



CDR Accreditation, Sample Application Form: Unrestricted Level (Full)

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

October 2022

Starting your application

This is an application for [*your entity's name will be displayed here*] to be accredited as an accredited person, at the unrestricted level, for the CDR. We recommend you read our [CDR Accreditation Guidelines](#) 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 with the [ACCC/AER Privacy Policy](#).

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 Regulation Authority, the Australian Securities and Investments Commission, the Australian Financial Complaints Authority, the Information Commissioner, the Australian Energy Regulator and the Essential Services Commission of Victoria) 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 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

You must tick yes to proceed with the application.

Once you choose to continue from this point an application is generated with its own unique reference number and will be displayed on each subsequent screen.

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? [Drop down box: 0-4, 5-19, 20-199, 200+]
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: [text]
 - b. Number of owners/shareholders: [Drop down box: 1, 2, 3,...19, 20+]
 - c. Names and shareholdings of top shareholders/owners (include no more than 5):

Shareholder/owner name	Shareholding (%)

3. Please provide a clear description of the applicant’s current business products/services [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: [number]
 - b. Net profit: [number]
 - c. Return on investment: [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. [number]

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

If yes, please provide the licence number. [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. *[drop down list with option to add]*
- b. Provide any relevant registration numbers (if known). *[alphanumerical]*
- c. Provide details of the applicant's use case for that country's regime. *[text]*

Country	Registration number	Description of use case

Options at bottom of page 'previous' and 'save and continue'

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.

Product/service	Business name	Description

For each product/service:

1. What is the name of the product/service the applicant will offer? *[text]*

Business name:

2. Under what registered business name (including any relevant registration number) will the applicant offer the product/service? *[text]*
3. Does the applicant currently offer the product/service?
Yes No

Description column:

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. *[text]*
5. What are the benefits to individual customers/businesses of the product/service? *[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? *[text]*
If no, what is the value to the applicant of providing the product/service? *[text]*
7. Who is the intended target audience of the product/service? *[Check box options - individuals/business/other (please specify)]*
8. How many individual customers/businesses does the applicant intend to service in the first year following accreditation? *[drop down box: <99, 100 - 999, 1,000 - 9,999, 10,000 - 49,999, 50,000 - 99,999, 100,000 - 499,999, 500,000+]*
9. How will the CDR data collected be used to provide the product/service? *[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? *[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. *[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.

Options at bottom of page 'previous' and 'save and continue'

Potential reciprocal data holder obligations

ATTENTION

Upon accreditation, an accredited person may be a data holder if they generate and hold designated CDR data. The obligations of a data holder are to 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.

Banking sector

An applicant will be subject to reciprocal data holder obligations if the applicant generates and holds designated banking sector data in respect of a product that is publicly offered by the applicant to consumers and generally known as one of the types of products in Phase 1, Phase 2 or Phase 3, as outlined in Schedule 3 of the CDR Rules.

For example, when a non-bank lender is accredited, it may have reciprocal data holder obligations in respect of data it generates and holds for its personal loan products. However, an accredited person that provides a budgeting app, but does not offer any products specified by the CDR Rules, will not be subject to reciprocal data holder obligations

What is designated banking sector 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 clause 1.4 of Schedule 3, [CDR Rules](#).

Energy sector

If the applicant is a small retailer, the applicant will become subject to data holder obligations, from either the later of 15 November 2023 or 12 months after the date of accreditation. See clauses 8.6 (7) and (8), Schedule 4 of the CDR Rules.

Who is a 'small retailer' for the purposes of the CDR?

The CDR rules specify that if a retailer, who is below the mandatory participation threshold (i.e., has less than 10,000 small customers), they are a 'small retailer'. Small retailers are not required to participate in CDR as a data holder unless they become an

accredited person or reach the mandatory participation threshold of having 10,000 or more small customers.

A person is a ‘small customer’ of a retailer if the person is:

- a domestic or small business customer of the retailer within the meaning given in section 3 of the *Electricity Industry Act 2000* (Vic) or
- a small customer of the retailer within the meaning of section 5 of the National Energy Retail Law.

