

# Building Organisational Capability:

How banks can improve compliance  
with the **Banking Code of Practice**  
and deliver better customer outcomes



**BCCC**  
Banking Code  
Compliance Committee

# Table of Contents

<b>Executive Summary</b>	<b>3</b>
<b>Introduction</b>	<b>8</b>
<b>Concerns about Code breach causes</b>	<b>8</b>
<b>Key areas that influence organisational capability</b>	<b>12</b>
1. Communication strategy	13
2. Learning and development	16
3. Systems, processes and technology	19
4. Culture	23
5. Enhancing capability through robust compliance frameworks	27
<b>Appendices</b>	<b>32</b>
Appendix 1. Success stories template	33
Appendix 2. Root cause analysis template	34
Appendix 3. Action Plan Template	35
Appendix 4. Maturity assessment tool	36
Appendix 5. About the BCCC	37

# Executive Summary

This report provides Code-subscribing banks' (banks) senior leaders with guidance on how to build organisational capability to improve compliance with the Banking Code of Practice (the Code).

The Banking Code Compliance Committee's (BCCC) recommendations in this report are focused on the steps banks should take to make compliance with the Code a core part of its strategy and culture. Banks can achieve better and more consistent outcomes for customers by developing an integrated approach to Code compliance.

The BCCC is concerned that too often banks identify 'human error' as the cause of Code breaches without establishing, recording or acting on the 'root cause' of the problem. When a breach occurs for which 'human error' is to blame, it is often the case that staff conduct or actions have been influenced or constrained by internal systems, processes, technology, training and/or organisational culture.<sup>1</sup>

The BCCC commissioned Deloitte's Human Capital team to research how banks can best equip, support and enable staff to comply with the Code, and build organisational capability within a banking context.

Deloitte conducted extensive research, including engagement with banks through an industry-wide survey, a series of focus groups and interviews to gather perspectives from employees at various levels within banks. The BCCC appreciates the candid feedback banks provided to support this research.

The research identified industry challenges, opportunities for improvement and good practice with respect to compliance capabilities. This enabled Deloitte to provide the BCCC with findings about which key factors influence organisational capability for Code compliance.

This BCCC report is informed by Deloitte's research findings and contains five key capability areas and recommendations for improved industry practice.

The BCCC considers this to be a 'live document' and expects banks to demonstrate how they have considered the report's recommendations to improve Code compliance capabilities and customer outcomes when responding to future BCCC monitoring activities.

<sup>1</sup> The issue was first identified by the Code Compliance Monitoring Committee (CCMC) from banks' responses to the 2017-18 Annual Compliance Statement. Banks reported that the overwhelming majority of Code breaches - 93% - were attributed to human error. This trend continued in subsequent periodic self-reporting of banks' compliance data. On 1 July 2019 the CCMC transitioned to the BCCC to coincide with the release of the Banking Code of Practice.

# Key capability areas and recommendations for better practice

**1** COMMUNICATION STRATEGY

**2** LEARNING AND DEVELOPMENT

**3** SYSTEMS, PROCESSES AND TECHNOLOGY

**4** CULTURE

**5** ENHANCING CAPABILITY THROUGH ROBUST COMPLIANCE FRAMEWORKS

For each key area the report contains insights from industry participants to Deloitte's research on what banks are currently doing well and where they face challenges, along with better practice recommendations.

The recommendations should be viewed holistically – an impactful communication strategy, effective learning and development, and designing all systems, processes and technology with the needs of customers and employees at their centre – are all inevitably underpinned by an organisation's culture and a mind-set of continuous improvement and delivering good customer outcomes.



## 1. COMMUNICATION STRATEGY

An effective communication strategy is one that ensures employees within a bank understand the intent and importance of processes related to the Code's customer protections. Ultimately, it is how front-line staff 'feel' about the message that will gain their commitment.<sup>2</sup> Effective communication should promote a customer-centric approach to all decision-making, proactive escalation of customer issues and encourage the reporting of compliance concerns. Communications should extend to all staff that directly and indirectly influence customer outcomes and organisational culture, including employees responsible for the design and distribution of products, systems, process, remuneration structures and talent acquisition. Messaging should be cascaded by those at the very top with sentiments reiterated down through senior leaders, middle management, and team leaders.

### Better practice recommendations:

- Deliver impactful and consistent messaging from the top down that highlights the importance of the Code commitments to successfully shift behaviours
- Engage staff with compelling narratives and storytelling that resonates with their business unit and respective roles
- Use breach data to guide topics for discussion in relevant team meetings, encouraging open communication by staff about real-life Code compliance case studies and learnings
- Use a range of communication channels to ensure the message is heard by all staff.



## 2. LEARNING AND DEVELOPMENT

Learning and development are crucial for ensuring Code competency among all staff within an organisation. Education about the Code should go beyond awareness. It should also educate staff right across the business about the Code's role in the consumer-protection framework, and the importance of all staff meeting their Code obligations to customers. It should also educate staff about how to escalate, report and manage incidents/Code breaches and why these steps are important to the bank and its customers. Learning and development should be engaging and relevant to employee roles to be effective in the long term.

### Better practice recommendations:

- Code training should educate staff on the Code's role in the consumer protection framework and the real impact that staff can have on customer outcomes
- Continuously iterate and improve staff training programs to close knowledge gaps identified by trends in the banks' breach data
- Establish a central repository for all staff to access supporting resources they need to do their jobs.

<sup>2</sup> Setting the Tone from the Top, Melinda Muth and Bob Selden, 2018 <https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/book-store/pdf/setting-tone-from-top-preview-pages.ashx>



### 3. SYSTEMS, PROCESSES AND TECHNOLOGY

Systems, processes and technology form an essential part of a bank's compliance framework. When effectively implemented, they support and guide employees to have the right customer conversations and comply with the Code obligations. They enable Code breaches to be prevented and detected, reported and remediated, and they ultimately enhance customers' experience with the bank. All systems, processes and technologies designed for Code compliance should have the needs of both the customer and the employee at their centre.

#### **Better practice recommendations:**

- Develop an organisation-wide design objective that puts good customer outcomes and employee compliance at the centre of all products, systems, processes and technologies
- Test and iterate processes and products using human-centred design in pursuit of continuous improvement
- Consolidate data from multiple channels on a central platform to get a holistic view of Code compliance and to ensure all breaches are captured
- Integrate learning and technology in a way that increases employee engagement, self-guided learning and compliant outcomes
- Develop and adopt real-time reporting and analysis to proactively prevent and detect Code breaches.



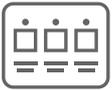
### 4. CULTURE

Regulators and the community at large expect banks to embed a strong organisational culture that champions fairness, honesty and transparency above all else. Good organisational culture ensures that staff behaviour is not guided by misaligned incentives and conflicts of interest and can be summed up as 'doing the right thing' even when no-one is watching. It consistently puts the spirit of the Code at the centre of decision-making, behavioural expectations, and empowers staff to take ownership of achieving the right customer outcome.

