Australian Government | data standards body

Regulatory Data Standards Development Reforms

Public consultation paper

30 April 2026

Contents

Consultation Process

Request for feedback

The Data Standards Body (DSB) is undertaking a public consultation on its approach to the maintenance and development of regulatory data standards for the CDR and Digital ID. The purpose of the consultation is to invite feedback from interested stakeholders and the broader public.

Generally, unless provided on a confidential basis, submissions may be made public. Upon review of submissions, stakeholders may be consulted regarding publication.

Questions are included throughout the paper as a guide for comments. Interested parties may wish to respond to some or all questions, or comment on issues more broadly. Interested stakeholders are invited to comment on the options discussed in this paper by 5.00pm on 29 May 2026.

To help you prepare your response, we recommend that you:

- prepare your response in Word (DOCX or RTF) format, you can also upload PDF files as an alternative
- read our submission guidelines
- read our privacy policy.

You must agree to our privacy collection statement to submit your response. If you have any issues submitting your response, you can contact us.

Converlens privacy policy

We use Converlens to collect and store your information in Australia. Visit Converlens' privacy policy for more details.

Use of artificial intelligence

Your feedback may be processed using Treasury approved AI products. Microsoft Copilot may be used to assist with preliminary analysis of submissions, such as identifying similarities. No AI will be used without the oversight of a Treasury employee and all submissions will be reviewed by a Treasury employee. For more information on Treasury's AI policy, please see our AI Transparency Statement. The use of AI complies with the policy for responsible use of AI in government and privacy laws.

Closing date for submissions: 29 May 2026

Online	https://consult.treasury.gov.au/c2026-763706
Enquiries	Enquiries can be directed to contact@dsb.gov.au

Introduction

The Data Standards Body (DSB) has been progressing reforms to provide long-term certainty for participants, reduce regulatory burden, and clarify the purpose and role of standards as a regulatory tool. This consultation seeks feedback on proposed changes to how the DSB develops and delivers regulatory data standards, including how their objectives are established, changes impacts assessed, stakeholders engaged and changes rolled out.

The reforms respond to participant feedback and recent review recommendations and aim to deliver a more focused, predictable and transparent approach to standards development and delivery.

The proposed reforms focus on three key areas:

1. **Regulatory data standards[1] purpose and scope:** The introduction of (i) characteristic and (ii) strategic foundations to define what good regulatory data standards look like, clarify their intended impact, and their role within their broader regulatory frameworks. Regulatory standards are one lever used to deliver policy objectives, and the foundations are designed to ensure standards are developed and applied in a way that operates coherently within their broader policy environment(s).
2. **Standards development process**: A refinement of the standards development and delivery approach, which clarifies (i) phases, (ii) engagement points and (iii) evidence and analytical activities to ensure standards changes are progressed through a consistent and transparent process.
3. **Standards publication and implementation**: The introduction of a more predictable publication approach through planned release[2] cadences and, for the Consumer Data Right (CDR), standardised Future Dated Obligations (FDOs)[3], to support implementation and resource planning.

After the consultation closes, the DSB will review all feedback and publish a summary of the outcomes. Agreed reforms will then be built into the DSB's standards development and delivery processes.

Background

The DSB supports the Consumer Data Right (CDR) and Digital ID programs and the role of the Data Standards Chair (Chair) in both, through standards development activities. For further information on the programs, see: https://www.cdr.gov.au/ and https://www.digitalidsystem.gov.au/.

The DSB was established in 2018 to support to the new role of the Chair in making data standards under the changes to the *Competition and Consumer Act 2010* which established the CDR. As the CDR ecosystem has expanded, the data standards have evolved to support new policy directions, address operational issues and respond to emerging security considerations. The iterative approach taken at that time enabled rapid establishment of the CDR framework. However, as the system has matured, the continued pace of change has created implementation challenges and compliance costs for participants.

The 2024 *Consumer Data Right Compliance Costs Review* highlighted the impacts of standards-related changes in a regulatory framework. It recommended improvements relevant to any regulatory data standards development, including on prioritisation, cost-benefit consideration and release management. Similar feedback has been provided to the DSB via other initiatives including participant journey analysis throughout 2025.

In response, the DSB has taken steps to reduce the rate of change and strengthen the governance processes of updating the regulatory data standards. As a result, the number of CDR standards changes has decreased from an average of 16 change decisions (released across 7 substantive standards versions) per year between 2020 and 2023, to 7 decisions (across 4 substantive releases) in 2024 and 9 decisions (across 4 substantive releases) in 2025.

---

[1] See the glossary entry for **Regulatory Data Standards**.

[2] See the glossary entry for **Release**.

[3] See the glossary entries for **Future Dated Obligation (FDO)** and **Obligation date**.

This reduced rate of change has been supported by improvements to the DSB's processes, including:

- The introduction of the Standards Assessment Framework in late 2024, to moderate the scale of change by requiring articulation of the problem, drivers and rationale for each proposed change.
- Revised Consultation Draft and Explanatory Document formats in early 2025, to improve consultation processes and clarity of changes.[4]
- The suspension of further quarterly maintenance iterations from September 2025, to reduce the volume of incremental technical changes.

