Deloitte.

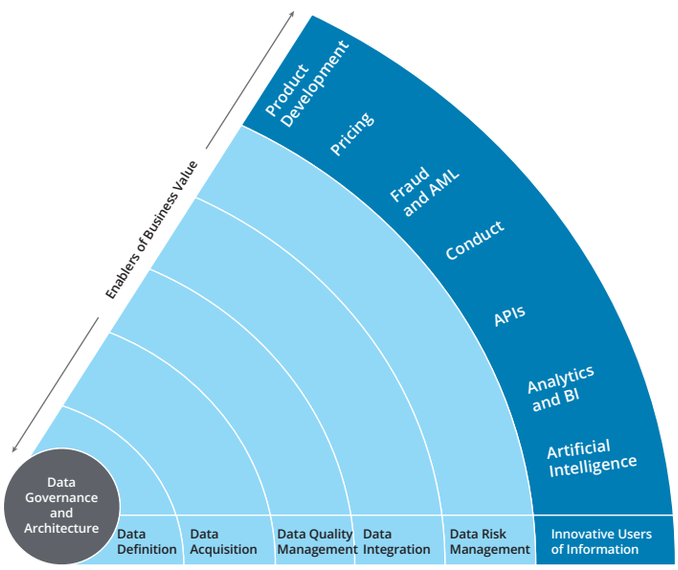
Open banking

Competitive edge through data architecture

September 2018

Data governance and architecture is a tightrope that organisations in the banking sector must navigate to realise the upside of unlocking information silos, and to protect themselves from potential threats in an open banking environment.

Figure 1.0 – Data Governance & Architecture as a critical enabler



Throughout this open banking series, Deloitte has highlighted key dimensions that organisations should consider while preparing for open banking. The topics have been many and varied, however they all share the underlying thread of data.

Australia's open banking regime will be delivered through the introduction of new legislation to establish a Consumer Data Right (CDR). The legislation will be underpinned by a rules framework defined by the ACCC, a designation instrument for the sector, and integration patterns and standards defined by Open Banking's data standards body –Data 61. Market participants will be responsible for delivering the enterprise changes required to both comply and flourish in this new open data environment.

Enterprise Data Governance and Architecture (DG&A) capabilities will be critical when preparing for the inherently complex challenges ahead. Designing and implementing the machinery for managing data throughout this ecosystem will require a considered and focussed approach. This will be further complicated by the incremental rollout and the ACCC's intention to expand the rules over time – which will mean further change management challenges.

APRA's guidelines for Managing Data Risk (CPG 235)[1] – established in September 2013 at a time of global economic uncertainty – elevate the profile and thinking about the way the financial services industry manages its data. Through this framework, many of Australia's leading financial services institutions have made measurable progress in data management maturity – however, a step change is required to unleash new innovative opportunities.

