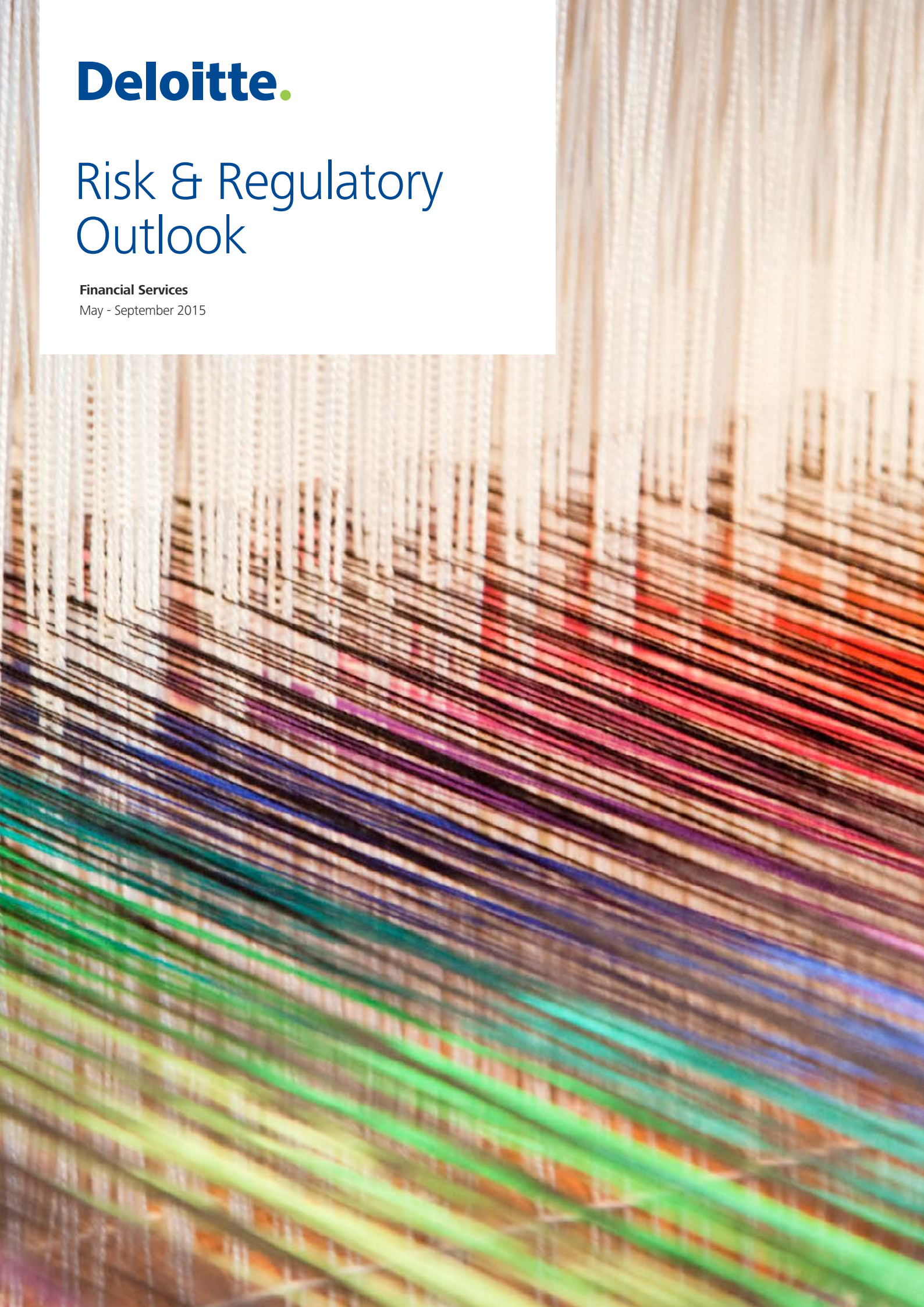
Deloitte.

Risk & Regulatory Outlook

Financial Services

May - September 2015



Executive summary

In our view four Cs will dominate the outlook for the financial services regulatory and risk management environment throughout the next twelve months at least. The Cs, as we conveniently term them, include the Australian Securities and Investments Commission Chairman's nominated potential Black Swan event, 'cyber', the Financial Stability Board and David Murray's Financial Systems Inquiry's focus on 'capital', a key focus for all organisations internationally and domestically 'conduct', and 'continuous change'.

In this Outlook we consider regulatory productivity, FATCA, OTC derivatives and breach reporting within the privacy reforms as part of continuous change – continuous change for better performance, for productivity, for improved governance and the ability to sustain good outcomes for customers and shareholders alike.

As with any reforms there is often short term pain for longer term gain – but in the long run the industry would all agree that the most important result is to secure a stable, safe and strong Australian system; a system capable of riding the vagaries of volatility, and managing the uncertainty of any future 'Black Swan' events.

In this edition of Risk and Regulatory Outlook a Deloitte subject matter expert outlines the situation, specifies existing or prescient change, and suggests practical steps in each of the nine key areas of regulatory change we focus on.

As always we trust your organisation will find this Outlook useful and pertinent to your business.