#### **Better practice recommendations:**

- Reinforce a culture that links employee compliance to clear customer outcomes and fosters a continuous improvement mindset
- Review reward and recognition programs to link employee performance and incentives to positive customer outcomes and avoid creating incentives that undermine those outcomes

- Bridge the gap between different bank functions through formal and informal feedback loops
- People leaders should model the desired behaviours and expectations that demonstrate a customer-centric approach and the spirit of the Code
- Create relationships between banks to share success stories and best practice.



## 5. ENHANCING CAPABILITY THROUGH ROBUST COMPLIANCE FRAMEWORKS

Deloitte has developed 'compliance capability tools' that banks can use to benchmark their own compliance frameworks to help:

- Strengthen their own compliance frameworks
- Improve their processes for identifying and addressing the root causes of Code breaches
- Enable and support employees across the business to understand their Code obligations, recognise when Code breaches occur and report them promptly
- Remediate Code breaches and prevent them from recurring.

# Introduction

The Banking Code of Practice (the Code) sets out the standards of practice and service in the Australian banking industry for individual and small business customers, and their guarantors. [Nineteen banks](#) subscribe to the Code.

The Financial Services Royal Commission Final Report described the role of industry codes as being to ‘set standards on how to comply with, and exceed, various aspects of the law’. To ensure that industry codes

work effectively, the Commissioner noted that there must be ‘adequate means to identify, correct and prevent systemic failures in applying the Code’.<sup>3</sup>

The Banking Code Compliance Committee (BCCC) is an independent compliance monitoring body established under clause 207 of the Code. The BCCC’s purpose is to monitor and drive best practice Code compliance.

## CONCERNS ABOUT CODE BREACH CAUSES

As part of its monitoring program, the BCCC requires banks to regularly self-report breaches of the Code. One key issue, which has come to the BCCC’s attention in recent years through our assessment of banks’ self-reported breach data, is the extremely high number of breaches attributed to human error. Banks attributed human error as the cause of 93% of all Code breaches in 2017–18. In 2018–19 this figure fell slightly to 91%. Human error topped the list of causes of Code breaches once again in banks’ Code compliance data for the period July to December 2019.<sup>4</sup>

Aside from the concerns that these breaches raise about banks’ Code compliance, the impact on banking customers has not been insignificant. In the 18 months from July 2018 to December 2019, at least 13.4 million customers were affected by banks’ Code breaches, with a minimum overall financial impact of \$190 million.

The BCCC is uncertain whether the statistics for why breaches occur are a true reflection of Code breach causes, or whether they are overinflated because banks more readily attribute non-compliance with the Code to human error as a default option in their breach reporting. Either way, the BCCC has concerns about banks’ organisational capability – particularly in relation to how they equip and enable staff to comply with the Code – the adequacy of staff training and the robustness of their compliance frameworks to identify the genuine root cause of breaches and prevent a recurrence.

This report identifies opportunities for improvement and gives banks actionable ways to improve practice in both these areas.

<sup>3</sup> Final Report, Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, 2019

<sup>4</sup> See BCCC reports: [Compliance with the Code of Banking Practice 2017–18](#); [Compliance with the Code of Banking Practice 2018–19](#); and [Banks’ compliance with the Banking Code of Practice – July to December 2019](#)

“ ... staff must act ‘fairly, reasonably and ethically’, and staff must be ‘sensitive, respectful and compassionate’ and provide ‘extra care’ with customers who are experiencing vulnerability.

## ORGANISATIONAL CAPABILITY IS ABOUT MORE THAN TRAINING

While the Code contains many prescriptive requirements of banks about the things they must do or not do, it also contains many principles-based provisions, for example, staff must act ‘fairly, reasonably and ethically’, and staff must be ‘sensitive, respectful and compassionate’ and provide ‘extra care’ with customers who are experiencing vulnerability.

The Code also contains the following obligations about staff training and competency under Chapter 4 of the Code:

*We will make sure that our staff and our representatives are trained so that they:*

- a)** *can competently do their work; and*
- b)** *understand the Code and how to comply with it when they are providing banking services.*

Banks’ self-reported data, along with intelligence gathered through the BCCC’s own breach investigations, shows that banks choose to address the high number of human error related breaches predominantly through staff training and, to a lesser extent, through enhanced monitoring activities, system fixes, process improvement and disciplinary action.

Yet, standalone interventions such as staff training in Code compliance are often not enough. While staff must understand how to comply with the Code and why it is important for customers, they must also be adequately supported by their organisation to do the right thing.

To address human error related breaches, banks should adopt a holistic approach, and question whether the bank’s infrastructure - including but not limited to, existing and new technology, systems and processes, remuneration and incentive programs – are all designed and geared to support employees to do the right thing, achieve the right outcomes for the customer, and by extension, the bank.

## PURPOSE OF THE REPORT

The purpose of this report is to help banks to effectively prevent and appropriately respond to Code breaches by improving organisational capability and Code compliance. It highlights that all staff – from frontline employees and team leaders through to senior executives and Board members – play a vital role in upholding the promises banks make to customers when they subscribe to the Code.

The report also provides banks with guidance to strengthen Code compliance frameworks and undertake a more rigorous breach investigation and root cause(s) analysis to understand the real cause of non-compliance. By knowing the true root cause, banks will be better placed to make sure the same breaches do not occur again.

Included throughout the report are proactive measures that banks can consider and self-assess against to build on their own organisational capability and Code compliance - see [Appendix 4](#). The report also contains industry insights and information about opportunities for improvement, including practical examples and better practice recommendations.

“ By knowing the true root cause(s), banks will be better placed to make sure the same breaches do not occur again.

The BCCC considers that reviewing and acting on the various measures and recommendations in this report will contribute to achieving better outcomes for banks and for their customers.

The BCCC considers this to be a ‘live document’ and expects banks to reflect on the key themes and recommendations in this report and:

- consider which recommendations require action within their business to improve Code compliance and customer outcomes
- take proactive steps to implement changes to prevent human error breaches, including review of internal systems, culture, communications, and learning and development programs, and
- demonstrate through reporting that they have conducted thorough root cause analysis of breaches and looked beyond coaching/feedback to fix human error related breaches to prevent recurrence.

The BCCC will use the themes in the report to inform its:

- analysis of banks’ breach data
- investigations and inquiries, and
- ongoing engagement with banks.

## BACKGROUND AND RESEARCH

The BCCC's concerns around the high number of breaches attributed to human error and the robustness of banks' compliance frameworks to identify the genuine root cause of breaches led it to commission Deloitte to conduct research into how banks' can best equip and enable staff to comply with the Code.

Deloitte was selected because of its expertise in financial services, organisational strategy and transformation through people, leadership and cultural change.

### **Deloitte's research sought to:**

- identify the challenges for banks to building organisational capability
- understand what best practice is with respect to training, supporting resources, systems and culture
- provide recommendations to the BCCC about how banks can equip and enable staff at all levels of the organisation to achieve Code compliance
- develop compliance capability tools that banks can use to benchmark their own compliance frameworks.

To understand the current landscape and identify best practice Code compliance activities, Deloitte considered the BCCC's existing reports and publications, alongside research and analysis compiled by its own risk and compliance experts.

