Australian Government

Consumer Data Right

Consumer Data Right Supplementary accreditation guidelines

Information security

25 May 2020

Table of contents

Glossary

Shortened form	Extended form
accredited person	an accredited person is a person who has satisfied the Data Recipient Accreditor that it meets the criteria for accreditation specified in the CDR Rules, and has been accredited by the Accreditor
ACSC	Australian Cyber Security Centre
ACCC	Australian Competition and Consumer Commission
the Act	Competition and Consumer Act 2010 (Cth)
AUASB	Australian Auditing and Standards Board
ASAE	Australian Standard on Assurance Engagements
ASAE 3150	Australian Standard on Assurance Engagements (ASAE) 3150 *Assurance Engagement on Controls* standard
ASAE 3402	Australian Standard on Assurance Engagements (ASAE) 3402 *Assurance Reports on Controls at a Service Organisation*
Controls Guidance	the CDR Information Security Controls Guidance accompanying these guidelines
CDR	Consumer Data Right
CDR data	CDR data is specific information for the relevant designated sector. See section 56AI(1) of the Act. For the banking sector this is set out in Schedule 3 of the CDR Rules.
CDR data environment	the information technology systems used for, and processes that relate to, the management of CDR data
CDR Rules	Competition and Consumer (Consumer Data Right) Rules 2020
CIS CSC	Center for Internet Security Critical Security Controls
CPS 234	Australian Prudential Regulation Authority Cross-industry Prudential Standard 234 – Information Security
description of the system	a definition of the people, processes, technology and controls in place to manage CDR data prepared in accordance with international auditing standards
information security capability	the accredited person's ability to manage the security of their CDR data environment in practice through the implementation and operation of processes, including allocating adequate budget and resources, and providing for management oversight
information security governance framework	the policies, processes, roles and responsibilities required to facilitate the oversight and management of information security
information security obligation	the requirement to take the steps outlined in Schedule 2 of the CDR Rules as detailed in rule 5.12(1)(a) of the CDR Rules
information security policy	a formal document that defines the mandatory requirements for managing information security at the organisation
ISAE	International Standard on Assurance Engagements

Shortened form	Extended form
ISO/IEC 27001	International Organisation for Standardisation/International Electrotechnical Commission 27001 – Information Security Management Systems
NIST CSF	National Institute for Standards and Technology – Cyber Security Framework
NIST SP800-53	National Institute for Standards and Technology – Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations
OAIC	Office of the Australian Information Commissioner
outsourced service provider	a person to whom an accredited person discloses CDR data under a CDR outsourcing arrangement
PaaS	Platform as a service
PCI DSS	Payment Card Industry Data Security Standard
SaaS	Software as a service
senior management	an accredited person's directors, and any person who is an associated person of an accredited person that is a body corporate
SOC	*System and Organization Control*
SSAE	Statement on Standards for Attestation Engagements

1. Introduction

1.1. Overview

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

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

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

(i) misuse, interference and loss

(ii) unauthorised access, modification or disclosure.

This guideline aims to provide information and guidance to accreditation applicants and accredited persons to assist them in meeting the information security obligation and is supplementary to the *CDR Accreditation Guidelines* and the CDR Rules.

Enquiries about applications for accreditation should be directed to the Director, Accreditation, Consumer Data Right Division, at ACCC-CDR@accc.gov.au.

1.2. Information security obligation

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

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

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

- **Part 1:** contains provisions about the overarching governance requirements, the boundaries of an accredited person's CDR data environment, the information security capability and controls program that must be maintained for that CDR data environment, the testing, monitoring and evaluation requirements, and requirements for security incident management and reporting.
- **Part 2:** specifies the minimum information security controls to be maintained by an accredited person as part of its information security capability.

When applying for accreditation an accreditation applicant will be required to provide an assurance report to demonstrate that it satisfies the information security obligation.

---

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

2 CDR Rules, rule 5.12

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

Accredited persons will be required to demonstrate their ongoing compliance with Schedule 2 of the CDR Rules by providing regular assurance reports and attestation statements.[4]

2. Applying for accreditation

2.1. Assurance report

When applying for accreditation, as evidence that an accreditation applicant will be able to satisfy the information security obligation, an applicant will be required to provide an assurance report, from a suitably experienced, qualified and independent auditor.

This assurance report must be:

- a report on the design and implementation of controls as at a date or as at a point in time (often referred to as a Type I report)
- in accordance with the Standard on Assurance Engagements (ASAE) 3150 *Assurance Engagement on Controls* (**ASAE 3150**)[5] (which falls within the ASAE 3000 series of standards), or an accepted comparable standard (see section 2.2 below)
- a reasonable assurance engagement
- conducted by suitably experienced, qualified and independent auditors who are capable of issuing reports either in compliance with ASAE 3150 and the additional supplementary standards defined within, or an accepted comparable standard,
- no more than 3 months old at the time of submission of the accreditation application.