These improvements intended to provide a foundation for more efficient regulatory data standards development in the CDR. However, their benefits will take time to fully materialise.

Additionally, the *Digital ID Act 2024* commenced on 30 November 2024 and provides for the appointment of a Data Standards Chair responsible for making and maintaining Digital ID Data Standards. To date, the Chair has not made any changes to the Digital ID Data Standards.

In adopting responsibility across multiple digital regulatory regimes, and in the maturing of the CDR as a regulatory regime, this consultation paper proposes further reforms building on the changes implemented throughout 2024-25. The proposed reforms aim to ensure the DSB maintains and develops regulatory data standards fit for purpose across multiple programs through: clarifying the purpose of the standards as a regulatory mechanism; and proposing processes making standards development more targeted, transparent and predictable. These reforms intend to improve long-term certainty and provide assurance of a reduced and proportionate level of regulatory burden for both CDR and Digital ID regulated entities.

Proposed reforms

1) Regulatory Data Standards purpose and scope

Policy objectives

Making regulatory data standards is one of several government activities that can be used to bring about a given policy objective, alongside others such as primary legislation, rules, guidance, convening powers, and communications. Accordingly, the regulatory data standards need to operate in alignment with the broader policy environment of each program. Within that environment, regulatory data standards are utilised to implement technical specificity where it is required to implement data sharing including in areas such as security, interoperability and data uniformity. As one method intended to facilitate the achievement of policy objectives, regulatory data standards are influenced by changes in policy priorities and the broader direction of the government of the day.

Legal and regulatory frameworks

As noted above, the data standards for each of the CDR and the Digital ID regimes are established under legal requirements and perform a function in the regulatory context of each program. Accordingly, the way in which they are developed and their function differs from many industry-based technical standards. For this reason, they are referred to as 'regulatory data standards' in this consultation paper.

The regulatory data standards exist in accordance with the *Competition and Consumer Act 2010* and the *Digital ID Act 2024*. Under these legislative and associated regulatory frameworks:

- The purpose of regulatory data standards is guided by the objects in the Acts;
- The scope of matters that regulatory data standards may cover is bound by the Acts and Rules; and
- The authority to make regulatory data standards is constrained by the standards-making power in the Acts.

[4] See the glossary entries for **Consultation Draft/Exposure Draft** and **Explanatory Document/Statement**.

The *Digital ID Act 2024* and the *Competition and Consumer Act 2010* define their objects as the below. It should be noted that the regulatory data standards play *a* role in achieving the below, together with other government activities across the programs, including rules making, guidance and communications.

OBJECTS	
Digital ID Act	Under s 3(1), the objects of the Digital ID Act are: (a) to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity in online transactions with government and businesses; (aa) to facilitate the inclusion of individuals in digital society by supporting the provision of digital ID services that are accessible for individuals who experience barriers in using such services; (b) to promote privacy and the security of personal information used to verify the identity or attributes of individuals; (c) to facilitate economic benefits for, and reduce burdens on, the Australian economy by encouraging the use of digital IDs and online services; (d) to promote trust in digital ID services amongst the Australian community.
Consumer and Competition Act	Under s 56AA, the object of Part IVD of the Act is: (a) to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently: (i) to themselves for use as they see fit; or (ii) to accredited persons for use subject to privacy safeguards; and (b) to enable any person to efficiently and conveniently access information in those sectors that: (i) is about goods (such as products) or services; and (ii) does not relate to any identifiable, or reasonably identifiable, consumers; and (ba) to enable consumers in those sectors to request accredited persons to give instructions: (i) safely, efficiently and conveniently on behalf of the consumers; and (ii) to service providers in those sectors; for the performance of actions; and (c) as a result of paragraphs (a) to (ba), to create more choice and competition, or to otherwise promote the public interest.

Multiple sets of regulatory data standards sit under the *Competition and Consumer Act 2010* and the *Digital ID Act 2024*. The Acts and associated Rules specify matters that the regulatory data standards may cover.

- *Digital ID Act 2024* – there are two sets of regulatory data standards: the *Digital ID (Accreditation) Data Standards 2024,* which set out the data standards for certain aspects of the voluntary accreditation scheme; and the *Digital ID (AGDIS) Data Standards 2024,* which set out the data standards for certain aspects of participating in the Australian Government Digital ID System.
- *Competition and Consumer Act 2010* – there exists the *Competition and Consumer (Consumer Data Right) Data Standards 2023*, which comprises all of the data standards for CDR entities.

Regulatory data standards foundations

The Data Standards Body (DSB) is proposing to make regulatory data standards changes in alignment with a set of foundations, the draft of which is being consulted on in this paper. The foundations are separated into characteristic foundations and strategic foundations. Both sets of foundations will guide decision making to

ensure changes operationalise current policy intentions, consider trade-offs between foundations, are proportionate, and aligned with existing expectations and requirements of regulatory instruments. Accordingly, these foundations are intended to describe how the standards operate and what they cover to contribute to the programs' policy objectives, and in line with the above noted legislative and regulatory boundaries.