It also engaged with industry, including banks of varying sizes, to gather insights and understand challenges and improvement areas for Code compliance. Feedback from banks was gathered via focus groups, an online survey, and interviews with employees across the businesses, from frontline staff up to executive leadership.

Deloitte's research was also informed by investigating 10 other codes of practice across varying industries in Australia and the United Kingdom to understand the strategies those industries employ to enhance organisational capability and promote compliance.

Taking into account the feedback from bank employees about the challenges they face in complying with the Code and keeping up with changes to the regulatory landscape in general, Deloitte sought to identify specific opportunities for banks to improve organisational capability and Code compliance.

This report is informed by the findings of Deloitte's research and goes further to make additional suggestions and recommendations for banks to self-assess against.

# Key areas that influence organisational capability

This section covers key areas that influence organisational capability and Code compliance with supporting recommended practice across each theme for banks to reflect on and self-assess against, including:

**1** COMMUNICATION STRATEGY

**2** LEARNING AND DEVELOPMENT

**3** SYSTEMS, PROCESSES AND TECHNOLOGY

**4** CULTURE

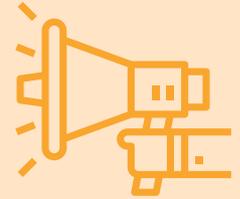
**5** ENHANCING CAPABILITY THROUGH ROBUST COMPLIANCE FRAMEWORKS

These key areas were established by the research conducted by Deloitte into building organisational capability (the research). The industry insights in each area of the report were established from the research findings.

The recommendations should be viewed holistically – an impactful communication strategy, effective learning and development and designing all systems, processes and technology with customers and employees at their heart - are all inevitably underpinned by organisational culture and a mind-set for continuous improvement and good customer outcomes.

# 1.

# COMMUNICATION STRATEGY



In the context of Code compliance, an effective communication strategy is one that ensures bank staff understand the intent and importance of processes related to the Code's customer protections. Ultimately, it is how front-line staff 'feel' about the message that will gain their commitment.<sup>5</sup> Effective communication should promote a customer-centric approach to all decision-making, proactive escalation of customer issues and encourage the reporting of compliance concerns. Communications should extend to all staff that directly and indirectly influence customer outcomes and organisational culture, including employees responsible for the design and distribution of products, systems, process, remuneration structures and talent acquisition. Messaging should be cascaded by those at the very top with sentiments reiterated down through senior leaders, middle managers, and team leaders in the business.



## INDUSTRY INSIGHTS: WHAT ARE THE CHALLENGES AND THREATS?

To glean insights into the challenges of implementing an effective communication strategy, and the potential implications of failing to do so, participants were asked about their level of Code awareness, the challenges they face in complying with the Code and what additional support banks could provide to help staff overcome these challenges.

### Code awareness

More than half of the overall participant sample indicated they were "very aware" of the Code, and 91% of those who participated in the online survey self-reported a high awareness of the Code. Participants cited "communications" as one of the main ways they were made aware of the Code but they also noted that Code awareness does not always translate into action, understanding and compliant behaviour, as the importance and consequences of the Code are not always made clear.

When employees have a limited understanding of the intent or spirit of the Code and its true purpose, they are less likely to put the customer at the centre of decisions, or recognise when something is not right and act to address it. The result will likely be an increase in poor customer outcomes and Code breaches.

### Regulatory complexity and change

Bank employees reported finding it difficult to stay up to date with Code compliance, in addition to the other legislation and regulation they are required to know in their roles. This was a common challenge in banks of all sizes, and affected not just frontline employees but also those employees responsible for designing and scheduling compliance training.

<sup>5</sup> Setting the Tone from the Top, Melinda Muth and Bob Selden, 2018 <https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/book-store/pdf/setting-tone-from-top-preview-pages.ashx>

Banks operate in a fluid policy and regulatory environment, where compliance obligations regularly evolve. Employees want their banks to make it clear and easy for them to stay on top of new compliance information and expectations.

### The importance of leadership

Employees said that communication about Code compliance and the Code's role in driving the right behaviours within the business should come from the top – the executive leadership – and cascade down to frontline employees.

If the leadership team is not seen as advocating a customer-centric approach and encouraging employees to flag compliance issues and Code breaches, employees may interpret this as a sign that Code compliance is not taken seriously within the bank or that it has been de-prioritised.

### WHAT ARE BANKS DOING WELL?

The research found that banks have adopted some good-practice strategies for communicating about the Code and related compliance issues throughout the business. These strategies include coming together via team meetings or huddles to discuss Code changes, breaches and scenarios, and, in the case of some smaller banks, facilitating two-way feedback loops between those who drive Code compliance (for example, business leaders and process owners) and front-line employees who are required to comply.

### RECOMMENDATIONS FOR ACHIEVING BETTER PRACTICE COMMUNICATION

Banks should consider the following recommendations to ensure employees understand the rationale and importance of processes related to the Code's customer protections and to create positive behavioural change that prioritises a customer-centric approach to all decision-making, proactive escalation of customer issues and reporting of compliance concerns.

#### **Deliver impactful and consistent messaging from the top down that highlights the importance of the Code to successfully shift behaviours**

- Communication, either verbal or written, has an intent – what it seeks to achieve – and an impact – how it is received by the recipient.<sup>6</sup> For senior leaders to create behavioural change, communications must align the intent and impact to get staff to act on what is being communicated.<sup>7</sup>

*For example: a senior leader can encourage all staff to report compliance issues and to see breach reporting as a good thing – as an opportunity to be a better bank, 'right a wrong' and prevent it from happening to the next customer.*

<sup>6</sup> Setting the Tone from the Top, Melinda Muth and Bob Selden, 2018 <https://aicd.companymen.com.au/-/media/cd2/resources/director-resources/book-store/pdf/setting-tone-from-top-preview-pages.ashx>

<sup>7</sup> Ibid.

- Messaging should be echoed and reiterated by middle management and people leaders in each business unit - to maintain awareness and support application in practice.
- Frequent messaging acts as a reminder to staff of the banks' priorities and ongoing commitment to uphold the promises made in the Code and what it expects from its people.

### **Engage staff with compelling narratives and storytelling that resonates with their business unit and respective roles**

- Use storytelling to highlight success stories and learnings from their business unit to connect employees to the spirit of the Code. See [Appendix 1](#) for a Success Stories template that can help staff to share these stories.
- Humanise the impacts or consequences of non-compliance, particularly for customers who are experiencing vulnerability and demonstrate the important role front-line staff play in ensuring the right customer outcomes are achieved. In contrast, the success stories should demonstrate how the bank empowers front-line staff to adopt customer-centric decision making, escalate issues and/or fix compliance issues when things go wrong.

### **Use breach data to guide topics for discussion in relevant team meetings, encouraging open communication by staff about real-life Code compliance case studies and learnings**

- Topics for discussion should vary based on breach reporting. Provide opportunities at informal team meetings or 'stands-ups' for employees to collaborate and discuss common Code breach scenarios, identify root causes and brainstorm areas for improvement.
- Consider opening team meetings with a 'Code compliance moment', where staff are invited to share recent personal experiences of a good compliance practice/learning, for example an interaction where they provided 'extra care' to a customer with non-standard needs or where they prevented a potential Code breach and how they did this.
- Use real instances of Code breaches to educate employees on what constitutes a breach, they may have learnt this in training, but refreshers are important, particularly for more principles-based Code obligations that do not stipulate what is right or wrong behaviour.