In the initial stages of the implementation of CDR in the energy sector, if a small retailer becomes accredited prior to 15 November 2022, the commencement of their data holder obligations will align with ‘larger retailers’ (i.e. 1 November 2023 for non-complex requests and 1 May 2024 for complex requests).

If a small retailer becomes accredited after 15 November 2022, their data holder obligations will commence 12 months (for non-complex requests) and 18 months (for complex requests) from the date they became accredited.

Once a retailer has entered CDR as a data holder, their CDR obligations will continue to apply regardless of whether they subsequently fall below the mandatory participation threshold or are no longer an accredited person.

An applicant who becomes a data holder because of accreditation will also need to register as a data holder in the CDR participant portal. For the energy sector, an applicant has 12 months from accreditation to register as a data holder and become compliant with data holder obligations for non-complex requests and then eighteen months for complex requests.

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

Does the applicant expect to be a data holder as a result of becoming accredited?

Yes No

If yes:

- a. What types of data will the applicant hold as a data holder? *[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? *[text]*

Options at bottom of page ‘previous’ and ‘save and continue’

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:

- (a) 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](#).

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.

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.

Option to add multiple associated persons

Reference number	Name
<u>Unique reference number will be generated for each entry</u>	<u>Display either company name or individual’s first and last name</u>

Questions to be asked for each associated person:

1. Is the person an individual or a company? [single selection, options - individual/company]

If an individual:

- i. Name. *[first name middle name/s and last name]*
- ii. Any other name the person has previously been known by. *[first name, middle name and last name]*
- iii. Date of birth. *[date]*
- iv. Residential address. *address]*
- v. Email. *[email]*

If a body corporate:

- i. Company name. *[text]*
- ii. ACN or registered business number for non-Australian companies. *[number]*
- iii. Country of registration.
- iv. If a body corporate:
- v. Registered business address and email. *[address and email]*
- vi. What is the [individual's/company's] 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). *[text]*

Options at bottom of page 'previous' and 'save and continue'

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 a fit and proper person to manage CDR data having regard to the fit and proper person criteria in the CDR Rules. 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. *[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. *[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?

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)*
- the National Electricity Law
- the National Energy Retail Law

- the *Electricity Industry Act 2000 (Vic)*.

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

Yes No

If yes, please provide details about all contraventions. *[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 \(Cth\)](#)?

Yes No

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

5. Has the applicant, or any of its directors (if the applicant is a body corporate) been disqualified from managing body corporates?

Yes No

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

6. Has the applicant, or any of its directors (if the applicant is a body corporate) been subject to a banning order under the [Corporations Act 2001 \(Cth\)](#)?

Yes No

If yes, please provide details about all contraventions. *[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.

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.

Yes No Not Applicable

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

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)*.

Yes No Not Applicable

If yes, please provide details about all bankruptcy events. *[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 the determination, at the time it was made, recognised under the *Privacy Act 1988* (Cth) or a recognised external dispute resolution scheme?

The [recognised external dispute resolution schemes](#) for the CDR are the Australian Financial Complaints Authority, Energy & Water Ombudsman (NSW) Limited, Energy & Water Ombudsman Queensland, Energy & Water Ombudsman (SA) and Energy and Water Ombudsman (Victoria) Limited.

In addition, the following external dispute resolution schemes are also currently recognised under the *Privacy Act 1988* (Cth):

- i. Energy and Water Ombudsman Western Australia
- ii. Public Transport Ombudsman (Victoria)
- iii. Telecommunications Industry Ombudsman
- iv. Tolling Customer Ombudsman
- v. Credit and Investments Ombudsman
- vi. Financial Ombudsman Service.

Yes No

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

Please [upload a signed declaration from each associated person](#) addressing each of the fit and proper person criteria.

