

Consumer Data Right Compliance Costs Review

Report for the
Department of the Treasury

December 2023

© Commonwealth of Australia 2023

This publication is available for your use under a [Creative Commons Attribution 3.0 Australia](http://creativecommons.org/licenses/by/3.0/au/legalcode) licence, with the exception of the Commonwealth Coat of Arms, the Treasury logo, photographs, images, signatures and where otherwise stated. The full licence terms are available from <http://creativecommons.org/licenses/by/3.0/au/legalcode>.



Use of Treasury material under a [Creative Commons Attribution 3.0 Australia](http://creativecommons.org/licenses/by/3.0/au/legalcode) licence requires you to attribute the work (but not in any way that suggests that the Treasury endorses you or your use of the work).

Treasury material used 'as supplied'.

Provided you have not modified or transformed Treasury material in any way including, for example, by changing the Treasury text; calculating percentage changes; graphing or charting data; or deriving new statistics from published Treasury statistics — then Treasury prefers the following attribution:

Source: The Australian Government the Treasury

Derivative material

If you have modified or transformed Treasury material, or derived new material from those of the Treasury in any way, then Treasury prefers the following attribution:

Based on The Australian Government the Treasury data

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the Department of the Prime Minister and Cabinet website (see <https://www.pmc.gov.au/honours-and-symbols/commonwealth-coat-arms>).

Other uses

Enquiries regarding this licence and any other use of this document are welcome at:

Manager
Media Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

Contents

About this report	1
Executive Summary	2
1. Background	7
2. Assessment of CDR compliance costs	11
3. Cost considerations in the regulatory process	18
Annex: Data standards decision proposals	26

About this report

This report presents the results of an independent review commissioned by the Department of the Treasury into compliance costs associated with the Consumer Data Right (CDR) framework. The review's objectives were to better understand the costs to participants of CDR rules and standards and to determine how effectively CDR decision makers evaluate costs and benefits.

The report is based primarily on a series of interviews with industry participants and government agencies over the period October through December 2023, as well as review of recent and proposed changes to CDR rules and data standards. Although the rules and standards have been implemented in both the banking and energy sectors, the banking industry was the major focus for this review, given its much longer operational experience with the CDR to date.

Participants were invited to assist with this review on the basis of confidentiality. As a result, information and opinions that could be considered commercial-in-confidence have been removed from this public version of the report.

Heidi Richards

Independent Consultant, Better Regulation Advisory

Executive Summary

The Australian Government's Consumer Data Right (CDR) framework is an ambitious initiative with far-reaching objectives: to promote open and standardised customer data access, enable new products and services and increase competition across designated industry sectors.

Like any regulatory program, the CDR imposes costs on regulated participants. Given the diverse nature of the entities and systems involved, the vital importance of information security and the concurrent evolution of technology, implementing the vision of the CDR was always going to be complex and costly.

Underlying cost drivers

At this stage, several years into the implementation phase of the CDR for the banking sector, and a shorter period for the energy sector, the costs of the CDR appear to have far exceeded original regulatory estimates. Industry participants have expressed significant concerns about the continued pace of change and the resulting costs. Although this review did not focus on quantifying benefits of the CDR, it was evident that many participants question the cost-benefit justification of ongoing changes to CDR rules and CDR data standards, based on the very low level of usage that they observe among their customer base.

CDR implementation costs have fallen most heavily on Data Holders—those entities that are mandated to share their data with certain recipients. There have been a number of factors contributing to these costs. For the most part, Data Holders did not have systems and data structures in place to meet technical requirements, so very significant systems development work has been required.

There was also limited consistency in how Data Holders define and manage their product and customer data, particularly in the banking sector. CDR requirements did not always align fully with international standards (or such standards were not yet available), which meant that economies from standardised vendor solutions were generally not available.

As a result, cost impacts have varied substantially across the relevant industry sectors. Indicative overall cost estimates across Data Holder implementation activities to date range from under \$1 million to well over \$100 million each.

The four major banks were the first to be covered by the phase-in of the mandatory CDR data sharing requirements beginning in 2020. These Data Holders have the most complex, bespoke technology and extensive product sets and so have, not surprisingly, faced the highest costs. Mid-sized Data Holders tend to operate in-house data systems but also have more limited financial and human resources compared with the major banks. Smaller Data Holders have outsourced most aspects of CDR compliance; their costs are driven mainly by their service providers' fees.

While the initial set-up costs reflected the extensive new technology development and deployment required to meet the CDR's specifications, maintenance costs have remained high, particularly for larger Data Holders, for which ongoing compliance costs appear to have reduced only marginally if at all, since the start of the CDR implementation phase.

CDR data recipients (formally Accredited Data Recipients or ADRs), which are typically fintechs and other businesses looking to provide innovative services using CDR data sharing, also face

compliance costs.¹ Becoming an ADR is voluntary and so bearing these costs is essentially a commercial decision. ADRs participating in this review generally did not express significant concerns about their implementation costs and as a result, this review tended to be more focused on Data Holders.

Cost of regulatory change

Changing regulatory obligations are a major contributor to CDR compliance costs and this was a key theme of the review. The CDR data standards, in particular, are constantly being refined and updated by the Data Standards Body (DSB) based on a community-generated backlog of issues as well as evolving policy and compliance requirements.

The shifting strategic direction, including the prospect of the CDR expanding to include Action Initiation requirements, is also a source of some apprehension within the Data Holder population about further significant implementation costs.²

To illustrate the pace of change, since the CDR 'went live' with data sharing in mid-2020, there have been:

- three major reviews of the CDR framework;
- 16 consultations on legislative and regulatory changes;
- 20 versions of the binding CDR data standards; and
- over 100 formal proposals for changes to the standards.

Limited analysis is published on how costs and benefits to different participants of proposed changes were assessed by the decision makers. This leaves the policy-making and governance process open to criticism.

Costs as barriers to CDR adoption

Ongoing compliance costs may also be contributing to slow adoption of CDR-enabled products and services.

ADRs note ongoing problems in areas such as data quality, customer useability and system responsiveness that they view as hindering their products' adoption and success. The minimal involvement by Data Holders in using CDR data was cited as a key reason for the lack of wholesale improvement. Without ongoing active use of the data, it is very hard to maintain data quality and performance.

Indeed, some Data Holders are actively exploring CDR use cases and are committed to the CDR as an essential component of the modern financial system. Others indicated that their CDR teams are fully occupied implementing ongoing changes to Data Holder requirements. Both Data Holders and ADRs noted that the stringent CDR privacy safeguards, such as restrictions on use of information derived from CDR data, pose barriers to developing potential use cases.

Suggestions for managing costs

Regulated entities are expected to implement regulatory projects within a defined project scope, set timeframes and with strong project governance structures. In contrast, the ongoing pace of technical

¹ References in this report to ADRs generally means specialised businesses that are not Data Holders, rather than Data Holders that have chosen to also act as ADRs.

