description of the system as required by clause 1.4 of Schedule 2 to the Rules? Yes No

A description of the system is a definition of the people, processes, technology and controls in place to manage CDR data prepared in accordance with international auditing standards. The description of the system should relate to the applicant's CDR Data Environment as defined in Schedule 2, [CDR Rules](#).

8. Does the applicant attest that it complies with the requirements of Schedule 2 to the CDR Rules for its CDR data environment? Yes No
9. If accredited, does the applicant presently intend that it would rely on any outsourced service provider(s)/third party provider(s) to meet any control requirements referred to in Schedule 2, Part 2 of the CDR Rules? Yes No

Then if yes

- a. Does the reduced scope assurance report adopt a carve-in approach to relevant controls performed by any outsourced service provider(s)/third party provider(s)? Yes No

10. Does the reduced scope assurance report identify any controls where exceptions were noted in the design or implementation of the control? Yes No

Then if yes

- a. How many controls were exceptions noted for? *Enter number*

11. For each control, please provide details where exceptions were noted in the design or implementation of the control:

- a. Control name? *Enter text*
- b. Please detail the exception. *Enter text*
- c. Please detail the steps being taken to remediate the exception. *Enter text*

Documents required

At the end of the application please upload:

1. latest annual PCI DSS Report on Compliance
2. latest Quarterly Network Scan
3. latest PCI DSS Attestation of Compliance Form
4. reduced scope assurance report

If relying on top tier ATO Digital Service Provider Operational Security Framework compliance

1. Date of latest ATO Digital Service Provider Operational Security Framework letter of confirmation? *Enter date*

2. Does the latest ATO Digital Service Provider Operational Security Framework letter of confirmation:
 - a. include the applicant's legal name
 - b. acknowledge that the applicant meets the requirements for products and services controlled by the Digital Service Provider with more than 10,000 taxation or superannuation client records: Yes No

3. Does the applicant have an accompanying reduced scope assurance report?
Yes No
 - a. Name of auditor of reduced scope assurance report? *Enter text*
 - b. Please outline the auditor's qualifications and previous experience in preparing equivalent assurance reports. *Enter text*
 - c. Date of reduced scope assurance report? *Enter date*
 - d. Was the reduced scope assurance report prepared in accordance with an accepted standard listed in the CDR Supplementary Accreditation Guidelines: Information Security? Yes No
 - e. Is the reduced scope assurance report 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)?
Yes No
 - f. Is the reduced scope assurance a reasonable assurance engagement?
Yes No
 - g. Has the applicant's senior management approved and commented on the reduced scope assurance report? Yes No
 - h. Does the reduced scope assurance report describe the applicant's information security governance framework? Yes No
 - i. Does the reduced scope assurance report include a detailed description of the system as required by clause 1.4 of Schedule 2 to the CDR Rules? Yes No

A description of the system is a definition of the people, processes, technology and controls in place to manage CDR data prepared in accordance with international auditing standards. The description of the system should relate to the applicant's CDR Data Environment as defined in Schedule 2, [CDR Rules](#).

- j. Does the applicant attest that it complies with the requirements of Schedule 2 to the CDR Rules for its CDR data environment? Yes No
- k. If accredited, does the applicant presently intend that it would rely on any outsourced service provider(s)/third party provider(s) to meet any control requirements referred to in Schedule 2, Part 2 of the CDR Rules?
Yes No

Then if yes

- i. Does the reduced scope assurance report adopt a carve-in approach to relevant controls performed by any outsourced service provider(s)/third party provider(s)? Yes No
- l. Does the reduced scope assurance report identify any controls where exceptions were noted in the design or implementation of the control? Yes No

Then if yes

- i. How many controls were exceptions noted for? *Enter number*
4. For each control, please provide details where exceptions were noted in the design or implementation of the control:
- a. Control name? *Enter text*
 - b. Please detail the exception. *Enter text*
 - c. Please detail the steps being taken to remediate the exception. *Enter text*

Document required

At the end of the application, please upload:

- latest ATO Digital Service Provider Operational Security Framework letter of confirmation
- reduced scope assurance report

Regardless of which type of evidence is relied on

Accredited persons are subject to ongoing reporting obligations relating to information security (Schedule 1, CDR Rules). Guidance on these obligations can be found in the CDR Supplementary Accreditation Guidelines: Information Security [Note: a link to the CDR Supplementary Accreditation Guidelines: Information Security will be provided].