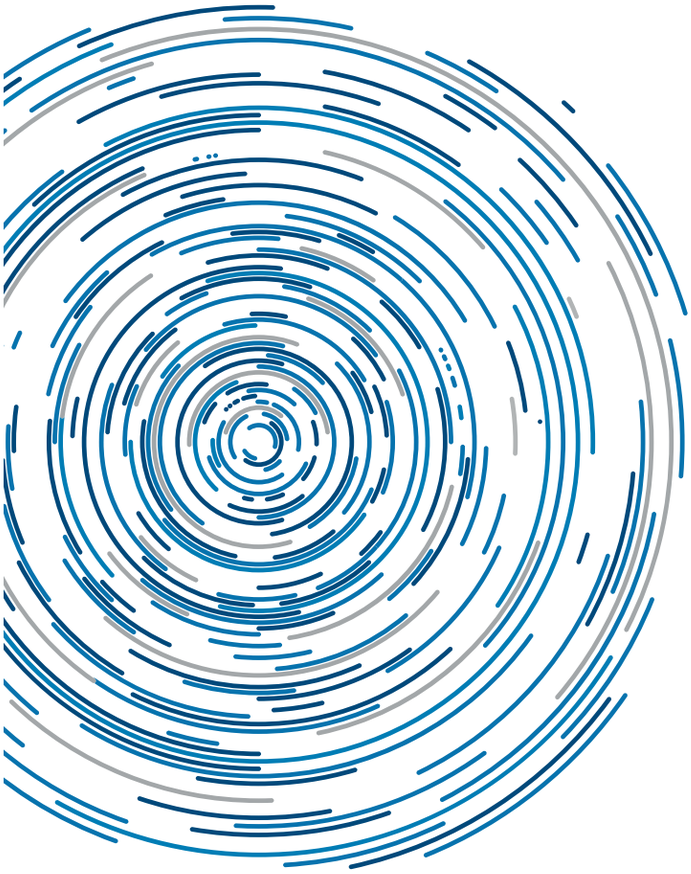
Notes

1. Australian Prudential Regulation Authority, Prudential Practice Guide, CPG235 Managing Data Risk, September 2013. See also https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk_0.pdf

While not a panacea for what lies ahead, CPG 235 is a useful checklist that market participants can use as they consider the readiness of their data governance and architecture for open banking. A useful approach can be to:

1. Adopt a systematic and formalised approach
2. Elevate staff awareness
3. Design for every stage of the data lifecycle including capture, processing, retention, publication, and disposal
4. Consider auditability, de-sensitisation, end user computing (including robotic process automation), and outsourcing/ offshoring of data
5. Ensure that data is fit-for-use
6. Establish a monitoring and exception management capabilities
7. Establish appropriate assurance and review regime.

In addition to these guidelines, the Consumer Data Right Rules Outline[2] contains a number of explicit obligations that should be under-pinned by thoroughly designed and tested data capabilities.



Some key considerations in the rules framework:

- There will be an initial pilot phase for the four major Australian banks where they must make generic product data available on basic accounts from 1 July 2019. They will also need to comply with CDR legislation, rules, and data standards for customer and transaction data on or before 1 February 2020.
- The initial scope for open banking will be limited to active online customers, with off-line customers and historical customers coming into scope in future releases. Australian Authorised deposit-taking institutions (ADIs) will need to consider how they match and merge data across these potentially fragmented data sets within their organisations.
- The ACCC has designated that the initial release of CDR rules will not include 'derived data,' and will not permit fees for data requests. ADIs should consider whether to include these capabilities within their baseline designs to minimise cost and rework, and position themselves to commercialise their data and analytical capabilities in the near future.
- ADIs will also have a streamlined registration process to become accredited data recipients, and so will likely need to comply with the obligations of data recipients as well as data holders.
- The data architecture for both data holders and data recipients will need to manage the complexities of consent including authorisation, authentication, expiry and withdrawal. This may include destroying or de-identifying data in near real time once it is redundant, or can no longer be used for a purpose or for a period for which consent has been received.
- ADIs will need to tailor consent management capabilities (authorisation and authentication) for accounts with multiple authorised parties in contrast to those accounts with a single signatory.
- Customer facing capabilities will need to be developed by both data holders and data recipients to assist customers in managing their data requests and usage; and in the case of data holders, will likely need to integrate into their online banking capabilities.

Notes

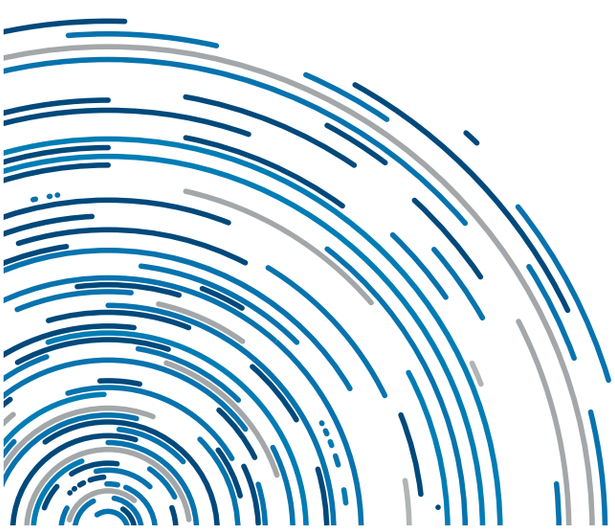
2. Australian Competition & Consumer Commission, Consumer Data Right Rules Outline, December 2018. A complete overview of the draft Customer Data Rules Outline can be accessed from the ACCC website at https://www.accc.gov.au/system/files/CDR-Rules-Outline-corrected-version-Jan-2019.pdf