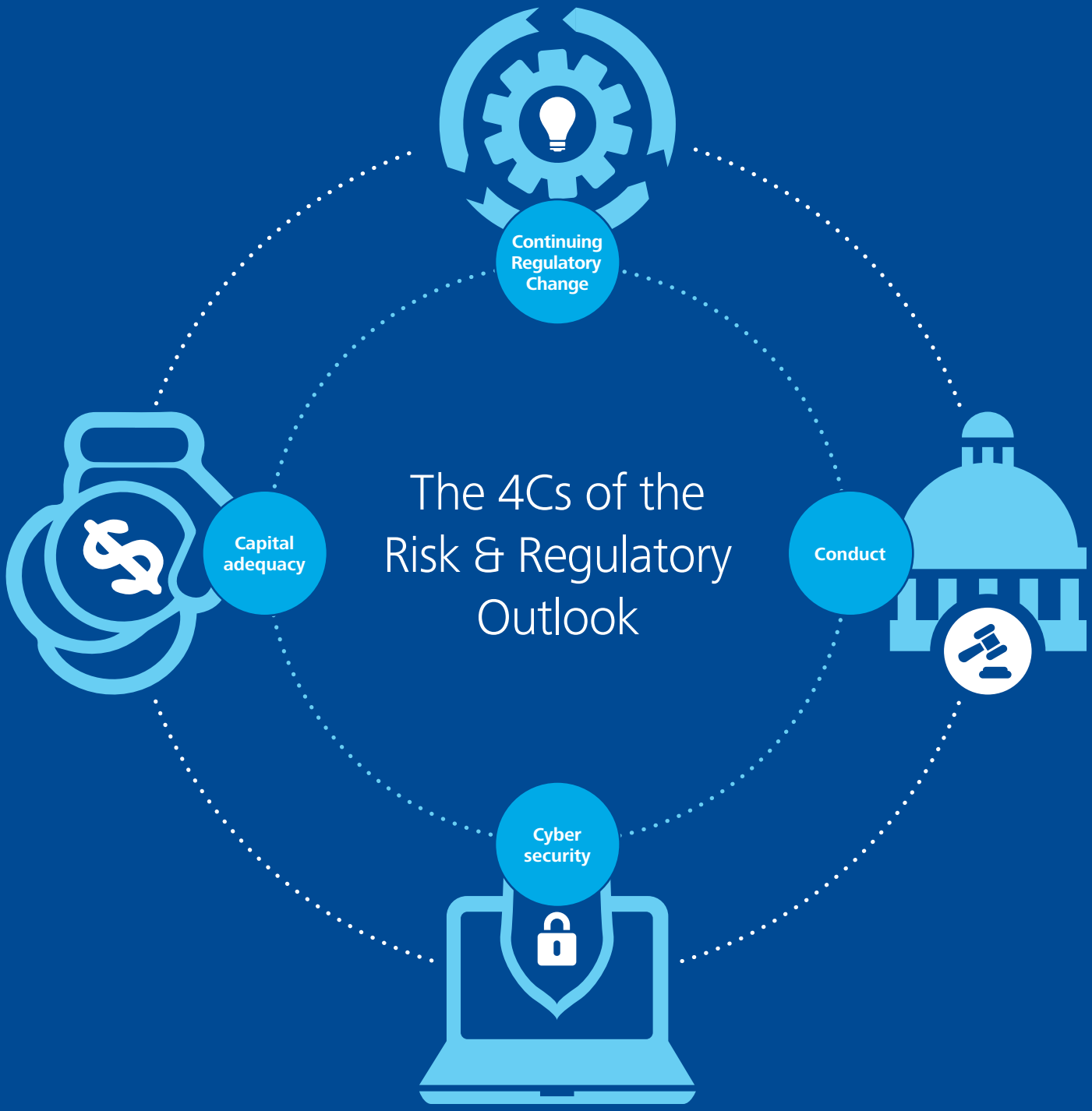
We look forward to meeting with you to discuss specific aspects as they relate to your organisation and ask that in the meantime you reach out to either of the three of us, or your specific contact as listed on page 19 for further immediate clarification or discussion.

Kevin Nixon
Lead Partner,
Risk & Regulatory,
Financial Services

Tim Oldham
Lead Partner,
Risk & Regulatory,
Banking

Sarah Woodhouse
Lead Partner,
Risk & Regulatory,
Wealth Management

Table of contents


Continuing Regulatory Change
Capital adequacy
The 4Cs of the Risk & Regulatory Outlook
Conduct
Cyber security

Benchmarks and wholesale market conduct reform

Restoring integrity to benchmarks and wholesale markets is a priority for regulatory policy makers. More activities are becoming regulated and authorities are coordinating policy development and enforcement across borders. **Martin Joy** explores how organisations need to assess their existing policies and processes against emerging standards and plan strategically for the changing regulatory and market environments.

Wholesale markets reform

The UK Fair and Effective Markets Review consultation paper raises questions on a number of aspects of the wholesale markets and the prospect of international coordination on reform.[9] Coordinated work on conduct standards and enforcement through 2015 has been already discussed at IOSCO's February Board meeting[10] and highlighted in FSB Chairman Carney's February 2015 letter to the G20.[11]

It will be necessary to engage with this policy process through 2015 and prepare for more extensive regulation of wholesale markets.

Remedial expectations

Benchmark manipulation and failings that allowed this manipulation have resulted in significant fines and remediation orders. These remediation orders are extensive and require affected organisations to assess and improve their standards. In fact the orders are an excellent way for organisations to assess their existing standards against emerging expectations.

The most detailed publicly available orders are those of the Office of the Comptroller of Currency (OCC) on FX benchmark manipulation.[1] They set out remedial expectations that cover board management and oversight, compliance risk assessments, compliance monitoring and assessment and internal audit. Critically, the OCC orders require the risk-based application of remedial measures to other wholesale trading activity.

Organisations should also refer to the Financial Stability Board's (***FSB***) September 2014 report on FX benchmarks.[2] This contains seven recommendations that apply to market makers and banks in the FX market. Reserve Bank Deputy Governor Guy Debelle (co-chair of this FSB work) has stated his expectation that these recommendations will be implemented.[3]

Combining the remedial orders and the FSB recommendations, organisations could review their wholesale trading operations against the following:

- **Governance** – ensure there is Board-level support for an adequate oversight regime that applies to wholesale trading activity
- **Culture** – foster a culture of integrity within the trading business
- **Conflicts of interest** – protect client and organisation confidential information and consider separation of fixing and other trade flow
- **Compliance** – adopt a comprehensive trading and communications monitoring system that covers all communication modes and is continuously updated for lexicon changes
- **Pricing** – consider transparent pricing structures for benchmark transactions.

Organisations should also consider whether the recently released Codes of Best Market Practice and Shared Global Principles from the foreign exchange committees require any changes to their practices, policies and procedures.[4]

Regulatory Policy Reform

These remedial steps represent current regulatory expectations. We anticipate the following substantial regulatory reform:

Regulation of benchmarks

Both administering and submitting to benchmarks are becoming more heavily regulated activities.

The International Organisation of Securities Commissions (***IOSCO***) released principles in 2013 that apply to all benchmark administrators.[5] These principles include a code of conduct for benchmark submitters.

The UK has taken this further and is extending regulation to important benchmarks (originally LIBOR, with a further seven recently included).[6] A benchmarks regulation is currently being developed in the European Union.[7]

Benchmarks are also being reformed through the FSB's FX and interest rate work. On interest rate benchmarks, this will mean existing inter-bank offered rates incorporate more transactional data (so-called IBOR+ rates) and risk-free rates developed or more widely used, particularly for derivative transactions.[8]

Organisations should prepare for benchmarks to change in response to these dynamics.

Product governance

With confidence in disclosure dying, regulatory policy makers are asking financial organisations to focus on product quality as well as information quality. **Martin Joy** and **Rosalyn Teskey** consider how the concept of product governance captures a series of actions by issuers and distributors that are intended to deliver the right product to the right customer. They outline ways Australian organisations can prepare for a product governance obligation by considering how they design, distribute and assess the performance of products.

What is product governance?

