REGCENTRIC

WHITE PAPER

APRA and Technology, what's next?

Overview

The management of non-financial risk, in particularly cyber security, by financial organisations is receiving increasing public scrutiny. Recent data breaches, most notably by Equifax in 2017[1], has alerted consumers and the public alike to the need for robust data management processes and more resilient cyber security practices. However, the management of data risks and mitigating practices are becoming increasingly more complicated, as consumer preferences move towards technology-enable financial services. This has led to open banking policy reform in the Australian financial system, which tasks banks with the challenge to safely and securely share customers' personal information across organisations[2]. This white paper briefly outlines prudential regulatory considerations with regards to data management, cyber security, and technology developments in the Australian financial system.

The current regulatory environment

Organisations operating in the Australia financial system have been under unprecedented scrutiny and review over the past 12 months. The Royal Commission stirred-up intense public criticism towards Australian financial service providers as Hayne's findings concluded that in many cases not only had the law not been obeyed, it had also not been effectively enforced. These sentiments drew criticism towards the performance of Australia's twin peak model of financial regulation. However, Hayne affirmed that twin peak model was here to stay and that financial regulators have an important role to play in reshaping the regulatory landscape and instilling community trust. Moving forward the supervision of non-financial risks will be a key area in addressing the failings of the financial system.

The Australian Prudential Regulation Authority (APRA) has signaled its intent to more closely supervise non-financial risks within the Australian financial system in its newly released 2019-2023 Corporate Plan. Cyber-resilience was named among four strategic focus areas which are aimed at strengthening outcomes for the Australian community[3]. The focus areas are:

- maintaining financial system resilience
- improving outcomes for superannuation members
- improving cyber-resilience across the financial system
- transforming governance, culture, remuneration and accountability across all regulated financial organisations.

The announcement to build more cyber-resilience in the financial system comes on the back of APRA releasing a new prudential standard on information security in July 2019. This standard aims to reduce the likelihood and impact of negative consequences associated with information security threats[4]. APRA has also been particularly vocal about its supervision of non-financial risks following the Capability Review, which called out that the regulator was not fully alive to the risks presented by non-financial risks including cyber threats and misconduct emerging from governance, culture and accountability failures[5].

The current regulatory environment

Over the past 12 months APRA has not been short of recommendations, the regulators activities and operations have been subject to six major reviews and inquiries. Collectively these reviews have delivered more than 100 recommendations for APRA to consider, plus another 50 that potentially involve multi-agency work[6]. Speaking to industry in August 2019, APRA chairman Wayne Byers acknowledged that the current regulatory framework was not designed for clouds, ecosystems and partnership models[7]. He went on to say that five years ago "...the technological disruptions which are now reshaping the financial system, and the associated cyber risks, were not as immediate as they are today." These comments raise questions about the ongoing feasibility of APRA's current supervision framework in dealing with cyber threats and other disruptive technologies. Many critics are calling for substantial overhauls to equip the regulator with the skills needed to supervise non-financial risks.

Concerns about APRA's internal capabilities in dealing with data management, cyber security, and technology disruptions have in part been addressed by the Federal Government through an increase to APRA's budget. Some of this funding has already been committed to improve APRA's data collection, storage, and analysis systems to bolster its supervisory assessment and decision-making capabilities[8]. However, speaking to a parliamentary committee in August 2019 APRA chairman Wayne Byers was assertive in setting expectations around the speed and intensity at which APRA will step-up into new areas of activity[9]. It is apparent, that following the Capability Review, the regulator is cautious about spreading its resources too thin in addressing non-financial risks, such as cyber security, as this may jeopardise its core tasks around financial safety and resilience.

Non-financial risks and prudential regulation

So, what exactly is non-financial risk? Non-financial risk is a broad term often defined by exclusion, that is any risk outside of traditional financial risks which are market, credit, and liquidity risks. Speaking to industry in March 2019, APRA chairman Wayne Byers outlined that discourse over the last 18 months in the Australian financial system has largely been directed towards conduct risk, treating customers fairly, and restoring consumer trust in the financial system[10]. These are all examples of non-financial risks. Moreover, all these concerns sit outside of traditional measures of financial system stability, which are focused on capital and liquidity requirements in addressing financial system resilience.