The Return on Investing in Data Governance and Architecture

An organisation's DG&A needs to be able to respond to the compliance obligations of the CDR legislation and rules. To understand the value of DG&A in an open banking environment it is also important to consider it through the lens of risk and reward.

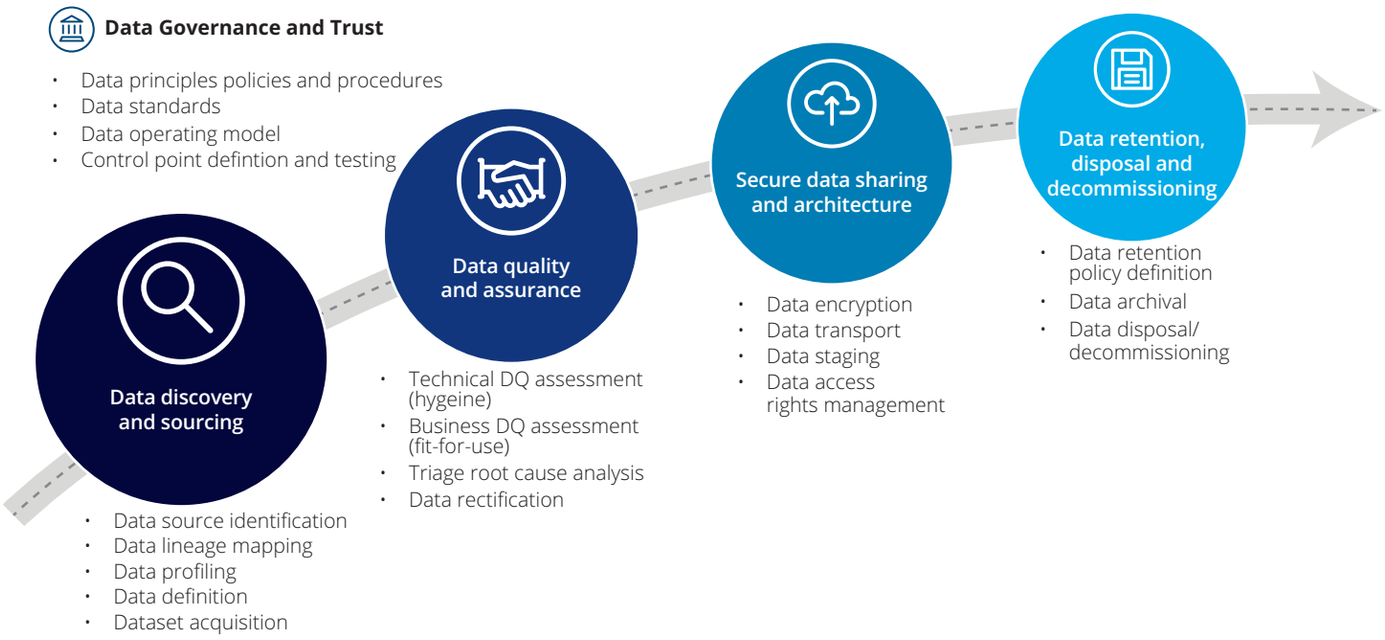
If done well, DG&A is a basis for helping organisations realise their business strategy. Unfortunately, the management of data can also be a double-edged sword, with the potential for adverse unintended consequences.

