KNOW YOUR CUSTOMER BETTER
Connecting Financial Crime to Conduct Risk
Increased regulatory scrutiny is one of the consequences of the Royal Commission, which highlighted Australian banks’ poor conduct towards customers.

More focused regulation will bring a greater overlap between banks’ business conduct and their Know Your Customer (KYC) capabilities: both deal with direct customer interaction and are based on similar information-gathering processes.

However, both have been used for different purposes. Instead, banks need to connect them to gain a single customer view that allows in-depth, real-time analysis across the organisation.

Better KYC should not be seen solely as an obligation; doing it well brings opportunities for a much-improved customer experience and increased trust.

Better KYC also leads to better business conduct — the two are mutually reinforcing — and reduces operational, reputational and financial crime risk.

Ultimately, banks should move from KYC to KYCB, or Know Your Customer Better. Getting there will require a change in corporate culture, which must be driven from the top, along with greater data capabilities and data use.
The Royal Commission’s findings on Australia’s financial services industry highlighted banks’ shortcomings in several areas, including their anti-financial crime obligations and their conduct.¹

Poor business conduct lies at the heart of the Australian banking crisis and helped to bring on what we recently called a perfect storm, including a collapse in consumer trust.² Fixing that, we noted, would require a sea-change in behaviour.

Among other things, the Commission recommended increased powers for regulators, and that laws covering financial services be simplified to remove loopholes that encourage poor behaviour. Overall, there is a clear expectation that banks apply both the letter and the spirit of the law.

Know Your Customer (KYC) is an ideal place for banks to start given the overlap between conduct and KYC capabilities: both deal with direct customer interaction and are founded on similar data-gathering processes.

Banks that can adjust their KYC capability should benefit from improved customer trust, and a more efficient, responsive business.

---

**CONNECTING KYC AND BUSINESS CONDUCT**

**KYC procedures** are in place to meet the requirements of specific laws designed to combat money-laundering, bribery and other financial crimes.

These procedures constitute a series of obligations: the “letter of the law”.

The bank’s conduct, on the other hand, is about serving the customer transparently, according to their needs, and giving suitable advice at a reasonable price.

These “spirit of the law” procedures are typically found in regulatory handbooks, notices and specific regulations, and should provide banks with a customer focus in areas such as:

- Improved governance of relationship managers;
- A defined corporate culture;
- Controls against conflict of interest.

Behaviour that undermines KYC requirements heightens the risk of financial crimes, while that which undermines customer focus gives rise to conduct risk, an area that Australia’s banks must fundamentally rethink (an issue we have assessed in separate research).³
Improving the flow of knowledge across the organisation means banks can use KYC to improve compliance and business conduct alike. Measures taken by banks in the US and UK show that a focus on KYC and business conduct at the same time leads to simultaneous benefit.

How KYC helps business conduct

It is our view that more effective use of KYC data will enable banks to understand their customers better and encourage more ethical conduct.

For example, via the use of analytical tools the KYC team can parse the data into a ‘single customer view’ to better understand the customer and their needs, such as product suitability. Allowing the relationship manager to use this information directly enhances the client experience, builds trust and reduces the risk of mis-selling.

**KYC LOWERS BUSINESS RISK IN TRADE FINANCE**

In this theoretical example, a trade finance customer wants to buy a large shipment of electronics.

The bank’s trade finance staffer assesses the documents and — noting no problems with price, shipping routes and sanctions listings — is minded to approve the application.

But after checking the customer’s KYC data via the single customer view, the staffer sees its primary business is textiles. That raises a red flag.

The staffer passes the trade finance request to the relationship manager, who confirms the client has no need to purchase a large shipment of electronics.

The case is flagged as suspicious and forwarded to the investigations team. It determines this is an instance of trade-based money-laundering, and the trade finance application is rejected.
How business conduct helps KYC

Good conduct of business can directly impact upon a bank’s ability to meet their KYC obligations. However, this is dependent on improvements in their ability to transfer data and correctly analyse and interpret it in a compliant manner. If successful, banks can achieve a ‘single customer view’ capability, something that is highly valuable for improved anti-financial crime controls.

Australia’s banks store client data in silos and rarely perform cross-analysis on it. But lessons from overseas show that improving real-time data transfer across the organisation allows more information to flow back to the KYC function. That helps the KYC team to generate new customer insights, cross-analyse customers, and make more accurate, timely and informed decisions.

For example, a relationship manager may learn from their customer of their intention to move their business into a higher risk country. Informing KYC immediately can allow for a prospective KYC refresh.

Stronger relations between teams are also important, for example between relationship managers in the front office and KYC staff. The latter, for instance, benefit from access to relevant insights and background, which further improves their understanding of the customer portfolio and increases the quality of their analysis.

In the case of a vulnerable customer a relationship manager can both ensure they are treated appropriately, but also in certain situations may identify a financial crime risk such as a customer who is being coerced. This should become KYC information too.

THE SINGLE CUSTOMER VIEW

Creating a single customer view requires that all KYC information is digitised, with data captured in a single stage (minimising client disruption) and stored in a repository that provides one consistent view of each customer.

This allows all customer-related teams in front-, middle- and back-office to access this data to inform their KYC decision-making process and their business conduct.