APRA chairman Wayne Byers has been vocal about the regulator needing to devote substantially more supervisory resources to its risk management and governance standards. In a recent speech, Mr. Byers indicated that these issues "...will need to become a core competency of APRA's supervision framework, just as much as bank capital and liquidity."[11] While these comments sent a strong signal to industry, recent criticism from the Capability Review suggests that APRA is currently ill-equipped to deal with other non-financial risks, like making cyber security assessments. It should be noted that monitoring information technology (IT) risks goes beyond APRA's data flow perimeter. To complicate oversight in this space further, financial technology organisations (fintechs) are increasingly farming out data to third-party service providers (including cloud vendors). This means APRA will have to become more collaborative with other government departments and also look at developing private sector partnerships to effectively improve cyber resilience across the Australian financial system.

The Probability and Impact Rating System (PAIRS) is APRA's risk assessment tool. APRA supervisors consider inherent risk, management and control, net risk, and capital support when making a PAIRs assessment of a regulated entity. Under this model non-financial risks, such as data management and technology, are defined within operational risk. However, other non-financial risks, including concerns about treating

Non-financial risks and prudential regulation

customers fairly and the appropriate alignment of remuneration frameworks, do not sit as neatly inside operational risk. Keeping to the PAIRs model, general conduct and management sits across all risks and are used to inform APRA's overall assessment of an entities board, its management, and their risk governance practices. The PAIRs model considers the following categories:

- board
- management
- risk governance
- strategy and planning
- liquidity risk
- operational risk
- credit risk
- market and investment risk
- insurance risk
- capital coverage/surplus
- earnings
- access to additional capital

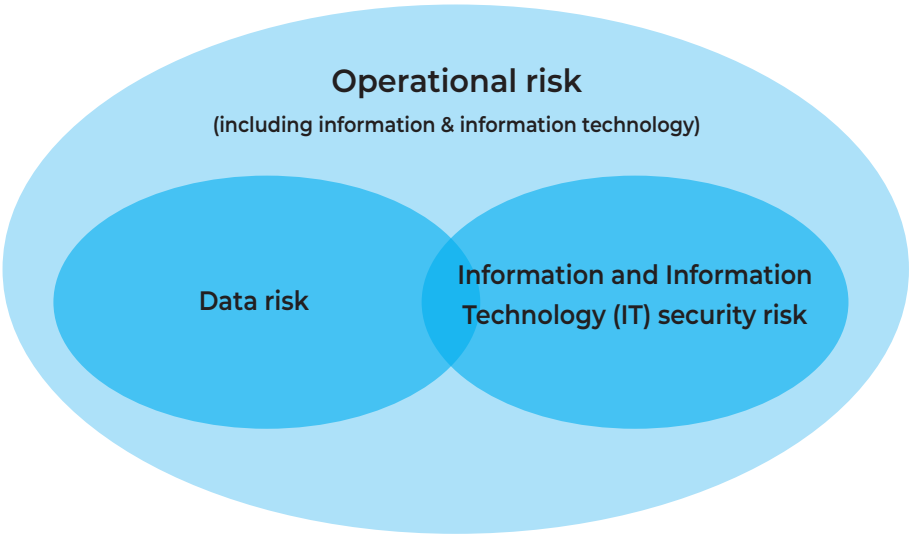
The development of more sophisticated cyber security systems, management and control frameworks to respond to cyber security threats, and an entities funding towards information security all sit under operational risk. As more organisations enter the domestic market with technology-based activities and business models, new practices will be required to mitigate against the risks associated with fintechs. The disruption of new technologies is compounded by changing consumer habits, as banking customers are increasingly accessing traditional financial services through digital channels. The speed of these developments has seen APRA's capability in supervising cyber security and IT risks repeatedly called in question[12] .

Looking ahead APRA has made improving cyber-resilience a top priority and announced that it will be developing cyber and technology strategies which include building strong allegiances with public and private sector experts[13]. It remains to be seen whether APRA will be revising its PAIRs model to more explicitly call out non-financial risks, such as cyber risk, along with traditional risks like liquidity, credit, and market risk which have the recognised potential to cause systemic risk to the financial system. Looking at the regulators Corporate Plan, it is clear that APRA will be heavily investing in developing internal capabilities to protect against threats associated with data management, cyber security and potential market disruptions from fintechs.

Data management and data risks

APRA published a practice guide in 2013 on managing data risk, which stands as its most current guideline on data management and data risks. Under APRA's regulatory framework both data risk and IT risk sit under operational risk, as shown below in figure 1. APRA defines operational risk as the risk of financial loss resulting from inadequate or failed internal processes, people and systems or from external events[14]. The guideline encourages a systematic and formalised approach to data risk and data management. This means that APRA expects an entity would adopt a set of high-level principles to manage data risk, which includes defining formal roles and responsibilities to staff. Moreover, that the entity has practices in place to ensure ongoing compliance and continuing assessments of effectiveness for data risk and IT risk.