A) Characteristic foundations

Characteristic foundations define what 'good' regulatory standards are, articulating their core characteristics and inherent qualities. These foundations are intended to be high level and have applicability across both CDR and Digital ID regulatory data standards. The proposed foundations include:

1. Harmonisation – the standards should align and set consistent expectations with whole-of-government, industry, and international standards, where possible and appropriate. This includes considerations of potential trade-offs (i.e. dis-harmonisation) across related policy and regulatory settings which may have competing objectives.
2. Efficiency – the standards should minimise complexity and cost in proportion to impact, supporting efficient and convenient implementation and use.
3. Technology neutrality – the standards should promote flexibility by remaining technology agnostic as a default, specifying technologies only where neutrality would not adequately meet a clearly defined requirement or risk.
4. Clarity – the standards should set clear, unambiguous requirements that include explicit signalling where flexibility is allowed.
5. Enforceability and auditability – the standards should set requirements that support independent assessment, verification and assurance.

B) Strategic foundations

The strategic foundations are intended to provide clarity of the content and coverage of the regulatory standards, made under CDR and Digital ID legislative frameworks.

The regulatory data standards are currently limited to specific technical, security, user and privacy-related matters prescribed by the CDR and Digital ID Rules. The emphasis and applicability of the strategic foundations below differs in accordance with the scope of matters permitted to be covered by the data standards in each regime. To that end, some strategic foundations may not currently apply to certain regulatory data standards. For example, the interoperability strategic foundation is not currently covered by the Digital ID (Accreditation) Standards. However, the strategic foundations provide a potential lens for future standards development, which may require rules changes to support boarder or comprehensive standards over time.

While the topics covered in each set of regulatory standards is broadly consistent, the content and policy emphasis on certain outcomes differs across each program. The strategic foundations are applied with nuance across individual programs and across the different data standards within DSB's remit, as outlined below:

Strategic Foundation	CDR	Digital ID	Overarching
User control	The standards should ensure consumers can provide voluntary, informed and express consent for the collection, use and disclosure of their data.	The standards should ensure individuals can provide informed consent, and can withdraw their consent for the collection, use and disclosure of personal information.	The standards should ensure individuals are able to provide informed, voluntary and express consent, and to effectively manage permissions for the collection, use and disclosure, of their data in an accessible and transparent manner.
User experience	The standards should require clear, intuitive, and accessible communication, ensuring consumers can easily understand and engage with CDR processes.	The standards should define simple, consistent user interactions to promote usability and accessibility of Digital ID services.	The standards should require clear, consistent and accessible interactions, supported by intuitive communication to ensure consumers can easily understand, engage and navigate within systems.
Privacy	The standards should set minimum requirements for protecting the privacy of consumer data to be disclosed, including controls that limit disclosure to authorised parties and for explicit uses.	The standards should define minimum requirements to limit the collection, use and disclosure of personal information.	The standards should set minimum requirements for the secure and proportionate disclosure of data, including protections for data confidentiality, restrictions on use to explicit purposes and mechanisms to support minimal and privacy-preserving disclosure.
Security	The standards for security requirements should be the minimum necessary to ensure secure data disclosure and transit.	The standards should define minimum-security requirements to protect personal information used in Digital ID service.	The standards should set minimum requirements to protect data, identify information and credentials, ensuring secure handling and transmission.
Data	The standards should define uniform data schemas and data quality requirements, sufficient to supporting consistent interpretation by diverse service providers.	The standards should define common identity data and data quality requirements to support consistent and reliable Digital ID services.	The standards should define uniform data schemas and data quality requirements, supporting broad reuse and consistent interpretation by diverse service providers.
System performance	The standards should ensure system performance, capacity and reliability is aligned to program objectives and is discoverable.	The standards should ensure the integrity and correct behaviour of identity systems and data across the identity lifecycle.	The standards should support reliable, well-functioning systems across their lifecycle, ensuring integrity, correct behaviour, and sufficient performance and capacity in line with program objectives and operational transparency.

Strategic Foundation	CDR	Digital ID	Overarching
Interoperability	The standards should set minimum interoperability requirements to facilitate communication between participant systems.	The standards should define minimum technical interoperability requirements to enable reliable identity verification using common protocols and data structures.	The standards should establish minimum interoperability requirements, including common protocols, to enable communication between participants.

Practical implementation

Both sets of foundations will be embedded throughout the standards development process, providing a consistent heuristic for decision making and solution design. They will be applied across all stages of the lifecycle, including problem definition, the development of proposed standards changes and the consideration and resolution of stakeholder feedback and engagement. These foundations are intended to provide an enduring reference point, and to help ensure that proposed changes are aligned with policy intention for standards and the program priorities for both the CDR and Digital ID.

The foundations are not organised in any hierarchy and there is no inherent priority expressed between the topics. However, they provide a basis for discussing and examining trade-offs of impacts throughout standards change option analysis. They intend to help demonstrate impacts to policy intent and ensure solutions designed stay grounded in the problem they are trying to solve. For example, if a standards change is considered which does not specify a technological solution, it may be necessary to also consider how a technology-agnostic requirement could be practically enforced by the regulator.

The foundations are intended to be applied to DSB work moving forward, and to be used to assess the extent to which existing regulatory data standards are fit for purpose. However, any work program to align current standards to the foundations will be assessed as part of the DSB process for impact, timing and alignment to program priorities. At this stage, this does not imply a comprehensive overhaul of the current regulatory data standards.