A reporting period can either be a financial year or a calendar year, as determined for the accredited person by the Data Recipient Accreditor.

If and when accredited, would the applicant prefer for its reporting period to be a financial year or a calendar year?

- Calendar year
- Financial year

Accreditation criteria

Reference number XX

Insurance

Overview

The applicant may satisfy the insurance obligation by holding adequate insurance or by having in place a comparable guarantee.

For further detail about what the Data Recipient Accreditor considers to be adequate insurance or a comparable guarantee see the CDR Supplementary Accreditation Guidelines: Insurance.

Does the applicant meet the insurance obligation

1. by holding adequate insurance? Yes No or
2. by having in place a comparable guarantee? Yes No

Document required

If relying on insurance display the below.

At the end of this application upload a statement signed by an authorised representative of the applicant:

- summarising the insurance policy or policies held by the applicant
- explaining why the applicant contends that the insurance policy or policies it holds are adequate to cover the liabilities it may incur in connection with the management of CDR data.
- addresses how the applicant considers its insurance policies meet the factors in Table 1 on Page 6 of our supplementary insurance guidelines [*Note: a link to the factors in Table 1 on Page 6 of the supplementary insurance guidelines will be included*].

If relying on comparable guarantee display the below.

At the end of this application upload a statement signed by an authorised representative of the applicant:

- summarising the terms of the guarantee and sufficient details about the guarantor to enable consideration of the financial capacity of the guarantor to meet the terms of the guarantee

explaining why the applicant contends that the guarantee it holds is adequate to cover the liabilities it may incur in connection with the management of CDR data.

The statement should address the matters the Data Recipient Accreditor will have regard to in considering whether the insurance obligation is met as set out in the CDR Accreditation Guidelines.

Accreditation criteria

Reference number XX

Insurance

Details

Please provide information about each separate insurance policy relied upon.

1. Insurance policy type? *Choose from check box options: professional indemnity insurance/cyber insurance/professional indemnity and cyber insurance combined/other [please specify]*
2. Policy number? *Enter number*
3. Insurance provider? *Enter name*
4. Expiry date? *Enter date*
5. What currency is your insurance in? *Enter currency*
6. Annual aggregate amount of cover? *Enter number*
7. Is the applicant a named insured? Yes No
8. Does the policy indemnify the applicant from civil liability to CDR consumers arising from the management of CDR data? Yes No

If yes, does the policy have any specific limitations, caps or exclusions in relation to civil liability to CDR consumers arising from the management of CDR data?

Yes No

If yes, please detail these specific limitations, caps or exclusions. *Enter text*

9. Does the policy include awards made by the Australian Financial Complaints Authority?
Yes No

If yes, does the policy have any specific limitations, caps or exclusions in relation to awards made by the Australian Financial Complaints Authority? Yes No

If yes please detail these specific limitations, caps or exclusions. *Enter text*

10. Does the policy cover third party liability from breaches of privacy legislation?
Yes No

If yes please provide details of the coverage. *Enter text*

11. Does the policy contain any exclusions relating to privacy legislation?
Yes No

If yes Please provide details of the coverage. *Enter text*

12. Does the policy contain any exclusions relating to data breaches?

Yes No

If yes, please provide details of the coverage. *Enter text*

13. Does the policy contain any exclusions relating to fraud and dishonesty?

Yes No

If yes, please provide details of the coverage. *Enter text*

14. Does the policy contain any exclusions relating to retrospective cover?

Yes No

If yes, please provide details of the coverage. *Enter text*

Documents required

At the end of this application upload both:

1. a certificate of currency, and
 2. the policy document
- for each insurance policy relied upon.