Figure 1: Data risk and IT risk fall within operational risk under APRA's regulatory framework



Source: CPG 235 – Managing Data Risk

Data management and data risks

More recently, APRA has been active in the area of data management in particularly information security management. In late 2018 APRA released a new prudential standard on information security, in an attempt to strengthen the financial system against information security incidents (including cyber-attacks). This standard aims to ensure entities are adequately equipped to swiftly and effectively respond to data breaches. APRA also published a new information security prudential practice guide, which was particularly prescriptive in the areas of software security, cryptographic techniques, and customer security. While APRA has long populated a view that its supervisory approach is forward-looking and primarily risk-based in keeping with international best practices. Recent developments suggest the regulator it is playing catch-up in its response to data management and cyber threats, as its IT risk capabilities have been called out in a 2018 review by the International Monetary Fund (IMF) and again in its own Capability Review[15].

Looking ahead, fining Westpac has put other financial organisations on notice that the enforcement of data management is firmly on the regulators radar. In August 2019, APRA issued a maximum penalty of $1.5M to Westpac and two of its subsidiaries for failing to meet their legal obligations to report regulatory data. While the reporting of data is a non-financial risk, it is clear the regulator wanted to send a strong message to industry that compliance with its reporting standards is mandatory and cannot be considered secondary to other business priorities[16]. The fine comes after APRA received criticism from the Royal Commission that it was too timid in its approach to enforcement. In a media statement APRA deputy chairman John Lonsdale said that access to accurate and timely data is critical for APRA to monitor effectively the safety and stability of the financial system[17].

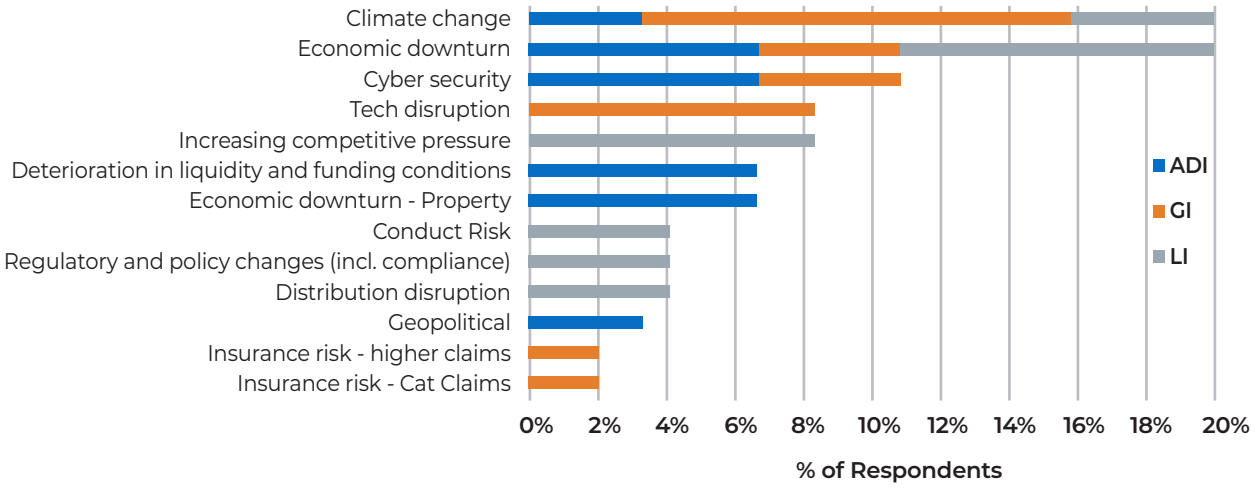
Cyber security and technology disruptions

Cyber security and technology disruptions have long been considered emerging risks by international regulators. The reality is that banks and other financial service organisations have long been subject to technology disruptions and sophisticated information security threats posed by new technologies. Speaking to industry in August 2019, APRA chairman Wayne Byers said there was ample discussion on the importance of technology and that "cyber security was definitely on the risk radar.[18]" However, the regulator also acknowledged that past attacks lacked the scale and complexity that are routinely encountered today. This admission suggests that instilling cyber-resilience best practices into the Australia financial system will be one of APRA's biggest challenges moving forward.