	Benefits	Unintended consequences
Analytics and AI	Proven ability to leverage enriched data sets to identify insights enabling retention of existing customers, and grow market share by tailoring products, services, and pricings to individual customer needs.	Low ROI from attempts to identify insights manifesting as failing to meet retention and growth targets due to data inconsistencies and anomalies.
Pricing	Successful adoption of sophisticated customer centric pricing algorithms running on complete and quality of market wide data sets.	Incorrect pricing decisions resulting from compromised data integrity and/or use of data for purposes other than original expected use.
Conduct	Recognition as ethical leaders based on the appropriate selection of algorithmic pricing taking into account customer segmentation and sensitive data.	Unintended discrimination of current/existing customers resulting from classification/ segmentation algorithms
APIs	Robust and effective APIs operating without exception based on agreed customer, product, and transaction data that conforms to agreed data standards.	Unintended outcomes, process failures, and exceptions resulting from non-conformance to expected data standards and data quality issues.
Privacy & Security	Seamless adoption of forthcoming GDPR style laws (including the right to be deleted/forgotten). Recognition as a trusted leader who has robust mechanisms for capturing, monitoring and enforcing consent. Recognition from regulators as a market leader able to prevent and/or efficiently respond to exceptions and breaches relating to data handling errors.	Breaches of policies, regulations and customer trust due to unsecure data sharing Inability to detect and/or remediate issues due to immature monitoring and data governance capabilities.
Financial Crime	Increased effectiveness of AML and Fraud Management capabilities based on market wide view of customer holdings and behaviours.	Breaches of policies, regulations and customer trust due to assessment of incomplete, inconsistent, or incorrect data sets.
Comprehensive Credit Reporting (CCR)	Better understanding of the customer with verifiable positive credit information will help lenders meet their responsible lending requirements and enable them to tailor offerings to customers with proven abilities to manage their credit obligations.	Inadvertent publishing of incorrect/conflicting information into the market.



The Journey to a robust and trusted Data Architecture for Open Banking

To realise their vision for open banking, organisations will need to understand a number of the delivery challenges and proactively plan for them.



Data governance and trust establishes the rules of engagement for the organisation including how data will be managed across roles, responsibilities, decision rights, policies and standards.

Data sourcing and discovery understands the legacy data landscape within the organisation – how to identify and acquire the data sets relevant to the customer, transaction and product data sets defined in the rules framework.

Data quality and assurance establishes the fitness-for-use of the data sets – identifying and resolving gaps, inconsistencies, and errors in data before datasets are either shared with market participants or merged with market data and used for analytics, automation or pricing.

Secure data sharing and architecture delivers the infrastructure and mechanics for consolidating, mastering, and securely administering data requests from customers, accredited data recipients or within the organisation.

Data retention, disposal, and decommissioning ensures that conditions of customer consent are adhered to, and that data is de-identified and/or deleted in alignment with the conditions under which the consent has been supplied.

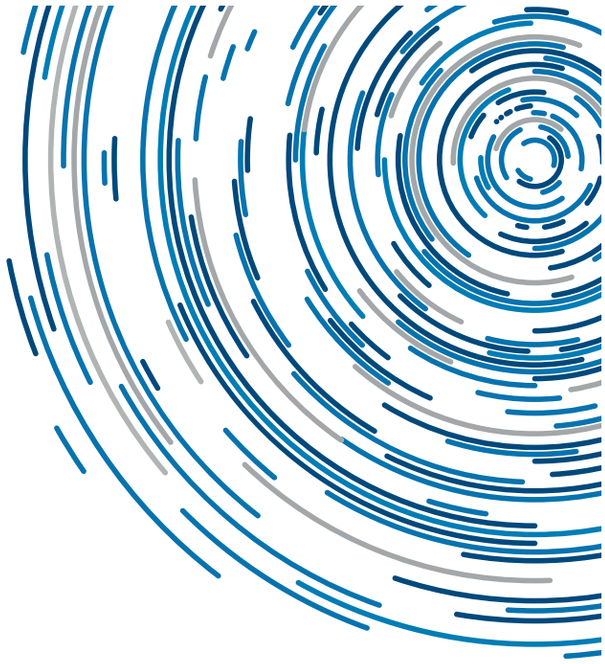
Consumer data right (CDR) participants

In addition to a CDR consumer (i.e. the person to whom CDR data relates), open banking introduces two distinct roles:

1. Data holders who are required to share customer, transaction and product information
2. Data recipients who are accredited to gain access to banking data.