The Financial System Inquiry (FSI) has recommended that Government 'introduce a targeted and principles-based product design and distribution obligation.'[12] This would mean issuers and distributors must consider customers' needs and capabilities when designing products and deciding on distribution channels. The intent is that customers end up with products designed and sold in a way that matches their circumstances. The importance of customer-centric product design and distribution is also emphasised in ASIC's 2015 Strategic Outlook[13] and its work on complex products.[14]

Organisations should consider any product governance obligation in the context of the FSI recommendation that ASIC has a product intervention power to ban products or product features where customer detriment is anticipated.[15] Obviously any such intervention against an organisation or product would have significant reputational consequences.

Both recommendations draw heavily on offshore regulatory toolkits. Product governance was highlighted by IOSCO in connection with retail structured products[16] and it is also in the UK[17] and in the European Union through MiFID II.[18] Product intervention is also evident in Europe through powers granted to the UK FCA and European Union wide powers under MiFID II.[19]

Thinking strategically

Whether the Australian government adopts the FSI's recommendations or not, organisations should be upping their focus on product design through a customer suitability lens. They should get better at considering distribution strategies as part of their overall conduct risk approach and as they understand their customers' capabilities and needs, integrate this with their product design processes and distribution strategies.

As Australia moves to facilitate innovative and interactive disclosure and sales techniques, as foreshadowed by the FSI[20] and ASIC's Consultation Paper CP224[21] organisations should also think more about what their digital customer engagement environments will look like, and how they can be designed to ensure good customer outcomes.

Practical steps

Most organisations will have a new product approval process and to align these processes with emerging product governance expectations they should make sure they have a value-chain approach to their products.

The following questions across four elements of the value-chain should help:

Pre-sale

- Use research to expand existing research around customers and their needs and capabilities
- Incorporate these needs and capabilities into product design.

Distribution

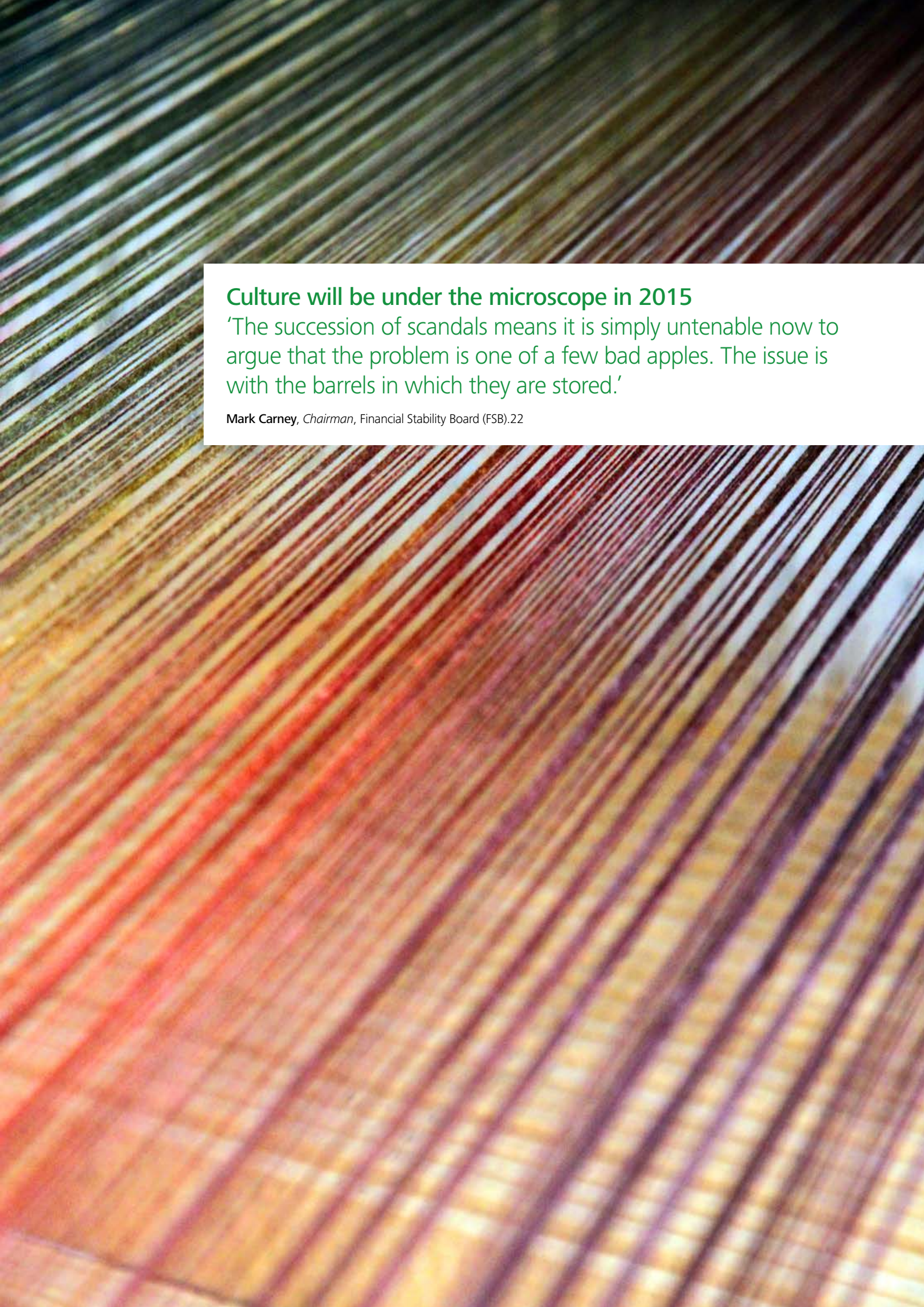
- Determine the mechanisms used to ensure that the product reaches its intended market
- Re-align sales incentives to the organisation's and consumers' long-term interests.

Point of sale

- Consider how the organisation can improve the way it presents information to customers and intermediaries
- As the organisation moves towards digital disclosure, consider how it presents choices to customers – and identify the default choice presented
- Assess how well your disclosure techniques are working.

Post-sale

- Once issued, review product performance to continue to improve the way each product performs
- Monitor any complaints to assess if the product works as intended and promised
- Ensure any insights from this monitoring are fed back into the product design process.



Culture will be under the microscope in 2015

'The succession of scandals means it is simply untenable now to argue that the problem is one of a few bad apples. The issue is with the barrels in which they are stored.'

Mark Carney, *Chairman*, Financial Stability Board (FSB).22

Risk culture

The recent culture conversations globally have been elevated through the current round of investigations into wholesale market conduct.[23] The FSB stated recently that 'The scale of misconduct in some financial institutions has risen to a level that has the potential to create systemic risks.' **Grant MacKinnon** outlines why the focus on conduct must also consider organisational culture, as even the best laid plans and processes are subject to weaknesses that stem from collective judgement and behaviour.