It also makes it easier to comply with data-privacy rules, because all of the information is held in a single place rather than being scattered across various silos. And it means that data previously disregarded as less valuable can be mined for insights.
From KYC to KYCB

Improving KYC and business conduct take banks from KYC to KYCB — or Know Your Customer Better. This will take work, because this is not how the KYC function currently operates at Australian banks (see Fig 1 below).

Figure 1. Characteristics of a typical KYC function in Australia

1. Inaccurate data flows between functions
2. Limited KYC/front office interaction
3. Data is captured to the minimum
4. Tactical solutions drive changes
5. Segregation of functions and information
6. Limited use of data outside of core function

Figure 2. Characteristics of a future KYCB function

1. Reliable data flows between functions
2. Shared anti-financial crime capabilities
3. Data capture is maximised
4. Strategy driven by culture
5. Easy access to information
6. Use of previously undervalued data

Source: Accenture

As the Royal Commission made clear, success will require wholesale change of banks’ culture, and a better use of data. These would form the heart of the KYCB function.
Cultural shift

Effecting wholesale cultural change means putting the customer first at each stage of the relationship, including during KYC activities. This is seldom easy as lessons from the US and the UK show. Banks that have managed this have refined their structures to ensure that the right legal and ethical behaviour was encouraged and supported.

The cultural change must be driven from the top — a consistent ‘customer first’ message from management, and emphasis on the importance of sharing information and knowledge. This message could be simply conveyed via a podcast showcasing examples of best practice.

It is crucial that these new values align so that staff in different teams are educated about each other’s customer obligations.

The compliance function must command respect and be allowed to act against poor conduct, such as trading with a customer outside of their financial crime risk tolerance, or trading via a mis-sold product.

Better data, and better use of it

The second aspect on the road to KYCB is improving data capabilities and use. Ensuring that data is thorough, accurate and available equally to staff who need it will provide banks with what they need in fulfilling both the letter and the spirit of the law.

Banks must ensure they have set up relevant and appropriate business, operational and technical capabilities that are tracked via KYC and Conduct Change Programs. Additionally, given how customer data will be used, they must ensure that they comply with privacy regulations.

The resultant clear flow of information connects the client information, the relationship manager, the KYC function and third-party information (such as media reports) to provide the bank with a comprehensive view of their customers.

Scenarios 1 and 2 in Figure 3 show how this process should operate from the start of the client’s relationship with the bank through to their passing the KYC checks and being assessed to ensure that they are low-risk and are recommended suitable products only.

Scenario 3 illustrates a timely information flow whereas scenarios 4 and 5 highlight what can go wrong when the information flow is not thorough, accurate and equal.

In scenario 4 the KYC function may miss increased financial crime risk if a significant change in behaviour is not communicated. In scenario 5, an RM risks unknowingly executing transactions for a customer who KYC now knows to have an increased risk.
Ensure clear flows of information. Quality of data is paramount to achieving both anti-financial crime and improved conduct outcomes. Policy dictates whether a customer can be sold to; a relationship manager will control the product that is then sold. In order for a KYC capability to work the information flow between a middle or back office KYC function and the front office must be thorough, accurate and equal.

Examples: Private Client in Relationship with Bank

PRIVATE CLIENT RELATIONSHIP MANAGER KYC FUNCTION THIRD PARTIES

Scenario 1
1. Background info received and passed to KYC Function

Scenario 1
2. Are able to assess risk tolerance and suitability of products

Scenario 2
2. Are able to assess risk tolerance and suitability of products

Scenario 3
3. Background info received and passed to KYC function

Scenario 3
4. KYC Refresh missed: risk may have changed

Scenario 4
4. KYC Refresh missed: risk may have changed

Scenario 5
5. Continues to execute transactions

KYC function can assess risk using basic customer information plus third party data plus RM knowledge

RM can advise with first hand knowledge of customer background plus results of thorough KYC check

Change in business may affect both financial crime risk and suitability of advice. Both RM and KYC receive information and share outcomes, RM advice remains suitable; risk tolerance is retained

Significant change in service type represents a significant change in behaviour. This may not trigger a KYC refresh though there is a risk underlying reasons represent a financial crime risk

KYC have access to far greater adverse media checks than RM. Knowledge of customer issue may not be received by RM until after transactions are executed in line with higher risk customer instructions

Key:
- Activity
- Communication success
- Communication missed
- Negative outcome

Source: Accenture
A KYCB function allows banks to show they are complying with their KYC obligations — by mitigating financial crime risk — and business conduct obligations — by mitigating risk of mis-selling. In other words, are addressing the themes outlined by the Royal Commission and beginning the process of restoring trust and rebuilding their reputation.

In short, there is a sound business case for banks to start changing their KYC process and the way in which they gather, store and access customer data. This will see them move from lagging behind best practice in KYC to a dynamic, forward-looking and comprehensive vision of KYCB.
References


2 Ensuring Seaworthiness to Charting a Course: How Australian Banking Can Survive the Perfect Storm, Accenture (2019).


About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 482,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

The views and opinions expressed in this document are meant to stimulate thought and discussion. As each business has unique requirements and objectives, these ideas should not be viewed as professional advice with respect to your business.