In order to fulfil the CDR roles, market participants will need to address their impact on business, technology and process, requiring an organisational review of the maturity of data assets to prescribed standards. The fundamentals of data governance and architecture will need to be adhered to with a focus on data quality, management of master and reference data, secure sharing and storage of data, ensuring privacy as well as auditability of sensitive organisational data.

Each of these roles has different obligations.



Data holders

Data holders includes all Australian ADIs with the exception of foreign bank branches. The table below sets out the key challenges for data holders.

What needs to occur		What could go wrong	Implications for data governance and architecture
1	Identifying and acquiring Customer, Product/Reference, and Transaction Data from relevant many and varied operational systems across the organisation.	• Incomplete, Inconsistent or Incorrect data is sourced from operational systems • Unanticipated delays and costs are encountered in accessing off-system archives in order to achieve complete view of transaction data.	**Data discovery & sourcing** Data within organisational systems will need to be catalogued and assessed for identifying trusted source of customer/product/transaction data for quality and completeness.
2	Cleansing and mastering data into a single coherent view aligned to agreed industry standards (anticipated to finalised in Mar 2019) for presenting data to the market.	• A consolidated view of customer holdings may be unavailable and difficult to construct • Customer and Reference Data may be inconsistent across operational system • Data may reside in complex unstructured or semi-structure formats.	**Data quality & assurance** A single source of customer/product/transaction data will need to be established to enable data holders to ensure accurate information is shared with the market.
3	Developing secure data sharing and storage mechanisms in line with agreed industry standards (anticipated to finalised in Mar 2019).	• Platform could be exposed to unanticipated privacy/security breaches • Platform may not accommodate customers who do not leverage online banking systems • Platforms may experience volume and performance challenges as more and more data/requests are established in the open markets.	**Secure data sharing & architecture** Secure storage and transmission of data will be paramount to avoid regulatory breach.
4	Establishing monitoring and compliance capabilities that ensure that requested data continue/cease to be published in line with consent provided.	• Data may inadvertently cease to be shared contrary to the customers recorded consent • Data may inadvertently continue to be shared past period of recorded consent.	**Data retention, disposal & decommission** Effective governance structures and mechanisms over underlying data assets will be critical to ensure timely response to regulatory requirements over data capture, cleanse, storage and purge in alignment with obligations.

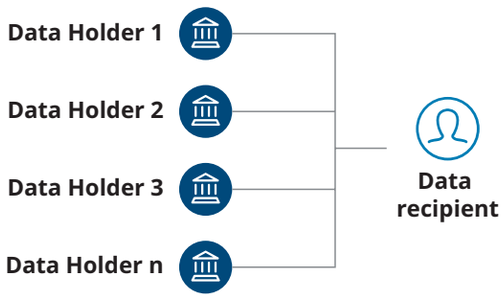
Data recipients

As the ACCC is proceeding with a Minimum Viable Product (MVP) approach for the CDR Rules Framework, the rules and obligations for data recipients will be subject to change and evolution.