### **Use a range of communication channels to ensure the message is heard by all staff**

- Specific communication campaigns should be tailored to all staff that directly and indirectly influence customer outcomes and organisational culture. This includes employees responsible for the design and distribution of products, systems, process, remuneration structures and talent acquisition.
- Use staff e-newsletters, intranet pages and/or collaboration platforms (for example, internal social media platforms) to promote real-time exchange of information and direct employees to more formal communication channels and information sources about Code compliance.
- Consider implementing a dedicated section on collaboration platforms or systems to enable employees to share stories, case studies and best practice to help 'bring the Code to life'.<sup>8</sup>

<sup>8</sup> Banks should ensure collaboration platforms are regularly monitored to ensure any compliance information being shared among employees is correct, appropriate and in line with the organisation's cultural expectations and legal obligations.

# 2. LEARNING AND DEVELOPMENT



Training about the Code should go beyond awareness, it should also educate staff right across the business about the Code's role in the consumer-protection framework, and the importance of all staff meeting their Code obligations to customers. Training should also educate staff about how to escalate, report and manage Code breach incidents and why these steps are important to the bank and its customers. Learning and development resources should be engaging and relevant to employee roles to be effective in the long term.

## INDUSTRY INSIGHTS: WHAT ARE THE CHALLENGES AND THREATS?

During industry engagement, participants were asked to highlight some of the challenges they encounter as part of their Code compliance learning and development, and where they believe improvements can be made and additional learning support provided by banks to help build capability to comply with the Code.

### **Effectiveness of training**

General feedback indicated that learning around Code compliance can be generic, with limited tailoring to suit specific roles within the organisation. Some participants felt that standardised Code training reduces employee engagement with the content, prevents knowledge retention, and fails to bridge the gap between employees' awareness of the Code and their understanding about role specific Code compliance obligations.

### **Information overload**

Participants noted that employees are expected to retain a lot of Code and non-Code training while also remembering product information, terms and conditions, and other processes related to their roles. This information overload creates a significant burden on employees. Training overload, particularly during the onboarding stage, which is when the majority of employee compliance training occurs, was also said to impact knowledge retention. Constraints on the time required to undertake training was cited as one of the top challenges by participants of the online survey.

## Support for customers who are experiencing vulnerability

Participants indicated that many employees find it challenging to identify customers who are experiencing vulnerability and need help to be able to effectively handle these customers' enquiries. Around one-third of respondents to the online survey said they would like to see additional ongoing learning opportunities to help them provide extra care to those customers who need it. Part 4 of the Code contains several obligations toward disadvantaged customers, including the requirement to treat customers experiencing vulnerable circumstances with sensitivity, respect and compassion. All banks acknowledged that training to support these customers is an ongoing area of development and will prioritise training that helps employees identify vulnerable customers and build emotional intelligence to better handle emotionally charged conversations.

### WHAT ARE BANKS DOING WELL?

Some banks have simplified learning for their employees by combining different Code, legislative and regulatory requirements into one easily digestible learning solution. Others have also empowered employees to create learning content to share with their teams via a social learning platform. This user-generated learning content complements formal learning and is supported by governance to ensure content quality. Some banks have developed customer care guides that provide training, online reference materials and contacts to external providers to assist them in supporting customers experiencing vulnerability, while others have leveraged dedicated internal vulnerable customer teams (via actual roles or committee structures) to provide a consistent point of reference for guidance on the treatment of vulnerable banking customers.

### RECOMMENDATIONS FOR ACHIEVING BETTER PRACTICE LEARNING AND DEVELOPMENT

The previous section of the report discussed the importance of impactful communication that ensures employees understand the rationale and importance of processes related to the Code's customer protections. Communication should build on and reinforce ongoing learning and development initiatives, which are crucial for ensuring Code competency among all staff within an organisation.

Banks should consider the following recommendations to improve employees' understanding of the Code's purpose and their duty to comply with it, in a way that increases their engagement with the learning process, supports knowledge retention and equips them with easy access to the information they need to comply with the Code.

## **Code training should educate staff on the Code's role in the consumer protection framework and the real impact that staff can have on customer outcomes.**

- Scenario-based learning is a particularly effective learning tool for educating employees about issues that all customers can face. Some employees may not otherwise have the life experience to relate to customers experiencing vulnerable situations.
- Use scenario-based learning to help build employees' critical capabilities such as curiosity, empathy and adaptive thinking when they encounter similar scenarios on the job.
- Incorporate guest speakers or external partnerships or community groups to help educate staff to support vulnerable customers where the scope of help is outside banking.
- Give staff strategies and tools that enable them to navigate emotionally charged conversations to address a customer's needs or concerns. These strategies and tools should extend to staff wellness post the interaction.

## **Continuously iterate and improve staff training programs to close knowledge gaps identified by trends in the banks' breach data.**

- Use bank-specific breach data to tailor learning programs to areas of the Code that are subject to breaches (particularly those where human error is deemed to be the cause).
- Additional formal education should be targeted to certain specialised front-line roles, such as dedicated vulnerability teams.
- Adjust learning programs where necessary to ensure they are contextualised and relevant to specific business areas.
  - *For example, a small business customer seeking financial difficulty assistance should be able to speak with someone at the bank that is experienced and familiar with the context and location in which the business operates and who has the capability to tailor a suitable arrangement.*

## **Establish a central repository for all staff to access supporting resources they need to do their jobs.**

- Develop a dedicated intranet page or knowledge sharing platform, where all employees can quickly and easily access up-to-date information about compliance with the Code, legislative and regulatory changes. This ensures that front-line staff can have quick access to the latest most accurate supporting resources while on the job.
  - For example, store relevant supporting documents such as, reference guidelines, conversation helpers and internal and external referral numbers that staff can promptly find while dealing with a customer's complex situation.

# 3.

## SYSTEMS, PROCESSES AND TECHNOLOGY



Systems, processes and technology form an essential part of a bank's compliance framework. When properly implemented, they support and guide employees to have the right customer conversations and comply with the Code obligations. They enable Code breaches to be both prevented and detected, reported and remediated, and they ultimately enhance customers' experience with the bank. All systems, processes and technologies designed for Code compliance should have the needs of both the customer and the employee at their centre.

### **INDUSTRY INSIGHTS: WHAT ARE THE CHALLENGES AND THREATS?**

Participants to the industry engagement were asked to explain what impact systems, processes and technologies have on their ability to comply with the Code's obligations, and whether systems, processes and technology currently create a challenge to providing good customer outcomes. The specific example of a cancellation of a customer's direct debits was also posed to participants.<sup>9</sup>

#### **Embedding the Code into systems and processes**

Some participants felt that embedding Code requirements into systems, workflows, policies and reference guides would better enable them to meet their Code compliance obligations.

#### **Direct debit cancellations**

Several participants noted that the processes for cancelling direct debits involve multiple touchpoints, systems and/or sign-off steps, which in turn create multiple points of potential failure. Multiple steps in the process increase the possibility of errors and breaches occurring, as well as the time taken to respond to and deliver what customers perceive as a straightforward request.