Over the past 12 months APRA has become increasingly more active on information security. The regulator has developed new prudential standards focused on information security management and updated its information paper on cloud computing services. APRA has also been supportive of calls from the banking industry to collaborate more closely together on cyber security threats to protect the national economy from online organised crime[19]. Growing concerns about the threat of cyber security were evident in a 2018 APRA industry survey, seen below in figure 2, where cyber security and technology disruption were second only to climate change and economic downturn as major long-term financial risks[20]. In addressing technology concerns APRA flagged to industry that it does not view cyber defences as a source of competition, neither should they be an issue of friction between regulators and the industry. Instead APRA has called for a coordinated effort from industry participants in addressing cyber security[21].

Cyber security and technology disruptions

Figure 2: Major long-term financial risks faced by APRA-regulated entities



Source: Buy now or pay later, Geoff Summerhayes, APRA Executive Board Member - International Insurance Society Global Insurance Forum, Singapore (21 June 2019)

Looking to the near future APRA will be placing greater regulatory emphasis on the supervision of non-financial risks, including data management, the use of cloud computing services, and information security. The regulator has also signaled that it will be constructively tough in its enforcement of breaches to prudential standards. New credit reporting and open banking regimes will be a challenge for many Australian financial organisations as customer data is often managed in siloed and disparate systems. Where there are IT issues, undertaking digital transformation projects often highlight backlogs of maintenance jobs and patchwork systems, which serves as evidence of under-investment in IT systems to the regulator. Managing the conflicting priorities of making customer data more accessible and also more secure will be a major challenge for financial organisations over the coming years. While it still remains to be seen how forceful APRA will be in regulating misconduct with regards to data management, the use of cloud computing services, and other cyber security risks.

Emerging technologies and traditional banking business models

Developments in cloud-based technologies are lowering barriers to entry into the Australian financial system at rates previously unexperienced. However, the impact of fintechs – which are adopting these enabling technologies – on banks and their business models remains uncertain. A 2017 consultation paper published by the Bank of International Settlements (BIS) estimated that between 10–40% of revenues and 20–60% of retail banking profits are at risk over the next 10 years[22]. Speaking to industry in September 2018, APRA chairman Wayne Byres said that "most technological advancements had worked to enhance the market positioning of the major incumbents", as larger organisations were able to control the pace and timing that new technologies were made available[23]. This means the biggest challenge for established banks in the Australian financial system is responding to speed and timing, as fintechs and neobanks are now able to quickly scale up operations by utilising cloud-based technologies.

"The concept of technological innovation improving the business of finance is as old as the abacus. But what is unsettling for today's financial organisations is the sheer pace of change"

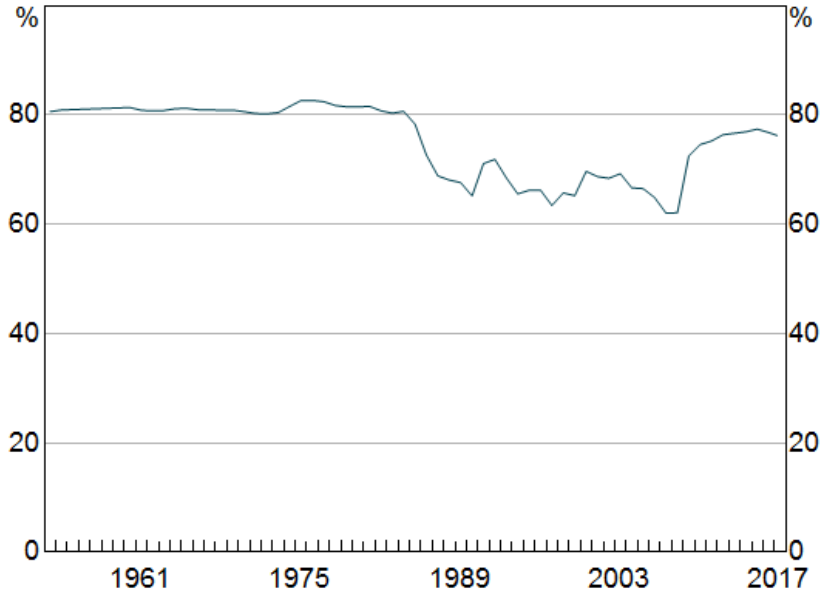
APRA Chairman Wayne Byres, Curious Thinkers Conference September 2018

Another uncertainty regarding the impact of emerging technologies on traditional banking business models is the ability of banks to absorb new competitors, whilst also successfully investing in their own capabilities. Australian banks are well capitalised and have already been investing heavily into cloud-based enabling technologies. They are also well positioned to absorb competition posed by fintechs, figure 3 below shows the major banks currently hold around 80% of domestic banking assets. Figure 3 also shows that the biggest disruption to domestic market share in the last 40 years came from banking deregulation in the mid-1980s and the entry of foreign banks.