Consultation questions

1. Do the proposed foundations provide sufficient confidence in the intention and role of regulatory standards, and the potential scope of future direction of standards changes? If not, how would you suggest these be further refined?

2. If scope of potential standards changes were limited to these foundation areas, what types of change would you be concerned might be excluded? What program or ecosystem impacts could occur from excluding certain change types?

2) Standards development process

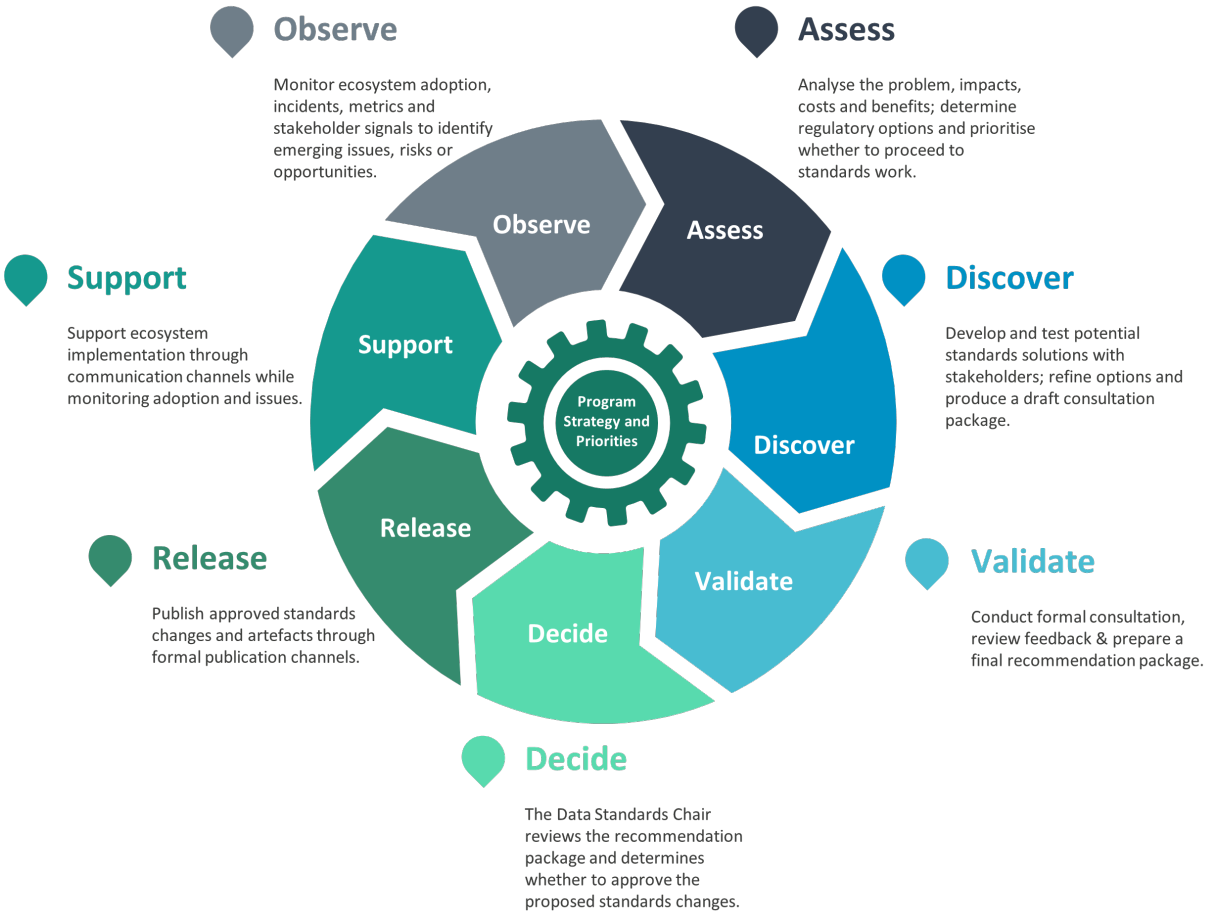
The DSB has developed a standards development and delivery framework to guide how regulatory data standards are assessed, designed, consulted on and released. The framework builds on some existing DSB practices as well as commonly used lifecycles in both policy and tech development. It intends to outline the process by which regulatory data standards are developed, noting that there are varying Digital ID and CDR agency responsibilities with regard to each of the phases below. Many will be done in partnership with policy and legal teams and the DSB will not lead every activity.

The framework provides a repeatable process to standards development, and transparency as to the way in which they are developed. A staged process intends to improve standards change coordination, identification and prioritisation of systemic issues, stakeholder engagement, evidence and analysis, and decision-making.

These phases operate as a continuous lifecycle, with insights from implementation and support activities informing future assessment and identification of potential improvements. However, it should be noted that the process is not often linear and more complex issues may require stages to be undertaken multiple times.

Lifecycle Overview

The standards development and delivery lifecycle framework consists of seven phases:



Observe

The Observe phase involves gathering and monitoring a range of data inputs. This may include implementation experiences, stakeholder feedback and broader regulatory or market developments. This phase involves the initial identification of emerging issues, implementation challenges or opportunities for improvement in the regulatory data standards.