² Action Initiation refers to the proposed expansion of the CDR to include requirements for Data Holders to act on instructions (such as to make a payment or close an account) through the CDR technical interface.

and policy change that has been a feature of the CDR regime is more consistent with how an agile fintech or technology start-up might operate.

There are opportunities to bring these divergent cultural approaches closer together. The suggestions listed below are aimed at better targeting the industry's investment in the CDR and improving governance to bring stronger collective ownership of the framework.

1. A clear prioritisation process for all CDR standards change proposals, based on transparent criteria and methodology, would promote more efficient use of resources across all participants.
2. While a formal Regulation Impact Analysis process is not necessary for all changes to CDR rules and standards, a more systematic policy impact approach, including explicit cost-benefit consideration, would help target and prioritise regulatory changes. Consultations on CDR rules and data standards should include questions to help quantify costs and benefits of proposed changes. The DSB Chair's objectives could be amended to include having regard to costs and benefits in determining standards.
3. Industry support for future investment in the CDR may be improved with a better understanding of how their feedback about costs has been considered in decision-making. Summaries of themes from submissions and how these were considered in the final rules and standards should be published at the time the decision is made. This information should also be part of the decision-making package provided to the DSB Chair.
4. Changes to CDR data standards would be more manageable for the industry if limited to a small, fixed number of scheduled standards releases per year, with implementation dates providing longer lead times. Changes to CDR rules may need to be aligned to these release dates. The Government would need to accept that this would likely slow down and limit the pace of change and the potential for new initiatives to be rolled out quickly. However, it would promote more effective outcomes and allow industry participants to better plan resources and maximise efficiency of development and testing.
5. Industry participants would benefit from clearer strategic and tactical planning for the CDR. This would allow them to plan and budget for future investment, including developing customer use cases. For example, the CDR agencies could publish a medium-term plan, with strategic priorities and explicit tactical objectives for improving the CDR experience and reducing costs in each industry over the next 1-2 years. This could also serve as a guide in prioritising future rules and standards changes.
6. Given the breadth of the CDR, there is scope for changes to rules and standards and associated enforcement and compliance activities to be more narrowly targeted. Tactical plans could include a focus on delivering a few specific use cases (agreed with industry) per year, that are likely to attract the most consumer uptake and benefit. This would include where appropriate clarifying or streamlining rules, improving testing and customer experience, improving quality of relevant data and refining measures of success.
7. The current Data Standards Advisory Committee (DSAC) could be more effective in providing a representative sounding-board for the DSB Chair. Considerations would include appointing an independent DSAC chair, expanding membership to ensure adequate representation, providing more structured governance and documenting DSAC feedback to the DSB Chair.

8. Technical performance and reporting requirements (non-financial requirements and metrics reporting) have recently been the focus of industry pushback due to high costs and short lead times. A collaborative, data-driven needs assessment could help identify areas where requirements could be removed or relaxed or where there is support for uplift.
9. Provide a permanent exemption pathway for Data Holders to apply for exclusion of legacy, small or highly specialised products or a class exemption for specific products (e.g. closed to new customers, customer numbers below a threshold, low customer benefit or no use case identified).
10. To provide incentives for Data Holders to invest in CDR infrastructure, exploring with industry opportunities for fee-based, voluntary data sets and establish a process for progressing these through rules or standards. This could include an industry working group on value-added CDR data.
11. Formalise a forum for industry to raise business implementation considerations across the Government agencies and discuss possible solutions.
12. Improve the consideration of implementation barriers to avoid unintended consequences by establishing a collaborative approach to industry testing of rules and standards prior to finalisation, through a sandbox, detailed workshops, pilot testing or other approach. The trade-off may be a somewhat slower pace of change.
13. Undertake a review of the CDR rules, in collaboration with industry participants, to identify lower value/higher cost obligations that could be removed or streamlined. Consider providing non-binding guidance or safe harbours, rather than expanding rules to address special cases.

Potential alternative governance models

The feedback from industry participants suggests that it may be timely to reconsider governance arrangements for CDR decision-making to maximise alignment between policy and technical industry implementation. The suggestions above could be implemented tactically, or could be the basis for the Government to consider an alternative governance structure for the CDR. Two different options—developed here only as a starting point and not indicative of the full range and nature of other alternatives, are summarised below.

1. Streamlined regulator-led model

This option would be based on a more centralised, top-down regulatory operating model. Rules and standards changes would be rolled up into a central regulatory process with a small number of well targeted change proposals per industry each year. These would include a Regulatory Impact Analysis detailing the rationale, including public feedback, of each change package.

This approach would be better suited to fewer, longer consultations and a more deliberate, disciplined pace. The benefits would include greater alignment of changes toward Government-wide objectives and outcomes, as well as ability for consumer advocacy groups and small Data Holders to contribute. This option could include regulatory consolidation of responsibilities among the current multiple CDR agencies into one or two regulators.

2. Industry-led governance model

There is a reasonable argument that the directive, highly prescriptive regulatory model needed to kick-start the initial phases of the CDR can now naturally evolve into an industry-led model, with

regulatory backstop and decision authority on key aspects, similar to other open standards organisations and the major payment systems.

Standards responsibilities would be effectively delegated to an industry body such as an expanded, representative DSAC. Some areas currently prescribed in the CDR rules could be delegated to the standards-making body, with baseline requirements remaining in legislation. Technical and administrative support could be provided by industry associations as well as by the existing DSB processes.

1. Background

Objectives and approach

The overall objectives and approach for this review into CDR compliance costs were determined by the Department of the Treasury. The objectives were:

- to help the Treasury better understand the costs for participants associated with the making of CDR rules and standards; and
- to determine how effectively CDR decision makers evaluate costs and benefits.

This report is intended to synthesise the information gathered into insights and key themes as well to provide suggestions that may help reduce compliance costs going forward.

The report is based primarily on a series of 26 interviews with industry participants and government agencies over the period October through December 2023, as well as review of recent proposed changes to CDR rules and standards and public submissions and comments on those proposals. Industry participants included banks and other authorised deposit-taking institutions (ADIs), energy retailers, software vendors, CDR Accredited Data Recipients (ADRs) and industry representative bodies.

The energy sector received limited coverage in these meetings given the very recent implementation of the CDR in that sector. No meetings were held with telecommunications sector or non-banking lending participants.

It should be noted that an assessment of the benefits of the CDR regime was not within the scope of this review. However, to the extent that industry participants mentioned their perception of the benefits to their customers or their own business, these are noted where relevant.

Regulatory landscape

A review of the regulatory structure for the CDR regime is outside of scope for this report.³ However, it is useful to lay out the extent of regulatory change that has occurred since the regime began.

The CDR was legislated in 2019 with a new section of the *Competition and Consumer Act 2010* (the Act) after two years of study and public consultation. The CDR's statutory application has operated on the basis of industry designations, starting with the banking industry and moving to energy retailers in 2023, telecommunications providers (currently on hold) and non-bank lenders (to commence 2024-25). The CDR rules were first issued in 2020 and include general and industry-specific requirements as well as provisions applicable to the making of technical standards.⁴

The CDR has a complex regulatory structure. Rulemaking and enforcement powers were initially the authority of the Australian Competition and Consumer Commission (ACCC), with rulemaking responsibility later shifted to the Treasury. The Data Standards Body (DSB), a government body within the Treasury, was designated to develop technical standards required to implement the CDR.