Options at bottom of page 'previous' and 'save and continue'

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

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](#)

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. *[text]*
3. Date of assurance report? *[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? *[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? *[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? *[text]*
11. Please outline the auditor's qualifications and previous experience in preparing equivalent assurance reports. *[text]*
12. Date of reduced scope assurance report? *[text]*
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? *[Number]*

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

c. Control name? *[text]*

d. Please detail the exception. *[text]*

e. Please detail the steps being taken to remediate the exception. *[text]*

Document required

In order to complete and submit your application, you will need to select 'Yes' to and upload the following documents at the end of the application:

- 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

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

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? *[text]*

b. Please detail the exception. *[text]*

c. Please detail the steps being taken to remediate the exception. *[text]*

Documents required

In order to complete and submit your application, you will need to select 'Yes' to and upload the following documents at the end of the application:

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? *text*

b. Please detail the exception. *text*

c. Please detail the steps being taken to remediate the exception. *text*

Document required

In order to complete and submit your application, you will need to select 'Yes' to and upload the following documents at the end of the application:

- 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](#)

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

Options at bottom of page 'previous' and 'save and continue'

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? or
2. by having in place a comparable guarantee?

Document required

[If relying on insurance]

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 [CDR Supplementary Accreditation Guidelines: Insurance](#)

[If relying on comparable guarantee]

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

If relying on insurance:

Please provide information about each separate insurance policy relied upon.

Option to repeat for each nominated insurance policy

Policy type	Policy number	Insurance provider

Questions to be asked for each insurance policy added:

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? *[number]*
3. Insurance provider? *[name]*
4. Expiry date? *[date]*
5. What currency is your insurance in? *[currency]*
6. Annual aggregate amount of cover? *[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. *[text]*

9. Does the policy include awards made by the applicant's designated external dispute resolution scheme(s)?
Yes No

If yes, does the policy have any specific limitations, caps or exclusions in relation to awards made by the applicant's designated external dispute resolution scheme(s)?

Yes No

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

10. Does the policy cover third party liability from breaches of privacy legislation?

Yes No

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

11. Does the policy contain any exclusions relating to privacy legislation?

Yes No

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

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

Yes No

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

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

Yes No

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

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

Yes No

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

Document required

At the end of this application upload both:

- a certificate of currency, and
- the policy document

for each insurance policy relied upon.

If relying on comparable guarantee:

1. Name of guarantor? *[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. *[first and last name, number and email]*

Document required

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

Options at bottom of page 'previous' and 'save and continue'

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.

Is the applicant an energy sector retailer for the purpose of the CDR Rules?

Yes No

An applicant is a 'retailer' if:

- it retails electricity to connection points in the National Electricity Market; and
- it is either:
 - the holder of a retailer authorisation issued under the National Energy Retail Law (as it applies in a State or Territory) in respect of the sale of electricity; or
 - a retailer within the meaning of the *Electricity Industry Act 2000* (Vic).

Clause 1.4 of Schedule 4 of the CDR Rules.

If yes, answer retailer applicant evidence below.

If no, answer general applicant evidence below.

Retailer applicant evidence

An applicant who is a retailer meets the internal dispute resolution requirements if its internal dispute resolution processes satisfy the applicable requirements for the retailer's standard complaints and dispute resolution procedures under the National Energy Retail Law or the Energy Retail Code (Victoria).

The requirements of both the National Energy Retail Law and the Energy Retail Code (Victoria) are that the retailer has in place, and publishes on its website, procedures that are substantially consistent with the Australian Standard AS ISO 10002-2006 (*Guidelines for complaints handling in organizations*) as amended and updated from time to time.

Clause 5.1(2), Schedule 4 of the CDR Rules

1. Does the applicant have documented internal dispute resolution procedures in place that meet the internal dispute resolution requirements?

Yes No

Document required

If yes, at the end of this application please update the documented internal dispute resolution procedures.

2. Are the internal dispute resolution procedures substantially consistent with the Australian Standard AS ISO 10002-2006 (*Guidelines for complaints handling in organizations*) as amended and updated from time to time?

Yes No

3. Are the internal dispute resolution procedures available on the applicant's website?

Yes No

General applicant evidence Schedule 3 and Schedule 4, Rule 5.1, CDR Rules provides that:

In the banking and energy sectors (other than for an applicant that is also an energy sector retailer) 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) policy and procedures
 - (vii) data collection, analysis and internal reporting
 - (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.

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>.