#### **Systems to simplify compliance**

Participants reported that legacy IT systems do not always contain the mechanisms that support employees to comply with the Code. This can lead to employees using manual workarounds to circumvent outdated systems, leading to an increased likelihood of errors and breaches.

<sup>9</sup> Under Chapter 34 of the Code, banks are required to promptly process a customer's request to cancel a direct debit. Banks must not inform customers that they should first raise the cancellation directly with the merchant.



## WHAT ARE BANKS DOING WELL?

Banks have implemented product management frameworks or checklists to assist when designing new products. This helps to mitigate the risk of staff making a mistake in the product design process and also to manage product change and development consistently. There are also procedural guidelines that translate Code sections into actions required in the workflow to ensure Code compliance. On the technology side, several banks have implemented incident management systems which allow all employees to log incidents, manage breaches and remediation, and provide sign-offs. Some banks also have systems that help identify and manage interactions with vulnerable customers through the use of flags and pop-up boxes with notes to assist future conversations.



## RECOMMENDATIONS FOR ACHIEVING BETTER PRACTICE SYSTEMS, PROCESSES AND TECHNOLOGY

Banks should review their systems, processes and technology with the following recommendations in mind, and with a view to ensure good outcomes for employees and customers. By optimising existing systems, processes and technologies and where viable, emerging technologies, the bank can more effectively prevent and detect Code breaches, self-report to the BCCC and improve customer outcomes.

### **Develop an organisation-wide design objective that puts good customer outcomes and employee compliance at the centre of all products, systems, processes and technologies.**

- Product management frameworks and design checklists should align with the organisation-wide design objective and help designers to successfully meet this objective.
- Design teams should collaborate with various stakeholders internally and externally to test that designs are fit for purpose and will deliver good customer outcomes.
  - ▶ *For example, listen to customer feedback and ask questions from those with 'lived experience' to develop a deep understanding of customer needs and pain points.*
- Create internal metrics to measure what successful design is – this should align with the intention of the Code and the banks' strategy.
  - ▶ *For example, capability to demonstrate how the role of a product or process design has contributed to consistently fair and ethical outcomes for particular customer cohorts.*

## Test and iterate processes and products using human-centred design in pursuit of continuous improvement

- Use human-centred design techniques such as process mining to identify which parts of a process or product will generate a high risk of breaches and iterate to mitigate this risk and test further until resolved.
- Front-line staff are well positioned to contribute to the effective design of products, systems, processes and technologies. Collaborate to understand customers' needs and gaps in the banks' capability to meet those needs.
  - *For example, a staff member reports that the collection system failed to suspend collections activity even though a formal complaint had been lodged by the customer. This type of staff or customer feedback should be cause for immediate system review and iteration to prevent recurrence.*
- Use bank-specific breach data to identify Code processes that are subject to breaches (particularly those where human error is deemed to be the cause) and proactively review process/system design for opportunities to streamline, and possibly automate for improved compliance outcomes.
  - *For example, collaborate with relevant staff to examine the end-to-end direct debit cancellation process using human-centred design to identify where steps are being duplicated and bottlenecks occurring, and to highlight areas for improving the process.*

## Consolidate data from multiple channels on a central platform to get a holistic view of Code compliance and to ensure breaches are all captured

- Complaints and incidents data should be centralised to get the full picture of the level of compliance. It will enable the identification of systemic issues to be corrected and will support more reflective self-reporting to the BCCC.
- Customer management systems (CMS) should be designed to give a holistic view of the customer's relationship with the bank that goes beyond individual products and accounts.
  - *For example, lending and collection staff alike, should be able to utilise the CMS profile to deliver a tailored and consistent interaction that meets the customer's needs.*

## Integrate learning and technology in a way that increases staff engagement, self-guided learning and compliant outcomes

- Build guided learning and directions into systems – Code requirements flagged or automated in workflows reduce the need for employees to remember everything.
- Consolidate the different Code, legislative and regulatory requirements into a central 'obligations libraries' to simplify compliance for employees and promote as a self-service reference tool.
- Integrate digital guided learning platforms with incident management systems to make it easier for employees to navigate and report compliance issues.

- Provide employees with a dedicated way to ask questions about Code compliance matters and receive answers in real time, leveraging technology where possible.
  - *For example, create a dedicated internal platform or inbox that is actively monitored by relevant risk and compliance functions who field on the job questions from front-line staff.*

### **Develop and adopt real-time reporting and analysis to proactively prevent and detect Code breaches**

- Incorporate flags and triggers into systems and processes to proactively prevent breaches from occurring.
  - *For example, some banks have systems that help identify and interact with vulnerable customers through the use of flags and pop-up boxes with notes to prompt staff to tailor their approach for the customer in future interactions.*
- Leverage existing data to proactively scan for issues and prevent poor customer outcomes.
  - *For example, define common scenarios to identify customer cohorts that may be more vulnerable to elder financial abuse, fraud or scams – any funding requests outside of the customers usual behavioural pattern can prompt a review and a tailored customer approach to mitigate the risk before it happens.*
- Ensure systems have built-in triggers for Code requirements relating to timeframes.
- Automate processes so that when breaches do occur, they are captured in real time, the appropriate personnel are alerted promptly to take action, and breach alerts and accurate reporting do not rely on manual intervention.

# 4. CULTURE



The Financial Services Royal Commission had much to say about poor organisational culture and the role it played in causing much of the misconduct that was exposed throughout the inquiry. Regulators and the community at large expect banks to embed a strong organisational culture that champions fairness, honesty and transparency. A good organisational culture ensures that staff behaviours are not guided by misaligned incentives and conflicts of interest as staff are encouraged to ‘do the right thing’ even when no-one is watching. The Royal Commission also made it clear that culture, remuneration and governance are linked, and an integrated approach is needed.

The previous recommendations in this report - about impactful communication, effective learning and development and designing system, processes and technology with customers and employees at their heart – should all be underpinned by an organisational culture that is committed to supporting continuous improvement, Code compliance and good customer outcomes.

This section of the report builds on these recommendations to help banks to more consistently put the spirit of the Code at the centre of decision-making and empower employees to do the right thing.

## **INDUSTRY INSIGHTS: WHAT ARE THE CHALLENGES AND THREATS?**

To find out how closely aligned Code compliance is to a bank’s organisational culture, participants were asked what barriers, if any, are currently preventing employees from doing the right thing by the customer, and how they think those barriers can be overcome.

### **Culture, reward and recognition**

Some participants, particularly those in frontline roles, said they are reluctant to raise compliance issues and report breaches for fear of being reprimanded or negatively impacting performance outcomes. It was noted that positive organisational cultures, where people feel psychologically safe to discuss breaches or compliance issues, encourage employees to proactively log incidents and suggest improvements.

### **Incentives**

Participants reported that employees’ key performance indicators (KPIs) may not encourage breach prevention or reporting. Frontline employees, for example, said some

KPIs, such as the number of customer calls they take, preference productivity over good customer outcomes. Performance measures that encourage employees to focus on efficient behaviour rather than getting the best possible result for the customer may lead to breaches being unreported or missed.