External change proposals and feedback are captured as a part of ongoing observation and evaluated and prioritised during the Assess phase.

Assess

The Assess phase involves in depth analysis of identified systemic issues. This may include proactive targeted evidence gathering and engaging with stakeholders to provide an assessment of the impact on the broader market and Digital ID or CDR entities. This phase intends to develop clear problem definitions in collaboration with policy teams, and clear benefits articulations of addressing the problem.

Problems will be prioritised with CDR or Digital ID policy and regulatory agencies. Where prioritised, exploration is undertaken across relevant agencies to identify the potential government activities that may best address the defined problem (e.g. rules, standards, guidance, support services, regulatory activity).

These alternatives to standards change options will be fully considered before progressing any standards changes. The intent is to ensure the DSB only progresses standards change options where there is a clear problem definition, a demonstrated need for standards changes as the most appropriate mechanism, and alignment with program and policy objectives.

Discover

The Discover phase begins once a valid problem has been identified and standards changes are likely required. The DSB works with program agencies, industry participants and public interest stakeholders to explore design options and develop standards-based solutions.

Activities may include collaborative design workshops, technical analysis, preparation of design papers and cost-benefit analysis to understand impacts and compliance considerations of potential changes. Early participation is encouraged to ensure diverse stakeholder perspectives are considered to refine standards changes before progressing to formal consultation.

Validate

The Validate phase involves structured engagement to test designed standards changes and gather feedback from stakeholders. This includes a public consultation on the proposed change and may involve follow-up targeted engagement depending on the scale, complexity and impact of the change.

Validation activities focus on confirming feasibility, identifying unintended consequences and refining proposed approaches prior to decision-making. Consultation materials will outline the analysis of options, proposed changes and consultation questions, and opportunities to provide submissions will be accessible to all stakeholders. Feedback and evidence gathered during consultation will be analysed to inform and rationalise the recommendation provided to the Data Standards Chair in the Decide stage.

Decide

The Decide phase involves finalising proposed standards changes and preparing a decision package for the Data Standards Chair. This package sets out the recommended solution, supporting rationale, summary of consultation and engagement, and relevant supporting materials such as explanatory documentation. The Chair then determines whether to approve the proposed changes, based on the evidence gathered throughout the lifecycle and in accordance with legislative responsibilities.

Activities in this phase may include preparing Decision Document[5] (CDR) or legislative instrument (Digital ID), confirming implementation arrangements (e.g. FDOs in CDR) where applicable, and communicating outcomes to stakeholders. Decision Documents or instruments may also be published to provide early visibility of approved changes that are expected to be included in upcoming releases.

Release

The Release phase involves approved changes being incorporated into the consolidated regulatory standards in the next scheduled release window or publication date. For CDR data standards, the standards release is accompanied with updated artefacts such as change logs, version history and the obligation date schedule. Compilations of the Digital ID data standards are published in the Federal Register of Legislation. Approved changes may be grouped into planned releases to support predictability, coordinated implementation, and alignment of related or interdependent changes. The new timeframes for publication and obligation dates are explained in more detail in the next section of this paper.

Support

The Support stage involves providing ongoing assistance to participants and other relevant stakeholders to support understanding and implementation of published standards. This may include guidance, clarifications, information sharing and engagement activities. The focus of this stage is to support implementation and identify operational issues in practice.

Insights gathered during support activities contribute to ongoing monitoring and feed into the Observe phase. These insights may inform future improvements to standards, guidance, or other support services.

[5] See the glossary entry for **Decision Document**.

Engagement and evidence approach

At each phase of the lifecycle, the DSB gathers and evaluates evidence to inform decision-making. This may include problem definition, market impacts, expected benefits, trade-offs between other related policy objectives, implementation complexity, compliance and enforceability considerations, cost factors and stakeholder feedback. Evidence gathering begins early and continues throughout the lifecycle to ensure that standards changes are evidence-based and proportionate. A summary of publications which will provide transparency as to the analysis undertaken to justify a problem or a standards change solution throughout the lifecycle is outlined later in this paper.

Engagement activities are embedded throughout the lifecycle and may vary depending on the phase and nature of the issue. Often, engagement activities will seek to gather evidence to be utilised for analysis and design activities. Early engagement may be used to clarify problem definition and validate assumptions, while later consultation focuses on proposed approaches and their associated impacts. Opportunities for open participation will be maintained, alongside targeted engagement where appropriate to support efficient development. The depth of analysis and breadth of engagement will vary, with complex or high-impact changes requiring greater consideration than smaller or low-impact changes.