More recently, the events which followed the Global Financial Crisis only led to further domestic market concentration, with the major banks share in domestic banking assets rising to pre-deregulation levels of around 80%.

Emerging technologies and traditional banking business models

Figure 3: Market concentration of domestic banking system assets by major banks*



Source: Big Banks and Financial Stability, Michele Bullock, Assistant Governor (Financial System), Economic and Social Outlook Conference, Melbourne (21 July 2017).

** Prior to 1983 there was up to eight major banks, which include their main subsidiaries; from 1983 major banks is defined as the four major banking groups.*

Considerable investments into cloud-based technologies and information security by Australian banks suggests that the disruption posed by fintechs is considered a real risk to traditional business models. APRA chairman Wayne Byres outlined a few scenarios in his speech titled “Peering into a cloudy future” which could play out in the domestic market in coming years:

- agile new fintech companies, better able to tailor their services to customers’ individual needs and built on modern technology platforms, could eat into the market-share of the large incumbents, and replace existing small incumbents; or
- big technology companies, with strong brand, advanced technology, reams of data and superior analytics, could elbow their way into the financial sector, usurping the major incumbents as the dominant market players; or

Emerging technologies and traditional banking business models

- the incumbents, using their regulatory and funding advantages as well as inherent customer stickiness, could partner with (and possibly eventually subsume) new market entrants, thereby maintaining their market positioning[24].

While it remains to be seen how fintechs and neobanks alike will transform the landscape of the Australian banking system, new technologies, such as artificial intelligence (AI)/machine learning (ML)/advanced data analytics, distributed ledger technology (DLT), cloud computing and application programming interfaces (APIs) all pose their own inherent risks. BIS has defined strategic risk, operational risk, cyber-risk and compliance risk as the key risks associated with the entrance of fintechs[25]. For APRA, new technologies and potential changes to traditional banking operational models means new supervision considerations. The regulator has been vocal that strong risk management and sound governance practices are required across the full spectrum of risks that banks face. Looking ahead, a key indicator to APRA that banks are equipped to mitigate against new risks posed by emerging technologies on their business models will be individual organisations' investment levels into operational and information security infrastructure.

Conclusion

The management of non-financial risks – in particularly information security and cyber threats – from emerging technologies will receive increased regulatory supervision over the coming years.

Speaking to industry in March 2019, APRA chairman Wayne Byers defined three dimensions of resilience which are needed to cultivate a safe and stable financial system in Australia[26]. These dimensions are financial resilience, operational resilience, and organisational and cultural resilience. Underlying these dimensions is consumer trust, which has been eroded by the failings highlighted in the Royal Commission. APRA now has stronger powers and will be expected to be seen more public in regulating misconduct. Restoring consumer trust will direct more scrutiny towards non-financial risks, as Australian consumers have come to expect financial resilience. This means that corporate governance, cyber security, and remuneration frameworks will be firmly on APRA's radar in the coming years.

Improving operational resilience, in the form of cyber security and IT risk capabilities, will not detract APRA from its core mandate of maintaining financial safety and resilience. The regulator recently highlighted a range of financial vulnerabilities domestically including very low interest rates, inflated asset prices, slowing growth rates, and high debt levels as challenges for the Australian financial system[27]. APRA flagged that it would also remain vigilant towards cyber-attacks, technological disruptions, and political risks (Brexit, and global political and trade tensions)[28]. Gaps in the regulators capabilities to supervise cyber threats and IT risks, which were identified in the Capability Review, have been in part addressed by $150m funding increase from the Federal Government. This funding will go towards increasing APRA's headcount from around 630 to over 700 in the coming years[29]. However, increased staff numbers alone will not address criticism of the regulator's poor enforcement record and opaque approach to dealing with misconduct[30]. A major challenge for APRA will be developing its capabilities in supervision areas like IT risk whilst also being seen to be acting more forcefully and swiftly towards misconduct.