If relying on comparable guarantee:

1. Name of guarantor? *Enter company name*

2. Is the comparable guarantee provided by a related company to the applicant?

Yes No

3. Name, phone number and email of a contact at the guarantor. *Enter first and last name, phone number and email*

Document required

At the end of this application upload a document signed by the guarantor providing evidence of the guarantee.

Accreditation criteria

Reference number XX

Internal dispute resolution

The applicant must have in place internal dispute resolution procedures that meet the internal dispute resolution requirements.

Schedule 3, Rule 5.1, CDR Rules provides that:

In the banking sector an applicant's internal dispute resolution procedures meet the internal dispute resolution requirements if these comply with provisions of Australian Securities and Investments Commission Regulatory Guide 271 that deal with the following:

- (a) standards that its internal dispute resolution procedures or processes must meet regarding the following:
 - (i) commitment and culture
 - (ii) the enabling of complaints
 - (iii) resourcing
 - (iv) responsiveness
 - (v) objectivity and fairness
 - (vi) data collection, analysis and internal reporting
 - (vii) internal reporting and analysis of complaint data
 - (viii) continuous improvement
- (b) outsourcing internal dispute resolution processes
- (c) acknowledgement of complaint
- (d) what an internal dispute resolution response must contain
- (e) maximum timeframes for an internal dispute resolution response
- (f) internal dispute resolution response requirements for multi-tier internal dispute resolution processes
- (g) the role of customer advocates
- (h) establishing links between internal dispute resolution and external dispute resolution
- (i) systemic issues.

References in Regulatory Guide 271 to:

- (a) complaints or disputes were references to CDR consumer complaints; and
- (b) financial firms and financial service providers were references to CDR participants.

Regulatory Guide 271 means Regulatory Guide 271 published by the Australian Securities and Investments Commission, as in force from time to time. It is available at <https://asic.gov.au>.

For further detail about the internal dispute resolution requirements see the [CDR Accreditation Guidelines](#). [Note: A link to the CDR Accreditation Guidelines will be provided]

- Does the applicant have documented internal dispute resolution procedures in place that meet the internal dispute resolution requirements? Yes No

Document required

At the end of this application upload the documented internal dispute resolution procedures.

1. Do the internal dispute resolution procedures cover CDR consumer complaints?
Yes No

A 'CDR consumer complaint' means any expression of dissatisfaction made by a CDR consumer to or about a CDR participant:

- (a) that relates to:
- (i) the CDR participant's obligations under or compliance with:
 - A. Part IVD of the *Competition and Consumer Act 2010 (Cth)*; or
 - B. these rules; or
 - C. binding data standards; or
 - (ii) the provision of goods or services to the CDR consumer by the accredited data recipient with their consent under rule 4.3; and
- (b) for which a response or resolution could reasonably be expected.

See rule 1.7(1) [CDR Rules](#).

2. Do the procedures meet the AS 10002:2014 – *Guidelines for complaints management in organizations* to the extent required by Regulatory Guide 271? Yes No

3. Do the procedures set out requirements for responding to complaints or disputes within appropriate time limits? Yes No

If yes, please specify which internal dispute resolution procedure this is contained in, including the paragraph or page reference. *Enter text*

4. Do the procedures set out the types of remedies available for resolving complaints or disputes? Yes No

If yes, please specify which internal dispute resolution procedure this is contained in, including the paragraph or page reference. *Enter text*

5. Do the procedures require a final written response to complainants within a maximum of 30 days? Yes No

If yes, please specify which internal dispute resolution procedure this is contained in, including the paragraph or page reference *Enter text*

6. Do the procedures contain a requirement to inform complainants of their right to take their complaint to a recognised external dispute resolution scheme for the CDR in relation to the matters required? Yes No

If yes, please specify which internal dispute resolution procedure this is contained in, including the paragraph or page reference *Enter text*

7. Provide details (name, email and phone number) of the person responsible for the internal dispute resolution procedures of the applicant, including the title of the person (for example, Chief Executive Officer or complaints manager)? *Enter first name, last name, title, email address and phone number*

CDR participants are also required to include in their policy on the management of CDR data information about their internal dispute resolution procedures. If accredited a hyperlink to the policy on the management of CDR data will be required to be published on the applicant's entry to the Register of Accredited Persons. Further information on developing a CDR policy can be found on the Office of the Australian Information Commissioner website.