## WHAT ARE BANKS DOING WELL?

There is evidence from larger banks that they are structuring the organisation to better enable Code compliance, with dedicated roles or committees (for example, a team to support customers in vulnerable situations and a dedicated channel for lodging complaints) responsible for promoting compliance. Dedicated roles or committees can act as a central point within the bank to target issues no matter where they originate, while also centralising accountability for compliance.

During product and program planning, banks are increasingly using human-centred design approaches, such as the development of personas, scenarios and immersive workshops, to better understand customers and what is important to them. Considering programs and products from the viewpoint of the customer also facilitates Code compliance, as it puts the customer at the centre of decision-making.

## RECOMMENDATIONS FOR ACHIEVING BETTER PRACTICE CULTURE

In the Financial Services Royal Commission's Final Report, Commissioner Hayne indicated that some financial services firms did not give compliance staff a strong enough voice in the business and failed to devote adequate resources to compliance.

Banks should use the following recommendations to self-assess their organisational culture and its role in driving customer-centric decision-making, empowering employees to proactively raise issues and promote 'getting things right' as a valued behaviour that contributes to continuous improvement.

### **Reinforce a culture that links employee compliance to clear customer outcomes and fosters a continuous improvement mindset**

- Foster a culture of psychological safety, where leaders actively listen, empower employees to speak up, show vulnerability and share personal stories. Emotionally secure employees are more likely to be engaged, productive, innovative and able to focus on effectiveness in achieving customer outcomes over task efficiencies.
  - *For example, front-line staff should be empowered to escalate or propose to triage a complex customer issue to a more senior decision-maker to achieve the right outcome – and feel supported to do so.*

- Annual risk forums and relevant internal committee meetings, should be open to relevant front-line staff who play a role in Code compliance. This is a great opportunity for employees to share practical knowledge, share any barriers to compliance and good practice.
- Build dedicated teams or champions focused on Code compliance across business units in the organisation.

### **Review reward and recognition programs to link employee incentives to positive customer outcomes and avoid creating incentives that undermine those outcomes**

- Align employee remuneration with customer-centric cultural values, not just revenue and cost focused KPIs.
- Develop a set of non-financial incentives that motivate and recognise front-line staff for their contribution to good customer outcomes and upholding the banks' commitment to customers.
  - *For example, a branch staff member taking ownership and supporting a customer in a vulnerable situation with sensitivity, compassion and respect, until the right outcome was achieved - could attract a congratulatory email from a senior executive or special mention in monthly branch network communications.*
- Set KPIs that reward desired behaviours and good customer outcomes rather than just achieving efficiencies. Regularly test and iterate these to ensure they are achieving their intended purpose.
  - *For example, develop metrics to assess the quality of customer conversations, and whether staff tailor their approach based on the customers' needs - across the various front-line channels.*
- Review KPIs to ensure that these desired behaviours are not deterred but encouraged. Front-line staff that proactively detect and escalate compliance issues should be viewed as demonstrating desirable behaviour that reflects the banks' commitment to the Code.

### **Bridge the gap between different bank functions through formal and informal feedback loops**

- Connect employees who drive compliance in the business with those who need to comply.
- Encourage all staff to take ownership of compliance issues and to escalate incidents through the appropriate channel.
- Create front-line team familiarity with compliance requirements (for example, accredit team 'champions', attend forums), facilitate regular collaboration with Risk & Compliance teams to ask questions, develop understanding and close feedback loops.

### **People leaders should model the desired behaviours and expectations that demonstrate a customer-centric approach and the spirit of the Code.**

- Encourage reflective practice by frontline employees of potential non-compliant behaviour and failing to meet a commitment made to their customer. Provide guidance so they know what they need to do differently in the next customer interaction.
- Dedicate time to provide regular compliance coaching to employees. Do not wait until breaches have occurred or the employee's annual performance management meeting – raise issues as soon as they occur as this demonstrates they are a priority to resolve.
- Use physical reminders in the team to promote and keep Code compliance front of mind, particularly for front-line roles. This might include posters that promote the benefits of Code compliance for customer outcomes.

### **Create relationships between banks to share success stories and best practice**

- Use industry associations to share information, discuss issues, develop standards and establish best practice initiatives within the industry.
- Use success stories and generate newsletter or digital forums to share what works well for Code compliance in your organisation.

# 5.

## ENHANCING CAPABILITY THROUGH ROBUST COMPLIANCE FRAMEWORKS



The BCCC has flagged its concern in previous reports about the adequacy of some banks' compliance frameworks to identify and address the genuine root cause of Code breaches. The consistently high number of self-reported Code breaches attributed to human error in recent years suggests that banks' compliance frameworks do not include sufficient measures to prevent human error related breaches from recurring.

There is also evidence that the way banks are remediating and managing these breaches is to carry out routine compliance training rather than enhance monitoring, fix systems or improve processes. For example, banks' 2018-19 breach data indicated that they remediated 58% of breaches through employee training, coaching or feedback. By contrast, just 16% of breaches were remediated through enhanced monitoring, 12% through fixing systems and another 12% through process improvement.

This section provides banks with guidance on how to strengthen their Code compliance frameworks, accurately identify breaches, drill down deeply to find their root cause, and prevent them from occurring again.

### COMPLIANCE CAPABILITY TOOLS

Compliance frameworks must be robust and able to rigorously prevent, identify and examine Code breaches when they happen, as well as determine actions to prevent recurrence. As part of Deloitte's research into organisational capability, they have developed compliance capability tools which consider best practice and insights from banks' current practices. They consider what is working well and identify where effort should be focused to support Code compliance. The purpose of the tools is to build bank capability and assist employees with compliance.

The compliance capability tools focus on two key processes: review and prepare; and recommended practice.

#### Review and prepare

This is a clear and simple three-step process that bridges the gap between the different functions that drive compliance. It can be used by different parts of the bank, such as Risk and Compliance, Learning and Development, and Incident and Complaints Management, to identify and understand why breaches occurred. This helps to inform the design of appropriate interventions or initiatives to reduce or prevent breaches.



## 1 INVESTIGATE

- Understand what, where and why breaches occur.



## 2 PLAN

- Devise actions to fix current breaches and prevent future breaches.



## 3 MONITOR

- Measure the impact of actions on Code breaches.

### Implement recommended practice

These initiatives have been identified as ones that will help shift employees from awareness of the Code through to adoption. Earlier in this report, four key areas were identified as focus areas where banks can improve compliance capability. Better practice recommendations have been made across these themes and the BCCC encourages banks to implement them where appropriate to improve compliance capability.

### PROACTIVE IDENTIFICATION AND ESCALATION OF CODE ISSUES

As part of Code compliance, all subscribing banks must have processes to identify Code breaches. They must then investigate, record and report Code breaches appropriately. An escalation process for Code breaches that are serious or systemic should also be in place and used when required. Building a positive compliance culture that reflects the recommendations outlined earlier in this report will ensure employees feel comfortable to follow these processes and speak up when there is a problem.