³ For information on the history, legislative framework, participants and technical operation of the Consumer Data Right, see <https://treasury.gov.au/policy-topics/economy/consumer-data-right> and <https://www.accc.gov.au/by-industry/banking-and-finance/the-consumer-data-right>.

⁴ *Competition and Consumer (Consumer Data Right) Rules 2020* available at <https://www.legislation.gov.au/Details/F2023C00735>.

The DSB Chair is required to make CDR standards as directed by the rules, in consultation with the ACCC, the Office of the Australian Information Commissioner (OAIC) and a CDR-specific advisory committee (the Data Standards Advisory Committee, DSAC).

There are now multiple government agencies which share responsibility for developing regulatory requirements and guidance, and undertaking compliance and enforcement activity. These agencies coordinate regularly through a CDR steering group; however, each has its own authority and responsibilities.

An unusual feature of the CDR regulatory framework is that the provisions of the legislation and the CDR rules are directly enforceable by both ACCC and OAIC, but the data standards are legislated as private contractual obligations. Nevertheless, the standards are viewed as equivalent to regulatory requirements by regulated industry participants.

Implementation of the CDR progressed with an initial intensive period of rulemaking and standards development over 2018-2020. There was strong industry involvement on technical working groups. Since then, it appears that more of the ongoing standards work is done by DSB staff rather than industry working groups.

The DSB has also expanded its research capabilities into the end-user customer experience (CX) as well as experimental use cases. Recently, a formal industry working group has been set up to discuss performance standards (known as non-functional requirements or NFRs), an area where significant concerns about costs have been expressed by Data Holders.

Regulatory change

Nearly all participants in this review expressed the opinion that the extent of ongoing change in the CDR is unlike any other regulatory program to which they have been subject in the past. To illustrate the intensity of regulatory activity, since the CDR data sharing 'went live' in the banking sector in 2020, there have been:

- three major reviews;
- five Privacy Impact Assessments;
- seven sets of revisions to the CDR rules;
- 16 consultations on policy, legislative and regulatory changes;
- 20 version of the CDR standards; and
- over 100 decision proposals for changes to standards.

With respect to compliance and enforcement:

- The OAIC has conducted three assessments, primarily focusing on compliance by ADRs.
- The ACCC has conducted two compliance reviews, including on data quality, in addition to its accreditation and other ongoing operational responsibilities.

During the month of October 2023 alone, the following major consultations were in progress:

- Non-bank lending rules and standards changes (Treasury and DSB)⁵

⁵ *Consumer Data Right rules – expansion to the non-bank lending sector* <https://treasury.gov.au/consultation/c2023-434434-expansion>; *Consumer Data Right rules and data standards design paper for non-bank lending sector* <https://treasury.gov.au/consultation/c2022-341682>; DSB Decision Proposal 318 - Non-Bank Lending Standards. <https://github.com/ConsumerDataStandardsAustralia/standards/issues/318>.

- Consent Review and Operational enhancements design papers (Treasury and DSB)⁶
- Screen scraping consultation (Treasury)⁷
- Authentication uplift proposals (DSB)⁸
- Banking product and account data standards changes (DSB)⁹
- Standards changes to implement v5 CDR rules (DSB).¹⁰

Regulatory cost assessment

Cost-benefit analysis is a traditional lens for public policy and regulation decision-making and is a core component of the Office of Impact Analysis regulatory impact guidance.¹¹

Implementation and compliance costs did not feature prominently in the published decision process to mandate an open data regime in Australia. The Government's 158-page December 2017 *Review into Open Banking* included a section of less than four pages on implementation and compliance costs.¹² While the *Review* report summarised public submissions on the nature of compliance costs, it did not attempt to quantify overall costs, but recommended that implementation costs should be looked at on a sector-by-sector basis. The *Review* suggested some means to reduce costs, such as providing an extra year for smaller ADIs to implement data sharing.

Cost estimates were ultimately developed as part of the Regulation Impact Analyses (formerly known as the Regulation Impact Statement or RIS process) for the CDR rules, legislation and sectoral designation decisions, shown in the table below.

Table 1: Annual Compliance costs - Regulation Impact certification

Sector	Estimate of annual average costs (\$million)
CDR rules (2020)	106
Banking (2018)	87
Energy (2021)	30
Telecommunications (2021)	N/A
Non-bank lending (2022)	16 - 19

⁶ *Consumer Data Right rules – Consent Review and operational enhancements design paper* <https://treasury.gov.au/consultation/c2023-434434-consent>.

⁷ *Screen scraping – policy and regulatory implications* <https://treasury.gov.au/consultation/c2023-436961>.

⁸ DSB Decision Proposal 327 - Authentication Uplift Phase 1 <https://github.com/ConsumerDataStandardsAustralia/standards/issues/327>.

⁹ DSB Decision Proposal 306 - Updates to Banking Product and Account Detail <https://github.com/ConsumerDataStandardsAustralia/standards/issues/306> and Decision Proposal 338 - Updates to Banking Products and Accounts - Binding Standards <https://github.com/ConsumerDataStandardsAustralia/standards/issues/338>.

¹⁰ DSB Decision Proposal 276 - July 2023 Rules | Standards Impacts <https://github.com/ConsumerDataStandardsAustralia/standards/issues/276>.

¹¹ See *Australian Government Guide to Policy Impact Analysis*, March 2023 at <https://oia.pmc.gov.au/sites/default/files/2024-01/australian-government-guide-to-policy-impact-analysis.pdf>.

¹² Australian Government, *Review into Open Banking: giving customers choice convenience confidence*, December 2017 available at <https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking- For-web-1.pdf>.

When the CDR rules were issued in 2020, compliance costs were estimated at \$106 million annually.¹³ The impact assessment for the banking sector conducted in 2018 arrived at a cost estimate of \$86.6 million per year, and regulatory burden for the non-bank lending sector was estimated at \$15.7-\$18.6 million annually.¹⁴

For the telecommunications sector, a sectoral assessment was commissioned by a consulting firm in 2021, which provided detailed cost estimates for large and small retailers to implement CDR data sharing.¹⁵ The Telecommunications cost report also made suggestions to help reduce potential costs. These included, for example, excluding high-cost products such as legacy products and making use of intermediaries to provide standardised solutions.

¹³ "Certification of Risk-like process: Consumer Data Right Rules," 5 December 2019 at https://oia.pmc.gov.au/sites/default/files/posts/2020/02/31_accr_certification_of_ris_process_-_cdr_rules.pdf.

¹⁴ "Regulation Impact Statement - Open Banking Review," 31 October 2018 at https://oia.pmc.gov.au/sites/default/files/posts/2019/06/2_deputy_secretary_certification_letter_-_redacted_1.pdf and "Certification of Independent Review: Consumer Data Right: Non-Bank Lending Sectoral Assessment," 11 October 2022 at https://oia.pmc.gov.au/sites/default/files/posts/2022/12/Certification%20Letter_1.pdf.