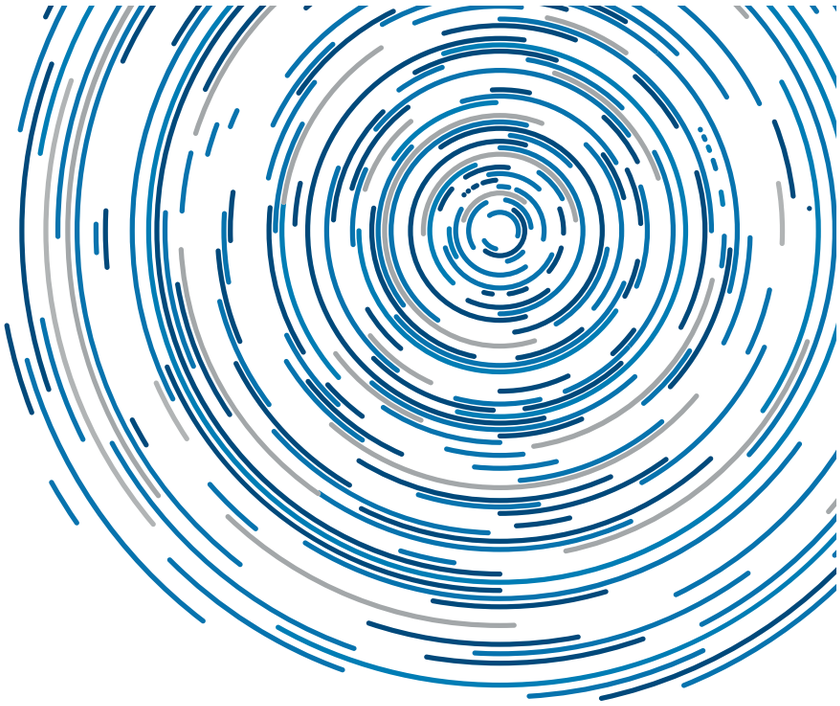
One of Farrell's key recommendations was entities receiving data which customers had shared under the Open Banking regime would be subject to reciprocal sharing obligations for 'equivalent' data.

Data recipients who provide account aggregation services – consolidating data from across the market – should consider the impact of the potential introduction of reciprocal data sharing obligations in the design of their open banking solutions.

Key challenges for data recipients include:



What needs to occur		What could go wrong	Implications for data governance and architecture
1	Securing data received from data holders and ensuring that it consent management and privacy safeguards are in place.	• Unauthorised access to data • Data breaches • Unauthorised/unethical use of customer data.	**Data security, privacy and governance** Policies, Procedures, and Capabilities will need to be in place in line with the CDR Rules Framework to ensure continued accreditation and ability to participate in the open banking regime.
2	Cleansing and mastering data from outside the organisation with data from within the organisation to form a single coherent view of the customer.	• Incomplete, inconsistent or incorrect data may be sourced.	**Data sourcing and quality** Data integration capabilities will enable merging and enrichment of a market wide view of customer/product/transaction data for quality and completeness.
3	Ensuring that data is fit for purpose and ensuring exception management mechanisms are in place to not rely on inherently compromised data sourced from a third party.	• Incorrect conclusions/decisions are reached from using the data. • APIs and/or operational systems encounter exceptions to anomalies in the data.	**Data assurance** Business rules based data quality firewalls will need to be implemented to enable capture and treatment of compromised data.
4	Preventing the proliferation of compromised data to downstream data recipients under reciprocal data agreements.	• Incorrect data is shared through the market adversely impacting customer credit decisions and organisation brand.	**Data retention, disposal & decommission** Strong data governance processes to avoid data dissipation.
5	Developing secure data sharing mechanisms in line with agreed industry standards (anticipated to be finalised in Feb 2019).	• Data is exposed to infiltration once it is published into the market • Platforms experience instability due to volume/performance challenges.	**Secure data sharing & architecture** Secure storage and transmission of data will also be required be to meet reciprocity obligations.
6	Establishing monitoring and compliance capabilities that ensure that requested data continues/ceases to be published in line with consent provided.	• Data is used for purposes outside the boundaries of consent from the customer. • Data shared under reciprocal agreements is not purged from downstream recipients in line with consent.	**Data governance** Assurance and auditability will be critical to ensure that data is used and disposed of, in accordance with customer consent.