### INVESTIGATION OF CODE BREACHES AND ROOT CAUSE ANALYSIS

Investigating breaches is necessary to identify the issue and develop remediation actions to reduce the likelihood of recurrence. It helps banks understand what, where and why breaches occur.

Initial investigation should include these focus questions:

- What constitutes a breach?
- Where are our issues occurring?
- What is causing our issues and resulting customer impact?
- What is our goal for reducing and preventing breaches?

### Root cause analysis

Conducting root cause analysis is imperative to identify the real cause(s) behind an incident or breach and help to inform the design of interventions. See [Appendix 2](#) for a Root Cause Analysis Template.

Root cause analysis involves a four-step process to identify the genuine root cause of a Code breach:

- STEP 1** Start with the problem statement. Be as clear and specific as you can.
- STEP 2** Use a series of “5 Why” questions to drill down into successive layers of a problem. Frame each question in response to the preceding answer. This helps to peel away symptoms to get to the root cause. Use the “5 Why” questions for any primary causes and contributing problems related to your overarching problem.
- STEP 3** Organise related causes into categories to assist with development of corrective actions.
- STEP 4** Design corrective actions using the categories of the four drivers that are key to Code compliance: communication strategy, learning and development, systems, processes and technology, and culture.

Conducting genuine root cause analysis to identify the issue enables an organisation to develop actions and deadlines to fix these issues and prevent breach recurrence.

## REMEDIATING BREACHES AND PREVENTING A RECURRENCE

Once the genuine root cause or causes are established for known issues, a broad range of control interventions are available to remediate Code breaches and prevent recurrence. In many instances, more than one intervention will be needed.

With the high incidence of breach causes being attributed to human error, banks self-reported that they focused on employee training as a remedial action to prevent breach recurrence. They also used several other interventions to a lesser extent. However, in preparing this report, it has become evident there are many underlying factors that contribute to employee capability in complying with the Code.

After determining root cause analysis, the next steps of planning and monitoring in the Review and Prepare process are critical to Code breach remediation. See [Appendix 3](#) for an Action Plan template.

### Planning actions

This step involves devising actions to fix current and prevent future breaches.

Focus questions:

- What actions can we take to address issues? See 'Corrective action to take' at [Appendix 2](#).
- How do we implement any proposed changes to ensure they have the intended impact?

Actions may be prioritised depending on impact and effort to implement. Any interventions should be tailored to the audience for maximum engagement and a stakeholder engagement plan.

### Monitoring impact

The final step is measuring the impact of actions on Code breaches.

Focus questions:

- What is the right approach to monitor how the action planning is going?
- How are we tracking against:
  - ▷ *our goals?*
  - ▷ *our action plan?*
  - ▷ *the impact of our action plan?*

Planning and monitoring activities can be outlined using an action plan that tracks remediation actions. An action plan should include the following elements:

**1) Area for improvement**

- ▷ Describe the issue or problem
- ▷ Identify the issue type and populate root cause(s) from the root cause analysis

**2) Quality improvement actions**

- ▷ Describe the actions required to resolve the issue
- ▷ Assign owners to the actions
- ▷ Set a deadline for completion

**3) Monitoring of remediation**

- ▷ Identify owners of monitoring actions
- ▷ Identify the method of monitoring
- ▷ Identify the timeline for monitoring

Employees who are fixing breaches should be encouraged and should have the capability and support to use the recommended practice outlined in earlier sections of this report. By following the three Review and Prepare process steps – investigate, plan and monitor – it completes a feedback loop back to employees and the compliance framework controls.

# Appendices

# Appendix 1

## SUCCESS STORIES TEMPLATE

Recommended practice for communications include memorable messages that use story telling principles and compelling narratives. Consider the following four points when constructing communications.

**1**

**ISSUE**

Bank X had 8 months to roll out the refreshed 2019 Code of Practice. Given the scale of changes required in the bank to comply, this was deemed an impossible task given the short time frame.

**3**

*"It costed the bank over \$100M to roll out the new Code. It was a highly disruptive exercise. The key to getting buy-in from staff was the story that we're doing this for our customers."*

**2**

**SOLUTION**

A cross-functional taskforce of 400 people were stood up tasked with rolling out the Code. The program of work had multiple work streams with different owners. The focus was on training and learning due to the cost-effectiveness and fast benefit realisation, compared to long lead-time system and process changes. The key to getting buy-in from staff was a narrative focused on customers.

**4**

**IMPACT**

300 new learnings were created in a short period of time. Careful coordination of training rollout ensured a large number of staff were trained on the new requirements while minimising disruption to the business. Staff reported fairly good level of understanding of the Code during the time of rollout.

- 1) Describe the issue. Be as clear and specific as you can.
- 2) Describe the solution or approach to solve the issue.
- 3) Use an attention grabbing quote from a customer or employee to highlight importance and make it real.
- 4) Describe the outcome of the solution and how it solved the issue.

# Appendix 2

## ROOT CAUSE ANALYSIS TEMPLATE

A root cause analysis template should incorporate the following four points to help banks investigate the root causes of breaches. This tool should be used when there is a reoccurring high impact type of breach and encourages the individual or team to utilise reflective practice to understand primary causes and contributing problems.

PROCESS	BUSINESS UNIT	COMPLETED BY	DATE	
<b>1 DEFINE THE PROBLEM:</b>				
<b>2 WHY IS THIS A PROBLEM?</b>			<b>4 CORRECTIVE ACTION TO TAKE:</b>	
<b>PRIMARY CAUSE:</b>		<b>ROOT CAUSE:</b>		
WHY IS IT HAPPENING?	▶ WHY IS THAT?	▶ WHY IS THAT?		▶ WHY IS THAT?
				<b>3 WHY IS THAT?</b>
<b>CONTRIBUTING PROBLEM:</b>		<b>ROOT CAUSE:</b>		
WHY IS IT HAPPENING?	▶ WHY IS THAT?	▶ WHY IS THAT?	▶ WHY IS THAT?	
			<b>WHY IS THAT?</b>	
<b>OTHER CONTRIBUTING PROBLEM:</b>		<b>ROOT CAUSE:</b>		
WHY IS IT HAPPENING?	▶ WHY IS THAT?	▶ WHY IS THAT?	▶ WHY IS THAT?	
			<b>WHY IS THAT?</b>	
			<b>CLASSIFY &amp; DESCRIBE CORRECTIVE ACTION</b> <ul style="list-style-type: none"> <li>• Communication Strategy</li> <li>• Learning and Development</li> <li>• Systems, Processes &amp; Technology</li> <li>• Culture.</li> </ul>	
			<b>CLASSIFY &amp; DESCRIBE CORRECTIVE ACTION</b> <ul style="list-style-type: none"> <li>• Communication Strategy</li> <li>• Learning and Development</li> <li>• Systems, Processes &amp; Technology</li> <li>• Culture.</li> </ul>	
			<b>CLASSIFY &amp; DESCRIBE CORRECTIVE ACTION</b> <ul style="list-style-type: none"> <li>• Communication Strategy</li> <li>• Learning and Development</li> <li>• Systems, Processes &amp; Technology</li> <li>• Culture.</li> </ul>	

- 1) Start with the problem statement. Be as clear and specific as you can.
- 2) Use a series of 5 Why questions to drill down into successive layers of a problem, peeling away the symptoms to get to the root cause.
- 3) Organise related causes into categories to aid design of corrective action.
- 4) Think holistically when designing corrective actions using pre-populated categories of drivers key to Code compliance.