¹⁵ "Consumer data right: Telecommunications sectoral assessment: Final Report," November 2021 at <https://treasury.gov.au/sites/default/files/2021-11/p2021-225262.pdf>.

2. Assessment of CDR compliance costs

Overview

According to the ACCC's CDR performance dashboard as at December 2023, there were 111 active Data Holders (including separate brands) in the banking sector and 20 in the energy sector.¹⁶ The extension of the CDR to non-bank lenders (and potentially telecommunications) will bring over 100 additional Data Holders into the mandated CDR regime. Each of these entities faces costs associated with initial implementation of data sharing, and subsequent ongoing costs for maintenance, compliance and further changes to requirements.

Discussions and data provided by industry participants indicates that many Data Holders, including small ADIs, have spent over \$1 million in implementation costs to date. Costs for the largest banks have run to well over \$100 million dollars each. Note that the major banks began their implementation in 2020 or earlier so costs have accrued over a longer time period.

A significant proportion of the implementation costs could be expected to be non-recurring in nature; however, three years after the initial implementation of the CDR in the banking industry, ongoing compliance costs remain significant. This is particularly true for the larger Data Holders, where ongoing costs appear to have diminished only marginally since the initial implementation phase.

Data Recipients generally did not express significant concerns about their compliance costs. However, costs to operate as an ADR, particularly related to CDR privacy safeguards (such as restrictions on use of information derived from CDR data) were cited as a material constraint on developing use cases for customers. ADRs also report expending significant time and effort resolving data quality and system response issues with Data Holders.

Internally driven costs

Technology architecture

The nature of a Data Holder's technology infrastructure has been a factor in the extent of uplift required to meet the CDR's operational requirements. Most Data Holders indicated that their existing core banking systems were not able to support real-time API-based data sharing, with different degrees of architectural change required.

CDR data elements are generally pulled into a centralised database (a 'data lake') that can meet CDR performance requirements (known as non-functional requirements or NFRs). Various chokepoints inherent in this architecture can limit response speeds and other aspects of performance.

Small ADIs are reliant on their core banking vendors, which typically operate as shared service providers. There are two main vendors that service small ADIs. Typically, the vendor maintains the complete technology stack for a limited set of products. These core banking platforms are generally based on older batch-processing technology, whereas the CDR performance requirements mandate real-time responsiveness.

A separate cloud-based CDR layer is generally required to integrate with the core banking system. This CDR layer may not be able to be used for other services due to system design and CDR

¹⁶ The Performance Dashboard is available at <https://www.cdr.gov.au/performance>.

performance requirements, which are higher than what is needed for banking apps and other digital banking services.

Where a separate CDR system vendor is used, the Data Holder or core banking vendor must perform data mapping and integration with the core account systems and databases and keep this mapping up to date as CDR Standards or product features change.

Mid-sized banks typically operate their own core banking system but outsource their externally facing CDR services to specialised CDR vendors. They have less complex systems and product sets than a major bank, but may have complex integration challenges, with a vendor-provided CDR cloud-based layer sitting across and interfacing with other non-cloud bank systems. They may operate across multiple brands without well developed enterprise-wide data management practices. For these Data Holders, setting up and running CDR infrastructure may be equivalent to running an entire additional core banking system.

The major banks have much more complex system architecture and technology stack, often spanning multiple core banking platforms and fragmented supporting systems (some in-house and some vendor-provided). Legacy systems and the impacts of historical mergers and acquisitions further complicate implementing an enterprise-wide CDR capability. Major banks maintain large in-house IT teams, and as a result have had much less reliance on external software vendors.

Within the energy sector, there is considerable diversity, with some Data Holders operating quite sophisticated cloud-native environments while others rely largely on external software vendors.

Product complexity

The number and complexity of products offered by the Data Holder appears to add more than proportionally to the cost of CDR compliance. Data Holders may operate different products on entirely different supporting systems and databases, with different customer account management, communication and authentication methods. Some of these products are the results of historical mergers where products and brands have been deliberately kept separate, or white-labelling arrangements with distributors.

The mid-sized and large banks in particular highlighted the need to evaluate all individual products and their respective systems for each material change to CDR rules and Standards, and perform end-to-end testing for each change. One bank commented that "open banking can break anything," such that even small changes to Data Standards require a full suite of testing across the entire bank.

This aspect is highlighted by the CDR Exemptions Register, which provides current examples of products where Data Holders have been granted temporary exemptions by the ACCC.¹⁷ Products subject to exemptions include:

- margin loans;
- accounts provided under a distribution agreement (white labelled);
- reverse mortgages;
- asset finance;
- regulated trust accounts;
- SMSF property loans; and
- wholesale bailment loans.

¹⁷ ACCC Consumer Data Right Exemptions Register at: <https://www.accc.gov.au/public-registers/consumer-data-right-exemptions-register>.

Some banks indicated that the CDR has actually driven some product rationalisation or led to closure of particular product lines where it was not economic to bring them into CDR compliance.

Human resources

Understanding the CDR framework at a business or technical level requires expert skills, across technology, business processes and compliance.

Small ADIs generally do not employ technical staff and rely on vendors for most aspects of technology operations, including CDR capabilities. They would generally have a very small number of staff responsible for providing project and vendor oversight, board and committee risk and compliance reporting and regulatory liaison.

The core banking vendors servicing small ADIs have technical staff dedicated to ongoing CDR changes. These staff must also monitor and assess proposed changes to CDR data standards. Resources to conduct production testing at both vendors and their clients is generally very limited.

Mid-sized Data Holders generally maintain some dedicated CDR staff resources, but they often use specialised CDR consultants to assess the change impact arising from CDR rules and standards. Internal technical staff are needed to make modifications to core banking and related systems, and to conduct testing; however, these Data Holders generally do not have full-time technology resources dedicated solely to CDR maintenance, relying instead on flexible resourcing across IT projects. This model is particularly susceptible to unpredictable changes or short lead times.

Large banks have very large in-house IT teams; this includes dedicated CDR IT teams. Access to skilled resources is less of a constraint, but resource planning is very important given the complexity and volume of CDR maintenance requirements across the product and technology suite and the need to coordinate across numerous different business units.

Project structure

Internal CDR project structure can be a factor in cost management.

For example, whether a compliance program is administered as a once-off 'project', as a separate business unit or as part of Business-as-Usual (BAU) operations can influence its ability to obtain internal resourcing. Many regulated entities operate with annual compliance budget cycles and where predictability is important in maintaining resourcing. In addition, the community and regulatory expectations for extremely high resilience and stability in bank technology platforms dictate a tightly controlled release and change control process, which requires additional governance overhead but may help reduce unnecessary testing and other costs.

For small Data Holders, CDR compliance generally falls under existing BAU compliance staff responsibility and is not operated as a separate project. Although a vendor may be making all software changes, the Data Holder needs to sign off for compliance oversight purposes and be in a position to seek exemptions or notify the regulator about rectification as needed. Software vendors typically prefer to accommodate a very limited number of software releases during the year and need to manage these closely across all of their clients.