The assurance report must:

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

Where an exception is noted in either design or implementation of a control, ensure that in addition to the report, the applicant includes in its application a response from the applicant's management on the steps it intends to take to remediate these deviations/ exceptions and the expected timeframe to complete such steps. It is expected that these

---

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

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

responses will include what reasonable steps will be taken to prevent such occurrences in future.

2.2. Accepted comparable standards

Alternatively, an applicant may provide an assurance report prepared according to the following comparable standards:

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

If an applicant is providing an assurance report based on one of the above listed comparable standards, the applicant should also provide further information on the location of their data operations for the CDR and why they have not sought to be covered by an ASAE 3150 assurance report. We encourage applicants to discuss this proposed approach with us prior to submission of their accreditation application.

Assurance reports may be issued to satisfy multiple standards in order to satisfy different requirements. For example, where an applicant has data operations both within and outside of Australia they may provide a combined assurance report prepared according to both ASAE 3150 and the ISAE 3000 series (or SOC 1/SOC 2 under SSAE standards). If an applicant is relying on an assurance report prepared to satisfy multiple standards for the purposes of the CDR, the assurance report should clearly specify which standards it has been prepared in accordance with.

2.3. Utilising existing assurance reports

When applying for accreditation, an applicant may seek to use an existing assurance report prepared in accordance with ASAE 3150, or one of the accepted comparable standards listed in section 2.2 of these guidelines. The existing assurance report must meet the requirements outlined in section 2.1. However, the Data Recipient Accreditor will generally accept as part of an accreditation application an existing assurance report that contains partial coverage over the required controls in Schedule 2 and is no more than 6 months old at the time of submission of the accreditation application subject to the treatments below:

- If the existing assurance report contains partial coverage over the required controls in Schedule 2 the remaining controls in Schedule 2 of the CDR Rules will need to be assessed in a separate assurance report that satisfies the requirements of section 2.1 of these guidelines. Both assurance reports must be submitted when applying for accreditation.
- If the existing assurance report does not directly relate to the CDR data environment common controls that apply to all systems within the organisation may be leveraged if these also apply to the CDR data environment. Those controls which are specific to the CDR data environment would then need to be assessed in the separate assurance report. Both assurance reports must be submitted when applying for accreditation.
- If the existing assurance report does not fully address how the accredited person takes all the steps required by Part 1 of Schedule 2 of the CDR Rules when applying for accreditation the applicant can submit other documentation that addresses how the accredited person takes these steps.

Examples of potential scenarios and required treatment are provided below.

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

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

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

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

Company XYZ will need to identify those controls specified in Part 2 of Schedule 2 of the CDR Rules that are not covered in its existing assurance report and prepare a separate ASAE 3150 assurance report for these remaining controls, and to address how Company XYZ takes all the steps required by Part 1 of Schedule 2. Company XYZ's accreditation application should include both reports.

Example 2: The existing assurance report does not directly relate to the CDR data environment

Company XYZ prepares an ISAE 3402 assurance report for provision to its clients. The assurance report covers all the required controls. However, Company XYZ intends to implement a new application for the storage and processing of CDR data that was not included within the scope of the ISAE 3402 report.

Company XYZ will need to prepare a separate ASAE 3150 assurance report for the required controls which are unique to the new system. Controls that cover all systems (typically those relating to network, governance and data centre) do not need to be included. For example, the ASAE 3150 assurance report will not need to include physical access security if the CDR system will be residing in the same data centre assured under the ISAE 3402 assurance report. However the ASAE 3150 assurance report will need to include password authentication if it is unique to the CDR system. The applicant, in collaboration with its auditor, will need to make a determination as to which required controls will need to be included in the ASAE 3150 assurance report, and which can be relied upon from the existing assurance report.

3. Ongoing information security reporting obligations

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

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

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

3.1.1. Attestation statement

- The attestation statement must:
- meet the criteria for ‘responsible party's statement’, as laid out in ASAE 3150
- include details of changes, if any, to the CDR data environment since the previous assurance report was required to be submitted to the Accreditor.

3.1.2. Ongoing assurance reports

An assurance report for the purposes of maintaining accreditation will be consistent with the requirements of the CDR Rules if it complies with the requirements set out above for an application report save that the report must:

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

3.2. Acceptable auditors

Assurance reports must be conducted by suitably experienced, qualified and independent auditors who are capable of issuing reports in compliance with ASAE 3150, and the additional supplementary standards defined within.