# Appendix 3

## ACTION PLAN TEMPLATE

Once a root cause analysis or investigation of a breach has occurred, an action should be logged to track remediation actions. An action plan template should include the following three elements.

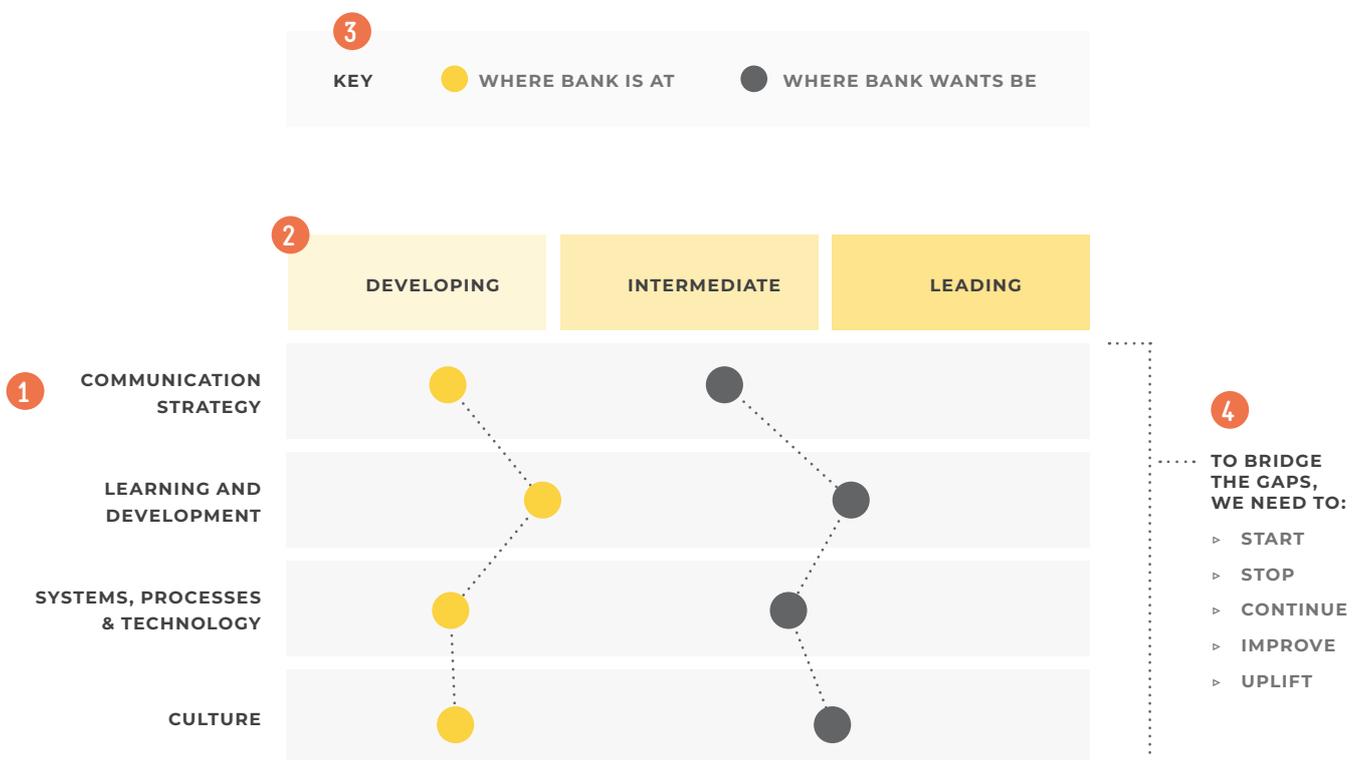
PROCESS		BUSINESS UNIT		COMPLETED BY		DATE		
1 AREA FOR IMPROVEMENT			2 QUALITY IMPROVEMENT ACTIONS			3 MONITORING OF REMEDIATION		
Issue	Significant or reoccurring (S/R)	Root cause	Remedial actions	Who is responsible?	Deadline for output	Who will monitor quality improvement actions?	Method of monitoring	Timeline for monitoring
Fail to recognise elderly customers as vulnerable	R	Staff not trained on identifying all customer groups	1. Develop scenario training for each customer group 2. Create guides listing vulnerable customer groups	1. xx from learning	20/02/2021	Senior leader L&D	Staff surveys	12 months post roll out

- 1) Describe the issue or problem, identify the issue type and populate root cause(s) from root cause analysis completed in the 'Investigate' step.
- 2) Describe the actions required to resolve the issue, assign owners and set deadline for completion.
- 3) Identify owners of monitoring actions, method of monitoring and timeline.

# Appendix 4

## MATURITY ASSESSMENT TOOL

In terms of Recommended Practice, it might be useful for banks to assess their current maturity and set a target state they would like to attain. A maturity assessment allows banks to consider current capabilities and where they wish to be given bank size, strategy and strengths. The assessment should include the following four elements.



- 1) Reflect on each capability driving Code compliance.
- 2) Rate maturity of each capability using a relevant rating scale. In this example, 'developing' denotes low maturity and 'leading' denotes high maturity.
- 3) Denote current state maturity and desired future state.
- 4) Describe what the bank needs to do to bridge the gap towards the desired future state.

# Appendix 5

## ABOUT THE BCCC

The BCCC is an independent compliance monitoring body established under clause 207 of the Banking Code of Practice.

The BCCC's purpose is to monitor and drive best practice Code compliance. To do this, the BCCC:

- examines banks' practices
- identifies current and emerging industry wide problems
- recommends improvements to bank practices, and
- consults and keep stakeholders and the public informed.

The terms that govern the functions and operations of the BCCC are set out in its Charter.

In accordance with clause 13.2 of the Charter, the BCCC has published its [2020-21 Business Plan](#), which is intended to be read together with its [2018-21 Strategic Plan](#) and sets out the BCCC's key priorities and focus areas during the 2020-21 period.

The BCCC has identified the following focus areas for its monitoring program for 2020-21:

- Customers experiencing vulnerability
- Small business and farming
- Data Collection through the Banking Code Compliance Statement program
- Financial difficulty
- Guarantees, and
- the cancellation of Direct Debits.

Through its risk-based approach to monitoring, the BCCC also conducts targeted inquires and investigations into emerging issues that may represent serious and/or systemic non-compliance with the Code.

Further information about the BCCC and members of the Committee is available on the BCCC's website - [bankingcode.org.au](http://bankingcode.org.au).

# Contact details

 [bankingcode.org.au](http://bankingcode.org.au)

 [info@codecompliance.org.au](mailto:info@codecompliance.org.au)

 PO Box 14240  
Melbourne VIC 8001

 1800 931 678  
(This is a telephone service provided by  
AFCA – please ask to speak to the Code  
Compliance and Monitoring team)



**BCCC**  
Banking Code  
Compliance Committee