For the mid-sized and large Data Holders, CDR implementation was typically set up as a compliance project, with project-specific governance and budget structures in place. The large banks now have permanent CDR-focused teams, which may operate as project offices, coordinating changes across other business units, but also with responsibility for technical assessment and implementation.

Externally driven costs

Pace and timing of changes

Most Data Holders, and some ADRs cited the constant flow of changes to the CDR technical standards, and to a lesser extent the CDR rules, as the primary driver of their ongoing CDR costs. This 'change overhead' includes analysis, system design, development, testing, and compliance assurance.

In addition to standards changes arising from CDR rules, the DSB runs four rounds of 'maintenance iterations' each year. These are designed to accumulate minor changes and various issues raised by participants into a single package. Other significant change proposals can be released at any time.

- During 2023 to date, seven revised versions of the technical and CX standards were published, similar to the level in 2021 and 2022.
- There were 20 Decision Proposals (DPs) issued for consultation by the DSB during the year (listed in the Annex).
- Three of the 20 DPs related to required changes to CDR rules. In addition, several proposals were issued in anticipation of future changes to CDR rules.

Data Holders reported that both maintenance and more significant changes are unpredictable and require overwhelming resource attention to assess impacts within the few weeks afforded for public consultation. This requires multiple staff dedicated solely to reviewing and commenting on consultation proposals at the vendors and larger Data Holders.

A number of proposed changes were flagged as involving significant work and requiring longer lead times. Commentary on the DSB GitHub site illustrates instances where industry participants requested further justification for a change proposal, suggested industry-level discussions on cost-effective options to resolve an issue or longer lead times for implementation.¹⁸

Products and performance standards

The very broad scope of the CDR across all products and accounts in each industry, as well as usage assumptions in its design has led to arguably disproportionate regulatory focus on special cases. This has led to resources spent addressing situations that may not occur to any regular degree in practice.

Some examples cited by Data Holders include:

- the requirement to make available seven years of data;
- providing data sharing for offline accounts;
- requirements for multiple account selection for business accounts;
- secondary user authorisations;
- data sharing for closed accounts;
- APIs for ACCC performance reporting; and
- displaying a customer's accounts under all of a Data Holder's brands.

¹⁸ The CDR GitHub repository is used by the DSB for public consultation on proposed changes to the CDR Standards, as well as for publication of draft, binding and archived technical Standards. References in this report to GitHub are to the CDR repository at <https://github.com/ConsumerDataStandardsAustralia>. For consultation on proposed changes, see <https://github.com/ConsumerDataStandardsAustralia/standards/issues>.

Some of the complexity results from restrictions that were in fact originally requested by Data Holders, such as requirements dealing with joint accounts. In some cases, rework has been required to provide a reasonable customer experience after implementation experience proved requirements to be impractical.

Consideration of implementation costs

A common theme among both Data Holders and some ADRs is the view that changes to rules and standards are often finalised without a full practical consideration of their impacts. Underlying these changes may in some cases be unrealistic assumptions about Data Holder data architecture, product structure, technical capabilities or consumer behaviour. This can lead to later rework if the change fails to actually fix the underlying issue.

The ACCC Rectification Schedule for implementation gaps provides a snapshot of requirements that proved problematic across the industry, including:

- expanded secondary user functionality; and
- changes to regulatory metrics reporting (GetMetrics).¹⁹

At the same time, Data Holders and ADRs have fairly consistent views on the most costly regulatory changes from an implementation perspective, namely those involving:

- authentication / security protocols;
- NFRs and performance metrics reporting;
- customer account permissions; and
- new or modified products or data items requiring changes to core banking systems.

A common understanding across the industry and regulators of which aspects of the CDR implementation are more or less costly could help promote industry alignment on the feasibility of future changes.

Standardised vendor solutions

Availability of standardised, off-the-shelf vendor solutions reduced implementation costs for many Data Holders. In fact, the smaller Data Holders that are able to rely entirely or mainly on specialised CDR vendor solutions appear to be the least concerned with ongoing CDR compliance costs and report the smoothest implementation experience.

Industry participants generally support consistency with international standards as a way of reducing costs. In the early phase of CDR implementation, there was a perception that the CDR front-ran international standards, such as the Financial Grade API (FAPI) security standards. As a result the initial Data Holders (the major banks) largely built their infrastructure in-house, adding to costs. This cost may be largely historical as more vendor solutions are now available.

However, the continued divergence of the Australian approach in some areas means that international products generally cannot be used and Australian vendors need to rebuild their products to market them overseas. Embedding existing industry standards by reference is an option that was cited that could help maintain alignment and reduce costs.

Vendor reliance also has some downsides. The smaller Data Holders do not generally appear active in responding to consultations, and so may not have a strong voice advocating for their interests.

¹⁹ The ACCC Rectification schedules are available at: <https://www.cdr.gov.au/for-providers/rectification-schedules>.

Software vendors do not necessarily have the same incentives as their clients. Concentration risk is also emerging as a potential future issue in the CDR vendor landscape.

Industry-specific considerations

There is a perception that the CDR rules are designed with a banking-industry focus. Participants in the energy sector have cited aspects of the core CDR rules that do not apply in the same way in the energy sector, for example, joint bank accounts. The non-bank lending sector has also argued in their public submissions that it should not be subject to the banking sector standards.

While there are likely synergies across ADIs and non-bank lenders, each industry needs to be considered separately to avoid unnecessary costs and unintended impacts on consumers in that industry.

Energy retailers point to the redundant expense in implementing CDR for their large corporate customers, which have other existing means of accessing data.

Testing capabilities

Data Holders and ADRs expressed concerns with current expectations and resources for testing. ADRs felt inadequate testing facilities contributes to the data quality and performance shortcomings they commonly see in the CDR data and consent flow. Data Holders, however, are not able to effectively conduct end-to-end production testing without being accredited an ADR. The existing ACCC Conformance Test Suite process is not considered to provide the same level of assurance as end-to-end production testing.

The frequent number of standards changes throughout the year also requires additional testing processes, which could be streamlined if changes were made through a much smaller, controlled set of releases.

There is limited ability to test draft or finalised changes to operational aspects of the CDR rules or technical standards before they become binding. This can lead to unintended consequences and rework being required where rules or standards changes do not result in expected outcomes. For example, some participants asserted that the recent changes to facilitate joint bank account data sharing has not improved the consent success rate for these accounts.

Impact of CDR compliance costs

Operational benefits

The compliance expenditure required to implement CDR has had some benefits for participants in other areas. For example, it has required some Data Holders and software vendors to upskill on cloud-based platforms, which may be useful for them in other projects.

Some Data Holders have used CDR compliance as an opportunity to rationalise legacy products and systems and to implement enterprise-wide data management systems.