The table below outlines the purpose of engagement and evidence gathering in accordance with the proposed lifecycle phases, and the types of stakeholders commonly involved:

Lifecycle phase	Purpose of evidence & analysis	Typical stakeholders involved
Observe	Monitor implementation outcomes and behaviour, operational experiences, benefits and disbenefits.	Regulated entities (business and technical) , policy teams and regulators, industry bodies
Assess	Identify issues and undertake analysis of their drivers and scale of impact, and benefits of addressing the issue. Analysis to support policy prioritisation of addressing the issue, and the exploration of solutions across the range of potential government actions.	CDR/Digital ID policy leads and regulators, regulated entities (strategy, compliance, business), industry bodies
Discover	Where standards change is required, detailed design input on draft changes and input on costs and broader non-financial impacts of potential standards change options.	Regulated entities (technical), policy teams and regulators
Validate	Seek all stakeholder views on the proposed standards changes and validate impacts, costs and benefits through formal consultation.	Industry bodies, regulated entities (business and technical)
Decide	Finalise cost-benefit analysis to support the final determination of whether to proceed with, modify or reject proposed standards changes.	Decision authorities within CDR and Digital ID agencies
Release	Determine implementation readiness insights and confirm quality and completeness of standards changes, and implementation tools for CDR data standards.	Regulated entities (technical)
Support	Gather ecosystem insights relevant to support services (guidance, tooling, support portals, etc) and identify emerging issues or feedback for suggested future improvements.	Regulated entities (technical), regulators

Cost-benefit analysis

The DSB will strengthen consideration of both financial and non-financial costs associated with implementing a standards change and maintaining CDR and Australia's Digital ID System. Cost-benefit analysis will consistently form part of the DSB's evidence-based approach to assessing proposed standards changes, considering the nature, size and distribution of impacts. This analysis will primarily be undertaken during the Assess and Discover phases of the lifecycle:

- The Assess phase involves an assessment of (i) the impacts of a particular issue to the market and regulatory ecosystem participants and risks of not addressing the issue, and (ii) articulation of the benefits in addressing that issue supporting the objects of the Act and Rules, policy objectives, and proposed standards foundations as outlined above.
- The Discover phase involves a standards change being designed and drafted. The DSB undertakes a more detailed impact assessment, concentrating on the direct costs (including both financial and non-financial impacts) of implementing the proposed changes, and informs the development of potential solutions.

To uplift the impact assessment process, a preliminary set of cost factors has been identified below. These are grouped into three overarching categories: technical and operational costs, compliance governance and regulatory costs, and vendor and supplier costs.

Technical and operational costs	Compliance, governance and regulatory costs	Vendor and supplier costs
• Technical implementation and systems uplift • Architectural and integration complexity • Data management and maintenance • Testing requirements and meeting non-functional requirements • Security and assurance lifecycle costs, including security uplifts • Operational impacts, readiness, and training at scale • Transition, change management, and decommissioning efforts • Consumer-facing changes and brand impacts	• Compliance and governance requirements • Legal costs • Costs from industry-specific regulatory changes • Cumulative impact from regulatory churn and late changes (rework) • Cross-program impacts • Engagement in standards development • Expertise contributed to Treasury, DSB, and related projects	• Vendor engagement • Discovery costs • Resourcing impacts and opportunity costs • Third party costs, including white label arrangements

Within the CDR in particular, impacts of standards changes have varied widely and, in cases, has been dependent on a number of entity-specific factors. Due to limitations in the availability and quality of financial cost data, the DSB will conduct targeted engagement to ensure analysis is as rigorous and representative as practicable. Cost-benefit analysis will consider stakeholder inputs on all relevant cost factors, including where input is incomplete or provided in confidence. This evidence will inform decisions on the development and design of standards changes, ensuring the expected regulatory burden is proportionate with the policy objectives and Act and Rules objects. The DSB is open to further refining cost types or categories to aid stakeholders in providing as high-quality feedback as possible.

Use of the GitHub platform in the CDR context

To date, the DSB has used GitHub as a platform to: (i) host the CDR data standards; (ii) allow stakeholders to raise issues (change proposals) on a publicly available backlog; and (iii) consult with stakeholders on proposed changes and publish Decision Documents. GitHub has enabled effective engagement with members of a technical audience, who are familiar with the platform. However, GitHub is less accessible to a non-technical audience which are increasingly more involved in the assessment of changes to the CDR system as it matures.

i) Hosting the CDR data standards

The DSB is considering how the CDR data standards can be presented and structured to better support the needs of a diverse range of stakeholders in response to independent reviews and evidence of user needs. Any such changes would be subject to consultation and are not intended to alter regulated entities' obligations or introduce additional compliance burden or costs. Specific implementation solutions, including the consideration of alternative hosting platforms to GitHub, are outside the scope of this consultation paper.

ii) CDR issues backlog

The DSB is currently reviewing and analysing items in the GitHub backlog to identify systemic issues with ecosystem wide impacts. Going forward, new issues (change proposals) will be treated similarly – as one source of evidence to understanding underlying systemic issues, their impacts and relevant risks. The DSB will issue a

revised change proposal template in 2026 and encourages participants to continue to raise issues. The DSB is seeking views on whether these change proposals should continue to be submitted via GitHub.

Separately, this consultation seeks views on whether a backlog should continue to be maintained publicly. A public backlog would allow stakeholders to have sight of issues brought to the DSB's attention and discuss participant-identified solutions or alternative approaches in lieu of a standards or other government-led change. However, if maintained publicly, the backlog items would *not* represent issues that the DSB is committed to resolving. These issues would be progressed through the above-mentioned standards development process and in alignment with policy priorities, the legislative and regulatory frameworks, and standards foundations.

iii) Consulting on standards changes

The DSB has received feedback that GitHub is difficult to navigate to identify consultation activities and creates additional channels to monitor across broader financial sector regulatory consultations. Stakeholders have also expressed concerns regarding the ability of participants to engage each other in consultation submissions.