All entities that wish to access data must be accredited by the ACCC using a risk-based standard "primarily directed towards ensuring that applicants demonstrate their capacity to manage CDR data in accordance with the privacy safeguards."[3]

The first version of the rules will provide for a general tier of accreditation with a streamlined accreditation process for ADIs to become data recipients.[4] Subsequent versions are likely to include lower tiers of accreditation based on the sensitivity of the data and the quality of the data recipient's risk management policies.

The Farrell Report had recommended that any non-ADI entity that is a recipient of open banking data, should also be obliged to provide 'equivalent' data in response to a direction from a customer. The ACCC has excluded the concept of reciprocity from the scope of the first version of the CDR rules.[5] While the concept of reciprocity and what constitutes 'equivalent' data is yet to be fully defined, it may be prudent for data recipients to consider this forthcoming obligation in the design and build of their base-line capabilities.

Start with the end in mind

With the sheer extent of organisational and technology change required for open banking, it is very easy to lose sight of the fact that banking is the first of the many industries that will ultimately become part of an open data regime.

In order to ensure that the organisational responses to open banking are strategic, scalable, and resilient, it would be advantageous for participants to baseline their end-to-end vision for open data and ensure that their approach incrementally delivers value while minimising rework and technology debt.

With the incremental expansion of the open data regime, there are three natural responses:

1. **Comply –** Ensure that DG&A capabilities meet the minimum requirements of the CDR legislation, the rules framework, and the data standards.
2. **Defend –** Leverage the DG&A capabilities developed to gain insight and enable responses required to retain market share in an environment where customer choice and tailored products and services, are beginning to flourish.
3. **Grow –** Leverage the data rich market view of customer, product, and transaction data to attract new customers within existing markets, and establish new market propositions.

A final consideration when developing a roadmap for DG&A is to consider the optimal return on investment (ROI) that can be achieved by looking for synergies across the organisation's comply, defend and growth agendas. By ensuring that competing or conflicting capabilities are not inadvertently mobilised by different stakeholders within the organisation, organisations can focus on developing a single integrated capability enabling them to optimise spending (and benefit realisation).

Notes

3. ACCC (2018), op. cit., page 25
4. ACCC (2018), op. cit., page 22. The Farrell Report had recommended that all ADIs be automatically accredited. Farrell Report (2017), op. cit., Recommendation 3.10, page 44-45
5. ACCC (2018), op. cit., page 21

Key questions organisations should ask

In considering the role of data governance and architecture in an open banking ecosystem, organisations should answer the following questions:

1. Does our data governance and architecture roadmap address the key data risks highlighted by APRA in CPG235?
2. Have synergies in data requirements been considered across analytics and AI, pricing, conduct, APIs, privacy and security, financial crime, and comprehensive credit reporting?
3. Have we considered data governance, data discovery, data quality & assurance, secure data sharing and storage, data retention, purge and decommissioning?
4. Have we addressed our dual responsibilities as both data holders and data recipients?
5. How will we respond to scenarios where new information from the market conflicts with historical internal data previously used for credit approvals?
6. How will we respond to scenarios where inconsistencies, gaps, or errors arise in data shared between data holders and data recipients?
7. How will we respond to scenarios of expiry and/or withdrawal of customer consent?
8. How will we ensure that future changes to our products, processes and systems do not result in inadvertent omission of customer, product, and/or transaction data from data published to the market?
9. What compliance and monitoring capabilities will we have in place to ensure that data continues/ceases to be published (or retained) in line with customer consent?
10. Does our vision and roadmap for Open Banking incorporate comply, defend, and growth agendas?

Last word

Market participants that optimise their investment in their data governance and architecture function will both meet their compliance obligations and defend and grow their customer base, and so benefit the most from open data.

Contacts

Melissa Ferrer
Partner, Data Modernisation
+61 403 349 192
meferrer@deloitte.com.au

Steve Jansz
Partner, Data Modernisation
+61 412 400 440
sjansz@deloitte.com.au

Series editor

Paul Wiebusch
Partner, Financial Services
+61 3 9671 7080
pwiebusch@deloitte.com.au