Raising awareness of the vulnerability

While many financial services organisations have taken deliberate steps to understand their risk cultures, there is considerable variability in their sophistication and the extent to which risk culture insights underpin organisational change. The CPS220[24] implementation has meant that most banks in Australia have programs underway to understand their risk culture and report on that to their Boards.

In a Deloitte benchmarking review of CPS220 risk culture responses we found the most common risk culture assessment approaches rely on surveys to identify cultural weaknesses. However, only a few organisations have a clear understanding of the behavioural root causes of these cultural weaknesses. The assessment outcomes will typically focus on training and communications to reinforce expectations. Unfortunately these tactical levers alone have little impact on sustainable cultural change.

Also we often see multiple initiatives intended to strengthen culture, risk, or conduct within the same organisation. Aligning these initiatives and their associated incentives to improve risk-related outcomes continues to be an area of weakness for Australian financial institutions.

In larger organisations there may even be competing initiatives that confuse 'end users' in the business. For example; a strategic focus on organisational agility, growth, or client experience can mean that risk related controls are regarded as 'bureaucratic' and are rated 'less important'.

Organisations that take a holistic approach to risk and culture can on the other hand achieve clear synergistic benefits from aligning these areas of focus, as well as a much stronger approach to misconduct.

In the year ahead the FSB will consider reforms to focus on culture and reduce the likelihood of misconduct. These will include:

- Assessing reforms to risk governance, compensation structures and benchmarks and, where appropriate, proposing additional measures in these areas
- Considering ways to improve market structure, standards of practice and incentives for good conduct in financial markets more broadly.[25]

As the volume of regulatory criticism of culture gets amplified globally, Australian institutions will need to lift the sophistication and integration of their risk culture approaches beyond simply reporting them, and strive to achieve an improved insight into their overall culture to formulate what may need to be substantive change in business practices.

Immediate and practical steps to take

Organisations should develop a meaningful framework of sustainable change to:

- Understand the risk culture across the entire organisation
- Establish governance for culture across the three lines of defence
- Assess the controls framework to reflect cultural strengths and weaknesses
- Consider a cultural refresh program that implicitly embeds strong ethics and the effective management of all risk classes.

While the sophistication of approaches to understand and strengthen risk culture is expected to mature over time, Boards should also carefully scrutinise the frameworks and outcomes in relation to culture within their organisations.

Cyber resiliency

Cyber Threats are at the top of organisations preceived risks in 2015

Boards and the C-suite have recognised the threat and potential devastating impact of cyber related incidents. For many organisations cyber security and protecting confidential information is this year's top initiative but how do organisations achieve cyber resiliency and maintain continuous operations with minimal damage? What should organisations do?

As ASIC points out in its *Cyber resilience: Health Check (REP 429)* 'cyber resilience is an organisation's ability to prepare, respond, adapt and recover from a cyber attack'.

Gavin Cartwright specifies four important areas to think about:

1. The specific things organisations rely on as a business to be successful, and consider how each one could be impacted by a cyber incident
2. Understand your current and target future state
3. Apply the appropriate operating model, processes and technical controls that help organisations become secure, vigilant and resilient
4. How to measure and report on the ongoing effectiveness of your cyber resiliency.

Immediate and practical steps to take

1. Organisations need to know their business, and the critical areas they rely on. For example the key systems and processes organisations use to make products, sell services, distribute goods or collect payments. Organisations need to analyse how a cyber incident could potentially impact these areas, whether by causing a loss of availability or losing sensitive information. By doing this organisations develop a cyber risk-based view of the organisation and help focus cyber security efforts on the areas that really matter.

2. Next it is crucial to understand how mature your current cyber resiliency is. Map out your current-state in terms of the security people, processes and technologies in place and ascertain how effective those capabilities are. It's best to use a security capability framework that is based on recognised standards, and that has good coverage of the main security capabilities. A framework that is simple enough to explain easily to senior management.

   A future target state can then be proposed that takes into account areas of greater risk, and provides clarity on which capabilities have the biggest gaps between the current and target state.

3. Calculate what skills, processes and tools are needed to meet the capabilities proposed in the future state. These typically fit into three categories:
   - **Secure** – Establish controls to guard against known and emerging threats
   - **Vigilance** – Establish situational risk and threat awareness across the environment to detect violations and anomalies
   - **Resilience** – Establish the ability to handle critical incidents quickly, and return to normal operations, as well as repair damage to the business and brand.

4. Finally, in order to provide ongoing measurement and reporting on the organisation's new top risk, 'cyber', it is necessary to establish suitable metrics and reporting processes that effectively present the status of this risk. However this is not straight forward.

   It takes knowledge of real-time network and system events, accurate manual reporting on incidents, and suspicious behaviour and actionable external threat intelligence.

   Additionally it is also difficult to take what is typically a very technically focused report and bring it up to a level that depicts the business impact and overall cyber resiliency status, so that it resonates with the board and C-suite. It is critical that the board and senior management can recognise and authorise appropriate levels of focus and funding to address unacceptable levels of cyber risk.

For a detailed breakdown of cyber resilience health checks, especially if organisations are a director, a listed entity, a responsible entity, a corporation or an AFS licensee, see ASIC's ***Cyber resilience: Health Check (REP 429)***.

Bank capital: significant changes ahead

Basel 4 is on the way: In 2015 there will be significant changes made to the Basel capital framework for banks. Work underway will see comprehensive revisions to the standardised approaches for credit, market and operational risk. In addition internal models will be subject to greater constraints in their calculations, and will be subject to an overall floor against the standardised frameworks. At the same time, author **Kevin Nixon** notes, the Basel Committee will consider at a more fundamental level whether to continue with internal models altogether for regulatory capital purposes.

Redesigning the capital framework

Revised standardised models for regulatory capital have now been proposed for all major risk classes. The new models have two key purposes:

1. Increasing the granularity of the current standardised approaches
2. Removing references to external credit ratings.

The proposed standardised models also remove any reliance on internal calculations. At the core of the new standard credit risk model are two-by-two look-up tables to calculate capital requirements.

Internal models

On internal models the Basel Committee has become increasingly concerned over the variance of risk-weighted asset calculations, and a general loss of credibility in the framework. As a result there are several streams of work underway, including tightening the definition of parameters, and modification of supervisory discretions.

However, while these may both have far-reaching impacts, the biggest impact by far will be the introduction of a floor applied to risk-weight calculations derived under internal models relative to standardised approaches. The Basel Committee is determined to implement this floor. Of this market participants should be in no doubt.