The DSB will move to publishing formal consultations on the Treasury consultation platform and continue the ability to submit confidential submissions. The DSB will notify stakeholders that the consultation is open through raising a GitHub issue and associated DSB communications channels including news on dsb.gov.au and regular newsletters and engagement forums. The DSB will also publish outcomes of the Assess phase on dsb.gov.au.

Consultation questions

3. Does the proposed standards development framework provide sufficient clarity on how issues are identified, analysed, and addressed? Are there areas where additional clarity or transparency would improve your confidence in how decisions are made?

4. Does the proposed approach to stakeholder engagement and evidence gathering support meaningful participation for your organisation? Are there specific improvements or alternative approaches that would better support your ability to contribute?

5. Do you consider the proposed cost (financial and non-financial) factors appropriate and sufficient for assessing the impacts of ecosystem-wide issues as well as proposed standards changes? What additional cost factors, industry specific considerations, or categories of impacts should be included to ensure a comprehensive assessment?

6. How would you like to raise issues or change proposals in the CDR and Digital ID? What benefits and risks do you see in maintaining a publicly visible record of such inputs?

3) Standards release and implementation

The following approach introduces change bundling, planned publication cadence and standardised implementation periods (where applicable) to improve predictability for participants and support forward planning, resourcing and coherent implementation. The requirements and approaches to the drafting and release of regulatory data standards differ under the CDR and Digital ID. Separate processes are outlined below.

CDR data standards

Decisions and releases

A CDR data standards release is the publication of an updated data standard consolidating changes from all decisions that the Chair made regarding standards changes made up to that point. Going forward, standards changes will be grouped into targeted releases to support predictability and reduce implementation burden. The scope of each release will be informed and limited by impact, complexity and ecosystem readiness.

Decisions regarding standards changes may be made independently of release timing. These will be published as individual decision documents, which will continue to be made public shortly after approval by the Chair (generally within five working days).

Release frequency

The DSB proposes to reduce the current publication frequency of CDR data standards through the introduction of fixed release windows. Planned frequency would be up to two releases per year, consisting of a mid-year (May) and an end-year (November) release cycle.

More complex changes will take longer than simpler changes, and as such, there is no set timeframe for progressing changes through the standards development framework phases. Standards changes will be scheduled for either a mid-year or end-year release, depending on when the necessary design and consultative activities conclude.

Implementation periods

Obligations associated with a standards change will become effective after an implementation period commencing on the publication date of the data standards release. The length of the implementation period will depend on the impact of the change on participants:

- Low-impact changes will have a 12-month implementation period.
- Moderate-impact changes will have an 18-month implementation period.
- Substantial (or complex) changes will have a 24-month implementation period.

Based on analysis undertaken during the Assess and Discover phases, these change impact categories balance the rationale and urgency for change with the effort required, associated costs, and the impacts on ecosystem participants.[6] Cost and benefit data as outlined in the above sections will be used to inform this assessment. The proposed categorisation of the implementation period will be formally consulted on the Validate phase.

Coordinating release and obligation dates

Obligation dates reflect the decided implementation period, calculated from the publication date of the standards release. As standards release windows are proposed as being set to May and November, associated obligation dates will be set to 31 May or 30 November, depending on the length of the implementation period.

In some cases, it may be appropriate to sequence the publication of substantial and moderate-impact changes. This may allow obligation dates to be aligned or offset by six months, to support effective implementation and manage cumulative impacts.

Exceptions

In rare and urgent circumstances, such as when a critical security, legislative or operational issue arises, the DSB may publish an out-of-cycle release or set a non-standard implementation period. The DSB will take all reasonable steps to avoid such circumstances and, wherever possible, provide early notice of any deviations.

Digital ID data standards

The Digital ID data standards are managed through a separate process and engagement of legal drafting resources through the Department of Finance. Changes to the Digital ID data standards will likely be published no more frequently than annually and will always include the setting of obligation dates.

The Digital ID data standards have only been in effect for a short period and were initially developed to support government, rather than private sector participation, in the Australian Government Digital ID System. Private sector participation is to commence from 30 November 2026. Consequently, the DSB and Finance are considering the extent to which current requirements are appropriate for the system's expansion to the private sector. This process will better inform the required frequency of forthcoming changes and suitability of standardised obligation dates as the system expands and stabilises.

[6] See the glossary entry for **Change impact categories**.

Publication and communication expectations

To date, the DSB has communicated with CDR stakeholders through a number of channels, including regular newsletters, implementation forums, the CDR support portal and GitHub forward views. The DSB is exploring opportunities to improve both the types of information provided and how that information is communicated in order to best assist stakeholders with planning to engage in the development process or planning to implement standards changes.

The DSB is proposing to publish, at a minimum, the artefacts outlined in the below table for both CDR and Digital ID data standards. Further consultation documents will be published as and where relevant to standards development, for example, consultations on the extent of issues across the ecosystem (under Assess) or consultations on the varied options for addressing an issue (under Discover).