Use of CDR data sharing

Data Holder concerns about costs stem in part from the fact that they see extremely low customer usage of CDR data sharing. With more demonstrated value and demand from customers, attitudes toward ongoing investment would likely be different. One mid-sized Data Holder reported having only one active CDR consent. It was noted that a CDR customer consent success rate of only 50-60% was not unusual.

A few Data Holders, including those that have received ADR accreditation, assert that high ongoing compliance costs is limiting their capacity to investigate use cases and other innovative services.

Protocols for sharing of additional data through the CDR for a fee could prompt more investment in use cases, for example, enhanced business data feeds. Fee-based voluntary data sharing is contemplated in the original CDR research and legislation, but has not been pursued while implementation of fee-free data sharing has been underway.

Industry competition

CDR compliance costs may be having an impact on industry competition, but this is very hard to detect and was not the focus of this review.

Mortgage comparison sites are starting to be able to use CDR product-level data to help consumers request discounts on their home loan rates. Recent proposed changes to CDR mortgage data items may help drive more consistent and standardised data definitions. These developments may help improve price competition in the lending market.

The significant costs of CDR compliance could hasten the trend toward small ADIs merging to remain viable. Industry consolidation within the smaller end of the banking industry has been a feature for many years. It was noted that mergers between ADIs could in some cases actually become more difficult due to the complexity in integrating different CDR solutions, particularly where different CDR vendors were used.

3. Cost considerations in the regulatory process

CDR rules

CDR rule-making, now led by the Treasury, follows a standard regulatory policy process: a conceptual consultation paper and opportunity for public submissions, followed by publication of draft rules, and then by final rules and explanatory documentation. There is generally a reasonable time to provide comments and industry participants appear satisfied with their opportunity for input and access.

The Treasury has also begun holding an annual open call for CDR 'rules maintenance' suggestions. Treasury staff are meet bilaterally with industry participants to obtain their input and this process has been well received by industry participants.

Changes to the CDR rules in the last year or so have generally been targeted at expanding access (such as through business consents) and designating new sectors, and so have not imposed significant new obligations or required technical changes for existing participants.

The CDR rules consultation process highlights specific implementation issues. However, consultation papers generally do not ask explicit questions about compliance and implementation costs nor do final decision documents outline how costs were taken into account.

There is a general view that CDR rules changes are often considered in the abstract, without a full understanding of the use cases and business practices. Requirements are not tested in a practical setting before being finalised, and so in some cases have led to expensive rework. The difficulties with joint bank account consents are commonly provided as an example.

Although many provisions are in fact set in legislation, the CDR rules appear to be the source of many of the requirements that participants commonly cite as particularly costly. These include, for example, complex requirements for data sharing involving secondary users and nominated business representatives, among others. The *Schedule 2 Information Security controls* have been described as overlapping with accepted industry standard security certification frameworks.²⁰

Issues raised by industry participants about the rule-making process include:

- difficulty in committing sufficient resources to multiple concurrent requests for submissions on significant policy changes;
- consultations that combine several different rules changes that may not be clearly signalled (for example, the recent rules consultation on non-banking lending also covered material technical changes affecting the banking and energy sectors); and
- changes which seek to address narrow issues through added complexity in the rules.

In addition, some Data Holders expressed significant concerns about the potential costs and risks in the move toward Action Initiation. The complexity and cost of accepting third-party instructions into internal core systems is much higher than for sharing of data. Some Data Holders indicated they would potentially need to rebuild their entire core systems to enable Action Initiation.

²⁰ See the *Competition and Consumer (Consumer Data Right) Rules 2020*, Schedule 2 - Steps for privacy safeguard 12 - security of CDR data held by accredited data recipients.

Case study: Operational Enhancements - August 2023 Treasury proposal

This package of proposed changes to the CDR rules included among other things additional requirements related to secondary users. The proposed solution to an identified problem is an increasingly complex set of logic rules around authorisation, termination of authorisations and blocking of secondary users. An analysis of the specific use of this feature was not provided.

The consultation document asks a series of very relevant consultation questions about impacts of the proposed changes. However, it does not ask for any data on implementation costs, the number of secondary users, or the types of use cases that would benefit secondary user customers. This information would help make a decision about the cost-effectiveness of this proposed change.

Another proposed change is the addition of Insight disclosures for the energy sector. While useful consultation questions are posed, information is not requested on the specific benefits to consumers, the likely extent of usage or the costs of implementation. There is a risk that participants will not provide this information if it is not flagged as being relevant to the decision.

CDR standards

Standards-making process

CDR data standards govern the data items to be shared, technical data exchange protocols, and the flow and wording of customer-facing screens that must be implemented by Data Holders and ADRs. The CDR standards are promulgated via an instrument and public GitHub repository.²¹

While data standards must be consistent with the CDR rules, the DSB has considerable latitude in the details, for example inclusion of individual granular data items, data definitions, specific security techniques and performance standards. Further, relatively small wording changes to standards can have very significant and costly impacts on industry participants.

The standards-making process is deliberately much more fluid and informal than a traditional regulatory rule or piece of legislation. The CDR Support Portal states that:

"The Consumer Data Standards (CDS) are continually under development. Development is conducted openly and in consultation with participants. Participants are encouraged to contribute to the development of the standards by raising issues, providing feedback and requesting changes."

The DSB has needed to move quickly while trying to juggle many competing objectives and perspectives. Industry participants appreciated how the DSB will answer questions and engage with comments on consultation proposals in train. The DSB staff are considered to be technically very experienced and responsive. The standards documentation material on GitHub is well organised and maintained.

²¹ The instrument *Competition and Consumer (Consumer Data Right) Data Standards (No. 1) 2023* is available at <https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/2023-02/Competition%20and%20Consumer%20%28Consumer%20Data%20Right%29%20Data%20Standards%20%28No.%201%29%202023%20executed.pdf>.

Much of the feedback received for this report about the pace and nature of regulatory change related to the relatively recent experience in the banking industry, and to some extent the electricity retailers, with the standards change process. Concerns expressed by industry participants include:

- change proposals not being prioritised based on impact and effort;
- change proposals made without documented evidence of cost-benefit considerations;
- material standards changes made binding without warning or full consultation; and
- lack of an overall timeline or set of priorities, resulting in what is perceived as a fairly ad hoc process.

Governance and decision-making

The CDR standards are made by the DSB Chair under authority provided by the Act and the CDR rules. The CDR rules set out obligations of the Data Standards Chair in deciding to make standards (or changes to standards). These include:

- publishing draft standards for public consultation for at least 28 days;
- having regard to submissions from the public consultation; and
- having regard to any advice from the Data Standards Advisory Committee (DSAC), the ACCC or the OAIC on the draft standards.

Proposals are published as Decision Proposals open for feedback on the CDR GitHub site. Comments are public on GitHub, although some industry participants indicated they also provide private feedback on specific proposals to the DSB, which are not published. A final Decision Paper is then provided to the DSB Chair, and if accepted the changes are incorporated into a new version of the standards.

Decision Proposals typically cover multiple individual changes, sometimes related and sometimes unrelated. In 2023 the DSB has issued around 20 DPs, not all of which progressed to binding standards (see the Annex). DPs may include future-dated obligations, which are included in subsequent versions of standards. It can be difficult for participants to track changes across DPs, current standards and future-dated obligations.