There is a more fundamental work stream underway already, driven by the loss of confidence in internal model approaches, that will consider whether internal models should remain part of the Basel Capital framework.

Given the work done to date by the Basel Committee and the conclusions it has reached, the removal of internal models, while not the base case, is looming larger as a possibility.

Implications for Australian banks

The reforms will have a major impact on all banks, but particularly those using internal models. All banks will have to implement the new standardised models, and the risk weights and drivers under those models will have an impact on business strategy and returns on equity depending on business mix.

The floors, depending on levels, will affect capital levels and the incentives to improve risk management under the internal model approach. However the work must also be looked at in the context of the final report of the FSI.

The FSI recommended, among other things, that APRA take steps to raise the average risk-weight for mortgages as determined under internal models. The Basel Committee work is far broader than the FSI recommendation, effectively seeking to tie internal model outcomes to standardised across all risk classes rather than just mortgages.

Influencing outcomes

Market participants should pay close attention to developments coming out of the Basel Committee this year. At a minimum, that would entail formally tracking the status and nature of proposals. However, banks should be assessing the impact on their own portfolios, and begin mapping potential impacts on business strategy. Australian banks should engage directly with the Basel Committee on these proposals, particularly as issues are brought to light under the suggested organisation-specific analysis.

Regulatory productivity in meeting the challenge of regulatory change

The increasing volume and complexity of the regulatory change pipeline, coupled with existing compliance requirements, will remain at elevated levels across financial services for the foreseeable future. In response, **Tim Oldham** argues, existing approaches to regulatory change management will need to evolve to productively address the pipeline.

We are living in a 'New Normal'

Regulatory change management will remain complex and challenging because of the:

- Difficulty for financial services players to develop clear and thematic regulatory strategies due to the volume and uncertainty of 'chronic crisis' regulation and the time it takes to finalise supervisory interpretations
- Key global regulatory reforms which remain subject to implementation timelines and the changing interpretations of multiple global regulators which are at times inconsistent or competing
- Regulatory uncertainty which means financial services players will remain subject to many 'unknowns'. When regulatory details are certain, plans can be implemented, but where many variables are 'known, unknowns' planning and possessing the agility to adapt, is difficult
- Uncertain impact on business strategy, appetite and operations. In the absence of clear business benefits, there are cost challenges in building ongoing regulatory changes into business planning, strategic thinking and capital allocation decisions
- Approaches to implementing regulatory change being dependent on the appetite and capability of financial services players and the tension between centralised oversight, versus decentralised implementation within the business
- Pipeline challenge with increased focus and pervasiveness of regulatory inquiries and actions that will continue to consume significant management resources and capability.

Do not ignore the blind spots

Financial services players need to enhance existing frameworks so that they can develop a regulatory change management toolkit that has:

- Clear situation awareness of the current and upcoming pipeline to be able to manage regulatory change productively without understanding what changes are coming and how they impact business and operations
- The ability to understand impacts on products and services and prioritise appropriate actions with a binary view on what it means to be compliant or non-compliant to business strategy
- Enhanced integration of regulatory change management with appetite and operations. Regulation impacts the markets in which businesses operate. Good regulatory change management will involve a decision as to whether to change strategic appetite and/or direction based on the assessed impact of regulation – e.g. do we comply with the regulation, modify strategy or exit a business?
- Developed or built fit-for-purpose regulatory implementation capability that complements change management processes across all business practices.

Build the organisation's regulatory change management toolkit

Immediate and practical actions to develop the organisation's toolkit can include a combination of:

- Enhancing regulatory advocacy and change processes to strategically review and build agility to manage the organisation's regulatory pipeline against business strategy, appetite and operations
- Assessing the organisations portfolio of regulatory projects against content complexity and cost in order to make informed decisions in prioritising regulatory change spend
- Analysing and, where determined, enhancing risk management capacity and capabilities to enable a consistent and coordinated method of addressing regulatory change implementation
- Mapping how regulatory change requirements can be built into end-to-end business processes across products and services from the perspective of the business-end user (so that regulatory implementation is an embedded business as usual activity).

Reflect on FATCA to move forward with CRS

CRS based on FATCA, but different

The OECD Common Reporting Standard (CRS) for the automatic exchange of information between tax authorities of signatory countries will apply to Australian financial institutions (FIs) from 1 January 2018 (or voluntarily from 1 January 2017). A number of other countries have committed to adopt the CRS from 1 January 2016 ('early adopters').

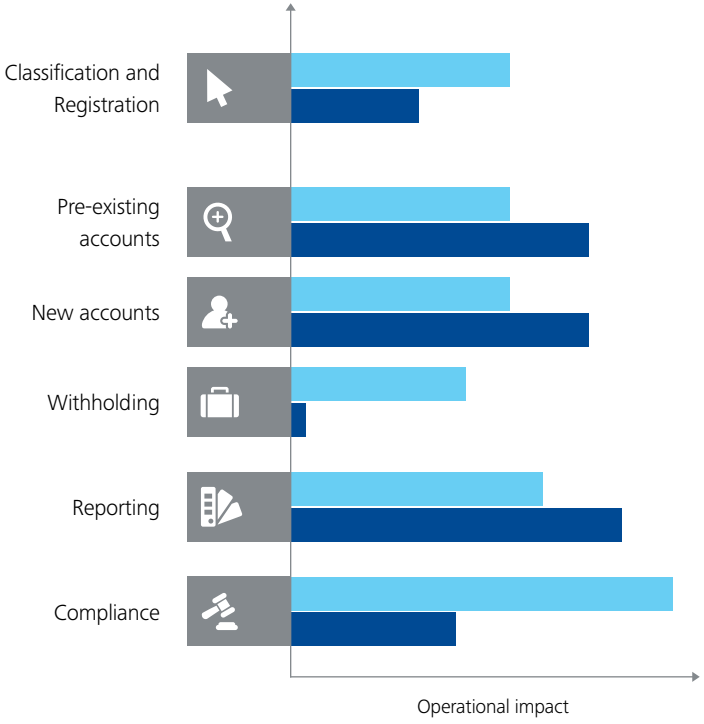
CRS is based on the intergovernmental agreements (IGAs) for the implementation of the Foreign Account Tax Compliance Act (FATCA) and, broadly, both CRS and FATCA impose compliance obligations on FIs to:

- Classify entities and products
- Identify and document pre-existing and new account holders
- Report information to tax authorities.

In this article **Alison Noble** outlines the differences between CRS and FATCA and what they mean. The two key differences to FATCA are that:

- The OECD has stripped out the U.S. centric aspects of FATCA to achieve a global standard, so that certain exclusions, exemptions and thresholds are not part of CRS
- Reportable accounts for CRS are determined by tax residency, which can be a more complex question than the U.S. person test for FATCA.