Lifecyle Phase	Publication
Assess	**Problem definition document:** Published at the end of the Assess phase to confirm a clear rationale and driver for change, which will proceed to the Discover phase in which standards changes are designed.
Validate	**Consultation Documents:** Published as a package, these artefacts will include the proposed standards changes and supporting explanatory materials that will be subject to the formal consultation process and intended to gather feedback and evidence of impacts from the proposed change.
Decide	**Decision Documents:** Published following the approval of the Data Standards Chair, confirming the standards changes, timing of release and implementation period.
Release	**Standards Published:** Release of standards changes, incorporated into the current version of the standards.

Consultation questions

CDR release windows and obligation dates

7. What risks and benefits do you see in setting a maximum of two standards releases and obligation dates per year for CDR? (Please note that Decision Documents with full standards changes would be published when signed by the Chair)

8. If there are two CDR standards releases per year, are May and November the most effective times of year to support planning periods? If not, what economy-wide standardised times in the planning cycle would be more appropriate?

CDR implementation periods

9. What approaches or criteria could be used to classify and set appropriate implementation periods for the CDR data standards? Please draw on effective practices from other regulatory or standards-based frameworks where relevant.

Publication and communication expectations

10. Do the proposed publications provide enough clarity for your organisation to plan and allocate implementation and compliance resources? If not, what additional information would be most valuable?

Glossary

Change impact categories

Change impact categories are used to describe the relative scale, cost and implementation effort associated with proposed standards changes. Categorisation is informed by objective indicators of implementation effort and cost, interpreted proportionately to account for differences in participant size, capability, and technical complexity. Categorisation is determined as part of the Discover phase, with the allocation of the category is subject to consultation during the Formal Consult phase.

- A **low-impact** change is one that requires minimal implementation effort for participants, involving small and isolated updates to existing systems, processes or user interfaces.
- A **moderate-impact** change requires coordinated system updates, typically spanning multiple components and/or business units, but does not require major redesign or re-engineering.
- A **substantial or complex** change requires major system uplift, integration redesign or the introduction of new operational or data handling capabilities.

Consultation Draft/Exposure Draft

For CDR, the document used for formal consultation during the Validate phase. It sets out the draft standards text.

For Digital ID, the draft standards text is set out in 'exposure draft data standards' or 'an exposure draft'.

Decision Document

For CDR, a document signed by the Data Standards Chair that confirms the final text of the approved standards change. The final standards reflect changes from feedback from formal consultation. The document also specifies the Future Dated Obligation(s) for implementation.

For Digital ID, the equivalent document is the amending legislative instrument.

Explanatory Document/Statement

For CDR, a companion document to the Consultation Draft or Decision Document that provides detailed analysis, rationale, stakeholder feedback (where applicable) and contextual information to support understanding of the proposed or final standards changes.

For Digital ID, explanatory statements accompany exposure draft data standards and the legislative instrument that sets out the standards changes, published in the Federal Register of Legislation. In both cases, the explanatory statements articulate the intention and effect of the standards changes.

Future Dated Obligation (FDO)

A requirement in the data standards that becomes effective on and from a date in the future. The term 'FDO' is sometimes used to refer to the future date (see Obligation date).

Obligation date

The date on which a requirement in the data standards becomes effective. If a requirement in the consolidated data standards is not accompanied by a statement of its obligation date, then the requirement is currently effective. For Decision Documents or legislative instruments that have not yet commenced, the requirement becomes effective on the commencement date or the obligation date (if any), whichever is later.

Regulatory Data Standards

Regulatory standards are mandatory, legally enforceable requirements made under statute—such as Acts, regulations, statutory rules, enforceable codes, and licence conditions. The scope of their application is focused on the regulated ecosystems or programs within specific jurisdictions. Regulatory standards are developed by government as one mechanism to achieve government-agreed policy objectives and are used where they deliver the greatest benefit relative to other policy tools for a technical expression of regulatory requirements. As a tool

specifically designed to support the achieving of policy objectives, they are driven by changes to policy priorities and government direction. Given their application across regulated ecosystems, any changes to the standards can have significant implications for achieving policy and consumer outcomes, and significant implications for a conformant entity's business operations, risk allocation and compliance activity.

Regulatory standards published by the DSB specify technical details for legal obligations, where necessary to enable policy objectives and shift the burden of risk and protect public interest. The regulatory data standards create legally enforceable requirements from a regulatory compliance perspective and as a matter of statutory contract formed by operation of law. This distinguishes these differs the risk nature of regulatory standards from industry-led technical standards where conformance is typically voluntary or commercially driven.

Release

For CDR, the consolidated publication of all approved standards changes at a scheduled date (proposed as May and November).

For Digital ID, the equivalent publication is the compilation of the standards in the Federal Register of Legislation.

Release window / Publication date

For CDR, a Release Window is a scheduled point in May or November (proposed) at which the consolidated data standards are published. The Publication Date is the specific date of that scheduled release. All approved standards changes from the preceding six months are incorporated into the consolidated standards at the Publication Date, and associated Future Dated Obligations are standardised so they are dated 12, 18 or 24 months after this date.