References in Regulatory Guide 271 should be applied as if:

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

For further detail about the internal dispute resolution requirements see the [CDR Accreditation Guidelines](#).

1. 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.

2. 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 the CDR participant's obligations under or compliance with:
- (i) Part IVD of the *Competition and Consumer Act 2010 (Cth)*; or
 - (ii) these rules; or
 - (iii) binding data standards; or
- 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](#).

3. Do the procedures meet the Australian/New Zealand Standard AS/NZS 10002:2014 - *Guidelines for complaints management in organizations* to the extent required by Regulatory Guide 271?

Yes No

4. 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. *[text]*

5. 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. *[text]*

6. 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. *[text]*

7. 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. *[text]*

8. 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)? *[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](#).

Options at bottom of page 'previous' and 'save and continue'

Accreditation criteria

Reference number XX

External dispute resolution

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

Is the applicant an energy sector retailer for the purpose of the CDR Rules?

Yes No

An applicant is a 'retailer' if:

- it retails electricity to connection points in the National Electricity Market; and
- it is either:
 - the holder of a retailer authorisation issued under the National Energy Retail Law (as it applies in a State or Territory) in respect of the sale of electricity; or
 - a retailer within the meaning of the *Electricity Industry Act 2000* (Vic).

Clause 1.4 of Schedule 4 of the [CDR Rules](#).

If yes, answer retailer applicant evidence below.

If no, answer general applicant evidence below.

Retailer applicant evidence

An energy sector retailer that only uses CDR data to provide services in the energy sector may satisfy the external dispute resolution requirement by being a member of the energy and water ombudsman scheme (or the equivalent jurisdictional dispute resolution scheme) for CDR consumer complaints in each jurisdiction in which it operates.

See clause 5.2(3), Schedule 4, [CDR Rules](#).

Please provide details about all jurisdictions in which the applicant operates as a retailer.

Jurisdiction	Member of ombudsman scheme?

Questions to be asked for each jurisdiction added

- Jurisdiction? [drop down list of ACT/NSW/QLD/SA/TAS/VIC]
responses to this question should populate the 'jurisdiction' column
- Is the applicant a member of the energy and water ombudsman scheme in this jurisdiction, or if the ACT is selected, able to participate in a relevant dispute resolution process as per rule 5.3(d) of Schedule 4 of the CDR Rules? [yes/no]
responses to this question should populate the 'ombudsman' column

Does the applicant intend to use CDR data to provide services outside the energy sector?

Yes No

For example, is the applicant an energy sector retailer who intends to use CDR data to provide services outside the energy sector, such as using banking data to provide financial management services?

General applicant evidence

The Australian Financial Complaints Authority is the recognised external dispute resolution scheme for the banking sector. For the energy sector, AFCA is the recognised scheme for all applicants except those energy retailers who will only be using CDR data to provide services within the energy 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. *[number]*
- date membership commenced (if currently a member) or application submission date. *[date]*

Options at bottom of page 'previous' and 'save and continue'

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

if yes

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

Applicant name	Application number

Questions to be asked for each related application added:

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

Options at bottom of page 'previous' and 'save and continue'

Finalise application

Reference number XX

Documents

Please upload the following documents in support of your application:

[To generate a tailored list of the documents that are required to be uploaded will depend on the answers an applicant provides to the previous questions.]

General information

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

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. *[upload]*
18. Policy document for insurance policy. *[upload] [repeat for each policy relied upon]*
19. Certificate of currency for insurance policy. *[upload]*
20. Evidence of the comparable guarantee (if relied on). *[upload]*

Internal dispute resolution

21. The applicant's internal dispute resolution procedures. *[upload]*

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

Options at bottom of page 'previous' and 'save and continue'

Finalise application

Reference number XX

Review

Please review the information you have provided and amend if required.

Options at bottom of page 'previous' and 'save and continue'

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. This must match the applicant's address as registered in the relevant business record.

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.

If accredited, the applicant's addresses for service will be displayed on the Register of Accredited Persons.

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 and satisfy additional requirements for inclusion on the Register of Accredited Persons, 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.

Options at bottom of page 'previous' and 'save and continue'

Submitted

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 *[reference number will be generated]*.