The technical differences between CRS and FATCA result in varying operational impacts and the diagram illustrates some of these differences.



- No central registration for CRS (such as via IRS FATCA-portal); potentially domestic registration under CRS
- No globally uniform identification number for FIs (such as GIIN)
- Certain non-reporting entities and excluded products for FATCA may be in scope for CRS.

- Potentially conflicting indicia indicating residence in multiple jurisdictions
- Population of accounts concerned much larger for CRS.

- Determination of tax residence is more complicated than U.S. person test
- No waivers required for CRS.

- No withholding imposed under CRS
- CRS may be linked with TRACE in the future.

- Number of accounts to be reported increases significantly for CRS
- Type of information to be reported mostly consistent
- Reporting via domestic tax authorities.

- No responsible officer concept foreseen (rather domestic audits)
- No group compliance required for CRS.

FATCA CRS

Reflect on the lessons learned from FATCA

Australian FIs invested significant time and resources implementing FATCA and the lessons learned can inform the approach for implementing CRS. We outline five lessons we have identified from FATCA implementation:

- The devil is in the detail of technical regulations and guidance, and also organisational information. A detailed understanding of both the technical and the organisational, correlated to a more thorough FATCA impact analysis is recommended
- A strong governance framework supported by documented roadmaps and defined roles and responsibilities is more successful
- The data can make or break organisations – from the volume and quality of data, to allocating sufficient resources to analyse the data in the required timeframe
- Identifying the legal and regulatory 'cans' and 'can nots' as early as possible, allowed sufficient time for changes to be made
- Collaborative communication with business units and other FIs created efficiencies drove a standard that was truer to the objectives of the rules, and reduced adverse impacts on the customer experience.

Moving forward: preparing for CRS

While 1 January 2018 seems some time away, FIs in Australia and other countries are starting to prepare. Preparatory activities should include:

- Ensuring that information about products, systems, processes and data collected for FATCA is available to recycle for CRS implementation
- Making strategic decisions on the implementation approach for CRS (e.g. dealing with different start dates within multinational groups, whether to comply from 2017 or 2018, wider approach or phased-in approach)
- Participating in consultation and the development of the law and guidance. The CRS is a global standard, but it is implemented through domestic legislation and guidance. So Australian FIs can influence exclusions and exemptions, as well as ways to determine tax residency and classify account holders
- Developing client and employee communication and information, taking into account cultural and language considerations
- Reviewing the data landscape, including information and data privacy constraints.

Next steps

In the next few months, Australian Financial Institutions should:

- Become familiar with the CRS and its commentary
- Get involved in consultation through the relevant industry body
- Set up a CRS project team that includes resources from FATCA and AML CDD teams
- Undertake a FATCA post-implementation review and gap analysis to assess the base for CRS implementation
- Start drafting requests for changes to technology, onboarding forms and processes.

OTC Derivatives

2015 will be a critical year for OTC derivatives regulation in Australia with much needed clarity on key aspects of the regulated anticipated for release. **Martin Joy** outlines the areas that organisations should watch out for throughout the year.

Reporting

ASIC has been implementing the requirement to report OTC derivative transactions on a phased basis. With larger OTC derivative market participants already reporting, Phase 3A entities started transaction reporting in April 2015.[26] Phase 3A entities will need to have their own reporting systems or rely on delegated reporting by counterparties. Clarity on liability for delegated reporting released in February 2015 by ASIC should make it easier to establish delegated reporting arrangements.[27]

In December 2014, the Minister announced that Phase 3B entities[28] would be able to rely on single-sided reporting where the counterparty is already required to report.[29] Detail on this relief has not yet been released. Before relying on single-sided reporting, Phase 3B entities should review this detail and verify that their counterparties are reporting as required.

Through 2015, all organisations should also be watching the international policy work on the global aggregation of reported data. The September 2014 Financial Stability Board report on this project recommended work on the harmonisation of aggregated data elements.[30] This could lead to changes in reporting fields.

Clearing

In July 2014, Treasury proposed a clearing obligation for US dollar, euro, British pound, yen and Australian dollar interest rate swaps for large financial institutions with significant levels of cross-border activity in the contracts.[31] Although Treasury proposed that a ministerial determination be released in H2, 2014, no further detail has appeared. This is another area where organisations will need to monitor developments.

Non-cleared transactions

We anticipate Australian regulators will consult on two sets of requirements concerning non-cleared OTC derivatives in 2015.

1. IOSCO released new risk mitigation techniques for non-cleared transactions in January 2015[32] which are intended to apply to the same entities subject to the margin requirements. They cover portfolio reconciliation and dispute resolution. IOSCO has asked for implementation as soon as practicable. As ASIC is the Australian member of IOSCO, it is reasonable to assume that it will take domestic responsibility for these requirements. Organisations should watch ASIC's releases to see if and how these requirements apply to them.
2. We now know that the BCBS/IOSCO margin requirements for non-cleared derivatives are scheduled to start 1 September 2016 (a delay of nine months from the original date).[33] These will require financial entities and systemically important non-financial entities (as defined domestically) to exchange variation margin and, over a four-year phase-in period, initial margin. While proposed domestic rules have been released offshore (reflecting the original implementation date), no such detail has appeared in Australia.[34]

Finalisation of the standardised initial margin model by ISDA will also help organisations understand the impact of these requirements.[35]

Additional developments

An emerging area of regulatory policy concern is the stability and oversight of central clearing facilities. Additional international and domestic policy work will occur on this throughout 2015.[36] In this vein, the Australian Treasury has just released a consultation paper on the resolution regime that should apply to financial market infrastructure.[37]

Also further, and much needed, work will occur on the cross-border application of domestic rules.[38]

Breach reporting as 'business as usual'

When did your organisation last stop to evaluate its internal breach reporting process to determine whether it really is an effective part of its 'Business As Usual' process? That time is now. **Tina Lin** looks at how organisations can determine how effective breach reporting is in the business.

As a compliance professional within an organisation, you have just been made aware of an incident by front line. The next step is to determine whether it is likely to be a breach and how significant a breach it is. Do you have all the information you need to make this assessment? Or is it a challenge to access this information easily and quickly? Is it clear who will actually make the decision on significance? And if this incident is determined to be a significant breach, does the 10 day clock start now? Or should your organisation wait until you have a better understanding of the size of the breach and whether any required action is complete before reporting to ASIC?

Note: A significant breach must be reported within 10 days from the date it was assessed as a significant breach to ASIC.[39]

While an organisation's internal breach reporting policy and procedure varies by the size, complexity and nature of its business, the above questions are useful when identifying common challenges that may become a breach no matter what the business type. The result of not following a checklist can mean a failure to meet your breach reporting obligations to ASIC.