ASAE 3150 contains a concept of the ‘lead assurance practitioner’, who maintains overall responsibility for the assurance engagement, including quality and alignment with certain standards and codes of ethics. The lead assurance practitioner is the person responsible for signing and issuing the assurance report. The lead assurance practitioner should maintain adequate experience and qualifications to meet the required standard of quality in assurance reporting.

3.3. Controls Guidance

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

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

The Controls Guidance does not aim to be prescriptive in the methodology by which an assessment should be performed. Further, it does not reflect the level of detail and complete set of elements that an auditor may require in order to complete their work and obtain assurance under ASAE 3150. An auditor utilising this template will need to use their own professional judgement in determining whether it is fit for purpose given the specific requirements of the entity they are auditing.

Accredited persons may also wish to use the Controls Guidance to conduct their own internal assessment of their ongoing compliance with the information security obligation.

4. Part 1—Steps for privacy safeguard 12

Part 1 of Schedule 2 of the CDR Rules sets out the steps for regarding the information security of CDR data.[7]

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

4.1.1. Information security governance framework

The CDR Rules require an accredited person to establish a formal information security governance framework for managing information security risks relating to its CDR data setting out the policies, procedures, roles and responsibilities required to facilitate the oversight and management of CDR data. An accredited person may leverage their existing information security governance structure where this will cover their CDR data environment. An accredited person may utilise existing frameworks, requirements and models in developing their information security governance framework and defining security areas (for example, ISO 27001, NIST CSF, PCI DSS, and CPS 234). Security areas are commonly employed in maintaining the security of data (for example, access security and network security).

4.1.2. Roles and responsibilities

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

4.1.3. Information security policy

An accredited person must have and maintain an information security policy. The information security policy must detail the accredited person's information security risk posture, that is, the exposure and potential for harm to an entity's information assets from security threats, and how the entity plans to address these. It should also set out the exposure and potential for harm from security threats. The policy must also detail how its information security practices and procedures, and its information security controls, are designed, implemented and operated to mitigate those risks. The information security policy should be enforceable,[8] and compliance with the policy monitored. The information security policy should document the various security areas managed by the accredited person.

4.1.4. Review of appropriateness

---

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

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

An accredited person must ensure its information security governance framework, including the definition and assignment of roles and responsibilities, remains up to date and fit for purpose. Updates are required at least every 12 months, or sooner upon either of the following occurring:

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

A material change is one that significantly changes the scope of the CDR data environment, such as the introduction of a new system, the migration of data onto new infrastructure, introduction of a new outsourced service provider, or a change to the terms and conditions of the services provided by an existing outsourced service provider.

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

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

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

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

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

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

As part of the assurance report, the accredited person will be required to document a 'description of the system' in accordance with international auditing standards. This will include defining the people, processes, technology and controls in place to manage CDR data. ASAE 3150 clearly defines what a 'description of system' means,[9] what elements it should cover,[10] what a suitably experienced, qualified and independent auditor should assess for determining if the description is complete and accurate in all respects,[11] and includes an example of what a description of system looks like.[12] Where this description has been reviewed by a suitably experienced, qualified and independent auditor, it is

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

[10] Section 51 of ASAE 3150.

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

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

expected that it will be sufficient for the purposes of documenting the CDR data environment.

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

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

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

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

An accredited person must review and adjust its information security capability in response to material changes to both the extent and nature of threats to its CDR data environment. Such changes could result from the development of new applications, migration to new infrastructure, or engagement of a new outsourced provider. Where no such material changes occur, this review must be undertaken annually.

4.4. Step 4: Implement a formal controls assessment program

An accredited person must implement a testing program to review and assess the effectiveness of its information security capability having regard to the factors set out in clause 1.5(1)(b) of Schedule 2 of the CDR Rules.

For example, in respect of testing the effectiveness of information security controls, a testing process may include independent audits and/or control self-assessments, in which the assessor identifies and assigns the associated control owner, assesses the effectiveness of those controls with respect to any deviations from expected operation, and identifies steps for improving controls. These deviations and remediation measures should be logged, tracked and reported to senior management.[13]

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

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

The expected level of independence and professional skills required for the performance of this testing is dependent upon the form of the test and assessment. For example, audits should be performed in line with generally accepted practices for independence and skill. Control self-assessments should be performed by persons with suitable knowledge and understanding of the controls and their expected operations (technical expertise), but independent from the day-to-day performance and administration of the control to

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

promote impartiality. Well known standards, such as Center for Internet Security Critical Security Controls (**CIS CSC**) and National Institute of Standards and Technology (**NIST**) SP800-53, provide detailed guidance on the performance of security controls for information systems, and may be applied by the accredited person in its development of a testing program.