Accreditation criteria

Reference number XX

External dispute resolution

The applicant must be a member of a recognised external dispute resolution scheme.

The Australian Financial Complaints Authority is the recognised external dispute resolution scheme for the banking sector.

Is the applicant a member of the Australian Financial Complaints Authority or a person who has applied for membership of the Australian Financial Complaints Authority?

Yes No

If yes

- membership number (if currently a member) or application number. *Enter number*
- date membership commenced (if currently a member) or application submission date. *Enter date*

Finalise application

Reference number XX

Related applications

Are there any applications by companies related to the applicant that you would like considered at the same time as this application? Yes No

Please provide details about all other applications that you would like considered at the same time as this application.

1. Applicant name. *Enter name*
2. Application number (if available). *Enter number*

Finalise application

Reference number XX

Documents

Please upload the following documents in support of your application:

[Note: a tailored list of the documents that are required to be uploaded will be generated. The generated list will depend on the answers you provided in response to certain questions.]

General information

1. The applicant's corporate structure chart (if applicant is a body corporate)
2. The applicant's organisational chart
3. Signed fit and proper person declaration for each associated person identified in the application by the applicant
4. The applicant's financial statement from the last financial year (or latest draft)
5. Document setting out worked example(s) of how a business/individual customer would use the applicant's product/service(s)

Information security

If assurance report then

6. The applicant's assurance report on its ability to satisfy the information security obligation

If ISO 27001 then

7. ISO 27001 information security management system certificate
8. Information security management system internal audit report
9. Statement of applicability describing the current state of the applicant's environment
10. Reduced scope assurance report

If PCI DSS then

11. Latest PCI DSS Report on Compliance
12. Latest Quarterly Network Scan
13. Latest PCI DSS Attestation of Compliance Form
14. Reduced scope assurance report

If ATO Framework then

- 15. Latest ATO Digital Service Provider Operational Security Framework letter of confirmation
- 16. Reduced scope assurance report

Insurance

- 17. Statement signed by an authorised representative of the applicant detailing how the applicant satisfies the insurance obligation

If relying on an insurance policy

- 18. Policy document for insurance policy [*Note: for each policy relied upon*]
- 19. Certificate of currency for insurance policy [*Note: for each policy relied upon*]

If relying on a consumer guarantee

- 20. Evidence of the comparable guarantee

Internal dispute resolution

- 21. The applicant's internal dispute resolution procedures

Additional documents

If you have any additional supporting documents related to this application, please upload here.

The maximum upload file size allowed for each document is 24MB.

Finalise application

Reference number XX

Review

Please review the information you have provided and amend if required. *Note: a link will be provided to the user and organisation profiles previously provided.*

Finalise application

Reference number XX

Submit

Before submitting your application, please check that the details we have about you and the applicant are correct and make changes where necessary. *Note: a link will be provided to the user and organisation profiles previously provided.*

In particular, please check the applicant's addresses for service are correct.

If the applicant is a foreign entity, please check that the applicant's local agent's details and the local agent's addresses for service are correct.

Is there anything additional you want to tell us before you submit your application? For example, information that may assist with the assessment of your application, or further information of interest. *Enter text*

Declaration

I declare that all the information I have given on this application, including any attachments, is complete and correct.

I understand that, if accredited the applicant will be required to comply with all the obligations of an accredited data recipient but a number of requirements will still need to be met in order to be made active on the Register, including passing the conformance test suite and issue of PKI certificates.

WARNING

It is a serious criminal offence under the Commonwealth Criminal Code to provide false or misleading information. False or misleading information in an application (including a material omission) may also be grounds to revoke any accreditation granted based on that information.

Submitted

Reference number XX

Your application for accreditation has been submitted. We may follow up to discuss details of your application or request additional information.

Your application number is [*Note: reference number will be provided*].