While standards development is an open and fairly transparent process, there are potential gaps that can give rise to miscommunication about the purpose and timing of changes or leave the outcome open to criticism.

The short consultation periods and highly technical content of the consultations means that only a few of the largest participants generally provide public comments. The final Decision Papers often do not fully summarise the feedback provided by industry participants and how this feedback has been addressed in the final decision. Particularly for more controversial changes, demonstrating an effective governance process is important to maintaining industry trust and support.

Under the CDR rules, the DSAC is an important part of the standards governance process, providing an industry view to the DSB Chair. The DSAC is established under the CDR rules and is comprised of industry representatives from the different CDR sectors across Data Holders, ADRs and other experts. The DSAC meets monthly and a discussion summary is published. The DSAC does not currently to have a consumer or privacy representative, as required under the CDR rules.

Case Study: NFRs and Metrics changes

In February 2023, the DSB published a Decision Proposal (DP 288) inviting feedback on enhancements to the non-functional requirements (NFRs). NFRs cover performance requirements such as minimum system speed and response time measures. The paper also outlined potential changes to the regular performance reporting to the ACCC (GetMetrics). In particular, the proposals recommended significant increases in throughput (transactions per second, TPS) standards, and more complex performance reporting on end-user consent flow.

No data was provided to support any of the proposals, but it was noted that the suggestions had been derived from various calls and discussions with participants.

The DP generated significant feedback. Ten Data Holders and their representatives commented, generally raising significant concerns with aspects of the proposals. Only one ADR was actively involved in providing feedback, and while not detailing specific benefits of the changes, recognised the complexity and need to accommodate longer implementation lead times.

One bank that supported aspects of the proposals stated:

"... implementation should be priority-based with appropriate consideration given to the ecosystem's capacity for change and demonstrable consumer benefit. A more predictable change cadence with sufficient lead time for implementation is recommended."

The Australian Banking Association commented:

"We propose an open discussion or workshop with the ACCC regarding their request for additional consent metrics as a way to understand and improve consent drop off rates. The cost and effort to add these metrics, when aggregated across all DHs is significant."

A final Decision Paper was published in June 2023 after several rounds of revisions to the proposals. It noted the significant level of industry feedback that had occurred and that detailed data was provided by some banks. However, this data or analysis was not published. It concluded that the changes were "broadly supported" and that most of the controversial changes were not breaking changes (that is, compatible with earlier versions).

The NFR changes were incorporated into the v1.25.0 of the standards, published in July. TPS tiering became effective immediately, requiring a 50% uplift in throughput performance by the major banks.

The GetMetrics changes were flagged as future-dated obligations, due for implementation in November 2023 and June of 2024. However, the key changes were initially incorrectly drafted as optional. In the meantime, further revised implementation dates were adopted in August based on a request by the ACCC, with GetMetrics changes accelerated to May 2024. A revision version of the standards was published in October to clarify the changes, but retained the original November 2023 implementation requirement.

This outcome led to considerable industry confusion and has resulted in additions to the ACCC rectification schedule.

A number of industry participants stated that they do not view the DSAC as playing an effective, independent role in CDR Standards governance. Good governance practice would suggest that the DSAC should have its advice to the DSB Chair formally recorded, and the matters for which the Chair legally must have regard should be documented in the decision paper on which the Chair bases their decision.

Case study: Updates to Product and Account Detail - DP 306/338

DP 306 was originally published in June 2023, outlining over 20 accumulated proposed changes to product and customer account data. Some changes were originally proposed by Data Holders to accommodate specific products. Other changes were requested by ADRs to improve comparability across products. A request for additional credit card data was made in 2022 by an ADR that no longer operates in Australia. Other changes were requested by a single ADR with no data provided to justify their importance. An assessment of the changes against the CDR rules was not provided.

A number of large and smaller Data Holders commented on the magnitude of systems changes required to implement this proposal. It was not evident how the proposed standards changes were tested to ensure they would address the underlying problems.

A revised proposal (DP 338) incorporating some revisions based on feedback was published in November 2023 and proposed to be made binding sometime in 2024. The DSB noted in this paper:

"As the proposed obligations dates are 9-11 months in the future, minor changes could be expected to be made to the affected endpoints through the Maintenance Iteration process. Such changes may require amendments to be made while retaining the same obligation dates without a version increment, or beyond the obligation dates, with the possibility of a version increment. These changes will be determined on a case-by-case basis through ongoing Standards Maintenance consultation."

Given magnitude of changes, industry participants expressed concern about the ambiguity of the implementation, given the extent of negative feedback and that further rework could result.

From a governance model perspective, positive comparisons have been made to the operation of domestic and global payments organisations, which generally feature a representative board, working groups, clearly defined operating mechanisms and timeframes that ensure that diverse views are considered in developing industry standards, according to predictable schedules. International standards organisations such as the Internet Engineering Task Force (IETF) provide another model for open standards development and governance.

Data and impact assessment

Changes to the technical CDR standards have far-reaching industry impacts on cost and usage of the CDR. Industry participants expressed the view that any proposed change to the standards with operational or systems impacts should be more explicitly informed by data. While some data is undoubtedly considered by the DSB on specific proposals, it was not evident this was a common or systematic approach or that there was an analytical methodology in place.

Decision Proposals and Decision Papers generally include a very brief section on implementation considerations, typically focusing on lead times. From the papers reviewed for 2023, it was difficult to find evidence about how industry concerns about costs and challenges of implementation were addressed in final decision documentation. This is not to say that data on implementation costs and benefits is not considered, but it is not readily apparent how this is done.










For example, the guidance shown below for raising change requests does not suggest the requestor of a change include any data about scale or impact of the issue or problem.

Change request template in GitHub

Add a title

[Descriptive Issue Title]



Add a description

Write Preview H B I  <>  |    |  @   

Description
Brief description of the issue that is leading to the change being required

Area Affected
Describe the area of the standard that is proposed to be amended. This could be one or more API end points or a specific section of the information security profile

Change Proposed
A detailed description of the specific change (or options for change) proposed. The more specific the proposal the easier investigation and consultation on the issue will be

 Markdown is supported  Paste, drop, or click to add files

Submit new issue

Decision Proposal papers often request views on different options but do not explicitly ask for potential implementation cost estimates or information about priority. Industry commentary also often does not address these issues, and there is some evidence of lack of engagement. Comments on some significant proposals on GitHub sometimes seems very sparse. For example, there were no comments from the non-bank lending industry on DP 318 CX standards for Non-Bank Lending.

More generally, GitHub is very useful as a transparent historical repository of change progress, but it is not necessarily conducive to open discussion about costs and benefits. Participants may be reluctant to risk disclosing proprietary information or publicly criticising their peers' or regulators' positions.

In addition, participants noted that a test period for final standards changes would allow the industry to surface any unintended consequences or unforeseen challenges earlier, that normally do not become evident until development work commences. The DSB's recent approach to publish 'candidate standards' may help move in this direction; however, there was some industry confusion evident about what this new process will mean for timing of finalisation of binding standards.