4.5. Step 5: Manage and report security incidents

4.5.1. General guidance

An accredited person must have formal plans, procedures and practices in place for responding to a security incident, including methods for identifying, classifying and rating the incident, managing the incident through its lifecycle, following appropriate escalation channels, reporting to relevant authorities where necessary, and post-incident review. As part of maintaining and ensuring the efficacy of these procedures, an accredited person must perform periodic testing such as through tabletop exercises or interactive simulations to achieve a base level of preparedness. This testing should occur at least annually, and should occur more regularly where there have been material changes to the accredited persons CDR data environment that would lead to changes in the plans, procedures or practices of responding to a security incident.

4.5.2. CDR data security response plans

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

The accredited person must create and maintain plans to respond to information security incidents that it considers could plausibly occur.

For their CDR data security response plans accredited persons should refer to the guidance published by the Office of the Australian Information Commissioner (**OAIC**) on the reporting of notifiable data breaches.[14] Accredited persons should also report all security incidents, even those of minor nature to the Australian Cyber Security Centre (**ACSC**). For example, such incidents may include, but are not limited to:

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

Reports to the ACSC can be made through the ACSC's online cybercrime and incident reporting tool.[15]

5. Information Security Controls

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

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

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

5.1. Control requirements and controls

In order to be accredited, an accredited person will need to demonstrate that it would, if accredited, be able to meet all control requirements through the audit of their controls environment, and submission of an assurance report. The control requirements will make up the content of this report, with individual controls provided to define the controls expected to be implemented in order to achieve the control requirement.

Failure of one or more control requirements will lead to a failure to be accredited. However, deviations in the effectiveness of individual controls will not in and of itself preclude the Accreditor granting accreditation (potentially with conditions) provided it was of the view that the accredited person would, if accredited, be able to meet all control requirements.

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

5.2. Industry standards

When assessing required controls, industry standards or frameworks that an accredited person has an existing certification against may be able to be recognised by an auditor to the extent they adequately address relevant parts of the requirements. This recognition of controls will also apply to the extent that accredited persons will use outsourced providers who are certified against industry standards (e.g. cloud providers). The term 'accepted industry standards' refers to a set of criteria relating to the standard processes and operations in that specific field. These are the generally accepted requirements followed by the members belonging to an industry. These are not fixed and are expected to evolve as circumstances change.

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

6. Guidance on outsourced service providers

6.1. General guidance

An accredited person may use an outsourced service provider to assist it in providing goods or services to a CDR consumer.[16]

An accredited person may choose to use outsourced service providers such as:

- data centres and backup providers
- SaaS (Software as a service) providers

[16] The CDR Rules do not currently permit entities to collect CDR data on behalf of one or more accredited data recipients, however rules allowing for broader use of outsourced service providers are being further developed and will be subject to public consultation. The consultation process will be announced by a CDR newsletter.

- PaaS (Platform as a service) providers
- cloud based service providers.

An accredited person may be liable for the use or disclosure of CDR data by outsourced service providers, or certain other recipients of that data, by virtue of rules 7.6(2) and (3) of the CDR Rules. Accordingly, accredited persons should consider carefully the terms on which they disclose any CDR data to outsourced service providers.

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

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

Outsourced service providers are not precluded by the CDR Rules from subcontracting, however, the CDR Rules specify various requirements in respect of a CDR outsourcing arrangement (see rule 1.10 of the CDR Rules).

6.2. Application of outsourcing to Part 1 of Schedule 2 Part 1

6.2.1. Treatment in assurance reporting

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

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

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

6.2.2. Assessment of controls performed by an outsourced service provider

Where a control defined in Part 2 of Schedule 2 of the CDR Rules is or will be performed by an outsourced service provider, an accredited person must assess these as part of their formal controls assessment program. This includes assessments prior to on-boarding a new outsourced service provider (during due diligence phase), as well as periodic assessments in line with the inherent risk of the outsourced service provider in regards to the security of the accredited person's CDR data environment. The accredited person may use a combination of security questionnaires, formal control assessments, site visits, or third-party assurance reports (for example SOC2, ASAE 3402 or other comparable standards) in performing these assessments.

Where an accredited person is reliant on information security control testing provided by the outsourced service provider, such as general use third-party assurance reports, the accredited person must assess whether the extent and frequency of controls testing

directly relate to the management of the accredited person's CDR data. Further, the accredited person must ensure that the controls tested align to the control requirements defined in Part 2 of Schedule 2 of the CDR Rules where the performance of a control is outsourced.

6.2.3. Security incidents at an outsourced service provider

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

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