ASIC announced a review of breach reporting by Australian Financial Services (AFS)[40] Licensees following its response to The Institute of Internal Auditors' (IIA) letter on 16 September 2014 on concerns about the delays and inconsistencies in reporting significant breaches. It is currently surveilling those licensees identified as having a higher risk of non-compliance based on what has been reported and their timeliness. ASIC's focus is on breach reporting of financial advisers and responsible entities operating managed investment schemes.

Key challenges and bottlenecks organisations may find in their breach reporting processes

How are organisations identifying breaches?

Front line staff members are responsible for identifying and escalating incidents, events, and issues so those responsible for breach reporting (often the compliance function) can determine if a breach has occurred and any action required. The extent to which this is done well depends on:

- Staff awareness
- Mechanisms used for capturing
- Categorisation, prioritisation, and accountabilities.

Breach identification also relies on those who respond to customer complaints, conduct compliance and risk monitoring, and audit internal controls to identify and escalate any issues. This means that clear accountabilities, effective training and open communication between these stakeholders will help identify any actual or potential breaches.

How long does it take to assess and evaluate a breach?

The time it takes to assess and evaluate an incident often relies on how quickly information can be accessed from the front line and other stakeholders.

A collaborative approach can only be achieved with commitment from all stakeholders so they understand and can meet their roles and responsibilities and the organisation's breach reporting obligations with clear guidelines in policies and procedures.

When does the clock start ticking?

AFS licensees must report significant breaches to ASIC within 10 business days of becoming aware of a breach or potential breach. However, how practical is this timeline and at what point does the clock start the 10 day countdown? ASIC's interpretation is that the 'clock starts' when a person responsible for compliance becomes 'aware' of a breach or 'likely' breach that it considers could be significant[41]. ASIC highlighted[42] that licensees should not wait to report until:

- After it has completed a full investigation to satisfy whether the breach, or likely breach, is significant
- The breach (or likely breach) has been considered by the AFS licensee's board of directors or legal advisers
- Steps have been taken to rectify the breach
- A likely breach has in fact occurred.

Is breach reporting everybody's business?

An effective governance framework should create an environment where incident identification and escalation is everybody's business. Those charged with the responsibility of assessing incidents to determine required action and reporting requirements, should expect full and timely cooperation from internal stakeholders so that decisions can be made and ASIC notified where relevant and within the required time frame. Clear action plans for remediation that address root causes should be prepared and followed through.

Will this breach happen again after it's been remediated?

How often do organisations close a breach event after it's been remediated and assume it will not happen again? Extending beyond a root cause analysis of the breach to identify indicators of any systemic issues in your business processes may signal weaknesses in internal controls. Evaluating the effectiveness of the internal controls to prevent and detect breaches is key to a wider action plan. Continuous improvement feedback to staff will also ensure the action plan informs an education piece to all affected internal stakeholders.

Key enablers to making breach reporting 'business as usual'

ASIC's announcement of breach reporting as area of focus should be a 'call to arms' to AFS Licensees. An AFS Licensee's breach reporting obligations forms part of ASIC's strategic focus for 2014/2015 particularly as significant breaches reported are a key for ASIC to highlight risk-based areas within the industry.

Licensees should undertake a proactive approach to evaluate the effectiveness of their internal breach management frameworks, including identification, categorisation, assessment, remediation, and reporting.

Securing commitment at all levels within an organisation to comply with this framework will be a key enabler to making breach reporting a 'business as usual' process.

Footnotes

1. An example of these orders is available at the following hyperlink: http://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-157a.pdf
2. Financial Stability Board Foreign Exchange Benchmarks – Final Report (30 September 2014); available at: http://www.financialstabilityboard.org/wp-content/uploads/r_140930.pdf
3. Guy Debelle FX Benchmarks – Address to the FX Week Australia Conference (12 February 2015); available at: http://www.rba.gov.au/speeches/2015/sp-ag-2015-02-12.html
4. Global Preamble: Codes of Best Market Practice and Shared Global Principles (30 March 2015); available at: http://www.rba.gov.au/afxc/about-us/pdf/global-preamble.pdf
5. International Organisation of Securities Commissions Principles for Financial Benchmarks – Final Report (July 2013); available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD415.pdf
6. See Financial Conduct Authority Bringing Additional Benchmarks Into the Regulatory and Supervisory Regime (PS15/6, March 2015); available at: http://www.fca.org.uk/your-fca/documents/policy-statements/ps15-06
7. Detail on this policy proposal is available at: http://ec.europa.eu/finance/securities/benchmarks/index_en.htm
8. Financial Stability Board Reforming Major Interest Rate Benchmarks (22 July 2014); available at: http://www.financialstabilityboard.org/wp-content/uploads/r_140722.pdf
9. Fair and Effective Markets Review How Fair and Effective Are the Fixed Income, Foreign Exchange and Commodities Markets? Consultation Document (October 2014); available at: http://www.bankofengland.co.uk/markets/Documents/femr/consultation271014.pdf
10. International Organisation of Securities Commissions Media Release – IOSCO Continues to Work To Strengthen Global Securities Markets as Drivers of Economic Growth (IOSCO/MR/05/2015, 13 February 2015); available at: http://www.iosco.org/news/pdf/IOSCONEWS366.pdf
11. Financial Stability Board, the Chairman Letter to G20 Finance Ministers and Central Bank Governors (4 February 2015) 2; available at: http://www.financialstabilityboard.org/wp-content/uploads/FSB-Chair-letter-to-G20-February-2015.pdf
12. Financial System Inquiry Final Report (2014), recommendation 21; available at: http://fsi.gov.au/publications/final-report/
13. Australian Securities and Investments Commission ASIC's Strategic Outlook (2014), 10; available at: http://download.asic.gov.au/media/2195181/asic-strategic-outlook-2014-2015.pdf
14. Australian Securities and Investments Commission Report 384 Regulating Complex Products (January 2014); available at: http://download.asic.gov.au/media/1344500/rep384-published-31-January-2014.pdf
15. Financial System Inquiry Final Report (2014), recommendation 22
16. International Organisation of Securities Commission Regulation of Retail Structured Products – Final Report (December 2013); available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD434.pdf
17. Financial Services Authority Retail Product Development and Governance – Structured Product Review – Finalised Guidance (March 2012); available at: http://www.fca.org.uk/static/pubs/guidance/fg12-09.pdf
18. http://blogs.deloitte.co.uk/financialservices/2015/01/mifid-ii.html
19. For an example of how the UK FCA has used these powers, please see the hyperlinked media release: http://www.fca.org.uk/static/documents/temporary-product-interventions/restrictions-in-relation-to-the-retail-distribution-of-cocos.pdf
20. Financial System Inquiry Final Report (2014), recommendation 23.
21. Australian Securities and Investments Commission Consultation Paper 224 Facilitating Electronic Financial Services Disclosures (November 2014); available at: http://download.asic.gov.au/media/2257756/cp224-published-14-november-2014.pdf