Prioritisation and planning

One of the most common concerns raised in discussion with industry participants about the standards-making process is that proposed changes do not appear to be prioritised based on clear criteria or a coherent forward timeline or roadmap. This can result in marginal and potentially unnecessary changes being considered and unrealistic implementation requirements.

A number of industry participants observed that there could be more filtering of the issues raised through the standards-making process. Their view is that there are proposed changes that may not be justified on a cost-benefit basis, or that are potentially outside the scope of the CDR rules.

The DSB is required to respond to changes to CDR rules, which can have unpredictable implementation windows. However, the majority of changes during 2023 appear to result not from mandated rules changes but from maintenance proposals from participants or from anticipation of future rules changes.

Industry participants were not clear on the process for the DSB Chair to consider whether a proposed change is required by the rules. The rules and Section 56FA of the Act give the DSB Chair quite broad authority to define the "format and description of CDR data." Whether a data item is required by the rules (or merely consistent with it) can be a matter of interpretation.

An example given is a recent request by a Data Recipient to add a flag for a customer being over 18 years old. Some Data Holders felt this type of data would be considered derived or enriched data and so should not be part of the basic CDR data sets, although others felt it could be included.

For any project, prioritisation is difficult without some degree of cost-benefit analysis. However, cost-benefit considerations are not a factor that the DSB Chair is required to have regard to in making decisions.

Cost-benefit assessments could include expectations that proponents of a change indicate how many users will be affected, what the benefit to them will be, what other benefits the requestor may be hoping to gain, whether other participants will also see these benefits or if it is a unique problem. The DSB could then document this information in a Decision Proposal or in a subsequent analysis paper provided as part of the decision package to the DSB Chair to help build industry support on the need for the change.

Timing considerations

Staging of standards changes has also been cited as an area that could be more systematic and controlled. Data Holders are highly regulated and are expected to operate with tightly controlled system development, testing and production release protocols. This generally involves making changes only in limited release windows and testing each change end-to-end. They need to fit the multiple technical standards updates into these release windows, which is not always feasible within the lead times allowed.

It was noted that the major payment card schemes and payment systems operate around a very small number of releases per year. This predictable schedule promotes change discipline and aids in planning and control, which is critical given the high security and resiliency standards of bank systems affected.

The published standards (currently v 1.28.0) include a mix of binding requirements, future-dated requirements, candidate (near final) standards and draft standards. There is evidence of some confusion about which aspects are mandatory or binding, and when.

Industry participants suggested options for the standards process more efficient for all participants, including:

- limiting standards releases to a small number (for example, 2-3 releases) per year;
- adopting criteria to filter out maintenance changes that are not cost-effective for the broader community;
- finalising and publishing change requirements with sufficient and clear lead times (for example, 9-12 months); and
- publishing a medium-term roadmap for future significant changes over the next several years.

In addition, some industry participants are of the view that standards should not front-run rules development, due to uncertainty about final design and timing. Historically, CDR standards development has often run in parallel with or ahead of rules development. The risk is that the process gets too far ahead and creates uncertainty about potential later rework being required.

The current consultations on the non-bank lending sector and buy-now-pay-later (BNPL) products, for example, are not proposed to result in customer account data sharing until 2025. Indeed, little public engagement has yet been observed from the non-bank lending sector, other than at a high level through the industry association. However, there are also reasonable arguments not to delay work starting on standards, provided there is sufficient time to revise the standards depending on the final rules outcome.

Other implementation considerations

A common theme from participants was that both rules and standards do not adequately consider implementation challenges.

In the case of CDR rules, it can be very difficult to assess implementation issues while drafting rules. Regulatory wording tends to be developed based on a somewhat theoretical understanding of consumer behaviour and industry practice based on general discussions with industry participants, rather than a detailed understanding of specific use cases. A more iterative approach involving longer lead-times for testing of rules and standards prior to finalisation could be considered.

Industry participants were interested in having more regular discussions with their peers and regulatory agencies on implementation challenges. The weekly DSB implementation calls are well attended and organised. Questions raised on these calls tend to be narrowly and technically focused, however.

Currently, a CDR Implementation Advisory Committee meets every month led by the Treasury; this forum is seen as a vehicle for updates from agencies rather than discussion on substantive implementation issues. There is scope to regularise this or a similar forum to focus specifically on discussion of implementation challenges and potential solutions.

In general, participants would like to see more collaborative approaches to problem solving, with the new NFR Working Group a step in the right direction.

Finally, some industry participants were concerned that decisions made on a range of technical issues may have broader impacts on how they operate, outside the CDR ecosystem itself. This is not necessarily something to be avoided, but is a complex topic which warrants further consideration as part of the broader CDR strategy.

Examples include customer identity authentication protocols, and the move toward Action Initiation. There are concerns that future CDR rules and standards in these areas could effectively dictate how Data Holders interact with their customers outside of the CDR, and therefore any expansion in scope would need to be considered very carefully.

Annex: Data Standards Decision Proposals

Decision Proposal	Issue date	Industry	Changes proposed	Source of proposed changes
338	16/11/23	Banking, Non-bank lending	Product Reference Data and customer account data changes; BNPL data items	Maintenance and ADR/DH requests CDR rules (draft)
334	24/10/23	All	Dashboard updates	CDR rules
333	24/10/23	All	Business consents	CDR rules
328	13/9/23	Banking, Energy	Number formats, energy billing, energy time format	Maintenance iteration DH requests
327	25/9/23	All	Authentication Uplift - conceptual proposals	DSB, general feedback and security reviews
322	1/8/23	All	Revised GetMetrics implementation schedule	ACCC
320	3/8/23	Non-bank lending	Non-bank lending CX	CDR rules (draft)
318	13/11/23	Banking, non-bank lending	Non-bank lending standards - general feedback	CDR rules (draft)
317	30/8/23	Banking, Non-bank lending	BNPL product and account data	CDR rules (draft)
316	25/7/23	Non-bank lending	Non-bank lending -conceptual approach	CDR rules (draft)
314	11/7/23	Energy	Customer account change date	Maintenance iteration
313	10/7/23	All	Minor changes	Maintenance iteration
306	22/6/23	Banking	Product Reference Data and account data changes	ADR and DH requests
303	26/4/23	All	Changes for OpenID and FAPI 1.0, additions to energy product details, digital wallet payees	Maintenance iteration - DH and ADR requests
302	19/4/23	Telco	General request for Telco feedback	DSB
298	11/4/23	All	Allow encryption of ID tokens until FAPI 1.0	Data Holder
288	25/2/23	All	Request for submissions on enhancements to NFRs and GetMetrics, including changes to TPS, consents	DSB, ACCC
287	10/1/23	Energy	General request for feedback	DSB
281	27/4/23	All	Solar feed tariffs, security-related changes	Maintenance iteration changes
276	22/9/23	All	July 2023 rules impacts - initial consultation	CDR rules