22. http://www.bbc.com/news/business-30079451

23. http://www.financialstabilityboard.org/wp-content/uploads/FSB-Chair-letter-to-G20-February-2015.pdf

24. CPS220 is a prudential standard released by APRA effective 1 January 2015 which requires APRA-regulated organisations to have an established risk management framework, including a sound risk management culture http://www.apra.gov.au/CrossIndustry/Documents/Final-Prudential-Standard-CPS-220-Risk-Management-(January-2014).pdf

25. http://www.financialstabilityboard.org/wp-content/uploads/FSB-Chair-letter-to-G20-February-2015.pdf

26. A Phase 3A entity is an Australian ADI, AFS licensee, a clearing and settlement facility licensee, an exempt foreign licensee or a foreign ADI with A$5 billion or more gross outstanding notional OTC derivative positions as at 30 June 2014 (and was not required to report in Phase 1 or 2). Phase 2 reporting entities were those with more than $50 billion in notional OTC derivative positions as at 31 December 2013

27. Australian Securities and Investments Commission Regulatory Guide 251 Derivative Transaction Reporting (February 2015); available at: http://download.asic.gov.au/media/2948586/rg251-published-13-february-2015.pdf

28. A Phase 3B entity is an Australian ADI, AFS licensee, a clearing and settlement facility licensee, an exempt foreign licensee or a foreign ADI with less than A$5B gross outstanding notional OTC derivative positions as at 30 June 2014

29. See Senator The Hon Mathias Cormann Media Release – Making Over-the-Counter Derivative Markets Safer (MC 139/14, 12 December 2014); available at: http://www.financeminister.gov.au/media/2014/1212-derivatives-markets.html

30. Financial Stability Board Feasibility Study on Approaches to Aggregate OTC Derivatives Data (19 September 2014); available at: http://www.financialstabilityboard.org/wp-content/uploads/r_140919.pdf

31. Australian Government Proposals Paper – Central Clearing of AUD-IRD http://financialmarkets.tspace.gov.au/proposals-paper-central-clearing-of-aud-ird/

32. International Organisation of Securities Commissions Risk Mitigation Standards for Non-centrally Cleared OTC Derivatives (28 January 2015); available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD469.pdf

33. Basel Committee on Banking Supervision and Board of the International Organization of Securities Commissions Margin Requirements for Non-Centrally Cleared Derivatives (March 2015); available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD480.pdf

34. See proposals by: US prudential regulators: http://www.gpo.gov/fdsys/pkg/FR-2014-09-24/pdf/2014-22001.pdf; Commodities Futures Trading Commission: http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2014-22962a.pdf; and European Supervisory Authorities: http://www.esma.europa.eu/system/files/jc_cp_2014_03_cp_on_risk_mitigation_for_otc_derivatives.pdf

35. ISDA's work on the margin requirements is explained at this page: http://www2.isda.org/functional-areas/wgmr-implementation/

36. See Financial Stability Board, the Chairman Letter to G20 Finance Ministers and Central Bank Governors (4 February 2015) 3; http://www.financialstabilityboard.org/wp-content/uploads/FSB-Chair-letter-to-G20-February-2015.pdf

37. Australian Government Resolution Regime for Financial Market Infrastructures – Consultation Paper (February 2015); available at: http://www.treasury.gov.au/ConsultationsandReviews/Consultations/2015/Resolution-regime-for-financial-market-infrastructures

38. Financial Stability Board, above n 11, 2

39. Corporations Act 2001 (Cth) section 912D

40. Australian Financial Services Licensees

41. ASIC Regulatory Guide, RG 78 Breach Reporting by AFS Licensees (26 February 2014), paragraph 27

42. ASIC's response to the Institute of Internal Auditors (Ref: CCU-14 \0429) dated 14 Sept 2014

Contacts

Kevin Nixon
Lead Partner, Risk & Regulatory
Financial Services
Tel: +61 2 9322 7555
kevinnixon@deloitte.com.au

Tim Oldham
Lead Partner, Risk & Regulatory
Banking
Tel: +61 2 9322 5694
toldham@deloitte.com.au

Sarah Woodhouse
Lead Partner, Risk & Regulatory
Wealth Management
Tel: +61 2 9322 7510
sawoodhouse@deloitte.com.au

Tommy Viljoen
Partner, Cyber Risk Services
Tel: +61 2 9322 7713
tfviljoen@deloitte.com.au

Michi Chan
Director, Governance &
Regulatory Consulting
Tel: +61 2 9322 7320
michichan@deloitte.com.au

Louise Denver
Director, Corporate Affairs &
Communications
Tel: +61 414 889 857
ldenver@deloitte.com.au

Alison Noble
Director, Tax (FATCA)
Tel: +61 3 9671 6716
alinoble@deloitte.com.au

Gavin Cartwright
Director, Cyber Risk Services
Tel: +61 2 9322 3580
gavcartwright@deloitte.com.au

Rosalyn Teskey
Governance & Regulatory
Consulting
Tel: +61 3 9671 6473
rteskey@deloitte.com.au

Ivan Zasarsky
Lead Partner, Financial Crime
Tel: +61 3 9671 7252
ivanzasarsky@deloitte.com.au

Andy Abeya
Director, Governance &
Regulatory Consulting
Tel: +61 2 9322 5691
aabeya@deloitte.com.au

Martin Joy
Director, Treasury & Capital
Markets
Tel: +61 3 9671 7863
majoy@deloitte.com.au

Tina Lin
Manager, Governance &
Regulatory Consulting
Tel: +61 2 9322 5846
tjlin@deloitte.com.au

Grant MacKinnon
Director, Risk Services
Tel: +61 2 9322 3693
gmackinnon@deloitte.com.au

Lisa Dobbin
Partner, Risk Services
Tel: +61 2 9322 3709
ldobbin@deloitte.com.au

Sydney office
225 George Street
Sydney, New South Wales
Australia
Tel: +61 2 9322 7000
Fax: +61 2 9322 7001

Melbourne office
550 Bourke Street
Melbourne, Victoria
Australia
Tel: +61 3 9671 7000
Fax: +61 3 9671 7001

www.deloitte.com/au/regulatoryreview

MCBD_Hyd_04/15_51580