Conclusion

APRA has committed to enforcing minimum cyber-resilience standards and information security practices to ensure that the response plans of financial organisations are fit-for-purpose. The regulator is also undertaking improvements to its own data analysis systems and plans to develop its own long-term baseline metrics to measure the cyber-resilience of organisations. APRA's updated information paper on cloud computing services is a definite call to action for regulated entities to be more aware of the inherent risks associated with emerging technologies. However, these actions have done little to quash criticism of APRA's internal capabilities, moreover suggesting the regulator may be playing catch-up with respect to IT risks like software security, data management, cryptographic, and customer security. Moving forward, it remains to be seen whether APRA's long held position of practising preventative medicine, rather than influencing behaviour policing via penalties, is the effective convention to ensure industry meet their regulatory obligations for data risk, cyber threats, and other non-financial risks.

To learn more or to find out how RegCentric can help in meeting your firm's regulatory and compliance obligations, contact our team here:

E info@regcentric.com

P (02) 8091 7187

www.regcentric.com

Disclaimer

We make every effort to maintain validity of the content incorporated in this article and believe them to be accurate. However, RegCentric cannot warranty the expressions and suggestions of the contents, as well as its accuracy, completeness and reliability. In addition to the extent permitted by the law, RegCentric shall not be responsible for any losses and/or damages due to the usage of the information contained in this article. Any action you take upon the information contained in this article is strictly at your own risk. The views and the other information provided are subject to change without notice. Where appropriate, excerpts have been taken from speeches, publications, and guidelines of the Australian Prudential Regulation Authority (APRA). By perusing this article, you hereby consent to our disclaimer and agree to its terms.

References

[1] Coulter, M & Shubber, K 2019, “Equifax to pay almost $1.1b in US settlement over data breach”, The Financial Review, viewed 23 September 2019, <https://www.afr.com/companies/financial-services/equifax-to-pay-almost-1-1b-in-us-settlement-over-data-breach-20190723-p52a0d>

[2] Eyers, J 2019, “Banks on track to hit 'good' open banking plan: APRA chairman”, The Financial Review, viewed 23 September 2019, <https://www.afr.com/companies/financial-services/banks-on-track-to-hit-good-open-banking-plan-apra-chairman-20190222-h1bkzo>

[3] Australian Prudential Regulation Authority 2019, APRA releases 2019-2023 Corporate Plan, viewed 4 September 2019, <https://www.apra.gov.au/news-and-publications/apra-releases-2019-2023-corporate-plan>

[4] Australian Prudential Regulation Authority 2019, APRA finalises prudential standard aimed at combatting threat of cyber attacks, viewed 11 September 2019, <https://www.apra.gov.au/media-centre/media-releases/apra-finalises-prudential-standard-aimed-combatting-threat-cyber-attacks>

[5] The Financial Review 2019, “Graeme Samuel's 24 recommendations for APRA”, 16 July, viewed 23 September 2019, <https://www.afr.com/companies/financial-services/graeme-samuel-s-24-recommendations-for-apra-20190716-p527ra>

[6] Byers, W 2019, “Opening Statement - 9 August 2019”, transcript, Australian Prudential Regulation Authority 9 August, viewed 5 September 2019, <https://www.apra.gov.au/news-and-publications/opening-statement-9-august-2019>

[7] Byers, W 2019, “Reflections on a changing landscape”, transcript, Australian Prudential Regulation Authority 26 August, viewed 5 September 2019, <https://www.apra.gov.au/media-centre/speeches/reflections-changing-landscape>

[8] Byers, W 2019, “Opening Statement – 11 April 2019”, transcript, Australian Prudential Regulation Authority 11 April, viewed 5 September 2019, <https://www.apra.gov.au/media-centre/speeches/opening-statement-11-april-2019>

[9] Eyers, J 2019, “APRA calls for more funding to target super, cyber, culture”, The Financial Review, viewed 23 September 2019, <https://www.afr.com/companies/financial-services/apra-calls-for-more-funding-to-target-super-cyber-culture-20190809-p52fjva>

[10] Byers, W 2019, “Building resilience in three dimensions”, transcript, Australian Prudential Regulation Authority 26 March, viewed 5 September 2019, <https://www.apra.gov.au/media-centre/speeches/building-resilience-three-dimensions>

[11] Byers, W 2019, “Reflections on a changing landscape”, transcript, Australian Prudential Regulation Authority 26 August, viewed 5 September 2019, <https://www.apra.gov.au/media-centre/speeches/reflections-changing-landscape>

[12] The Australian Government the Treasury 2019, Australian Prudential Regulation Authority Capability Review, viewed 17 September 2019, <https://www.treasury.gov.au/sites/default/files/2019-07/190715_APRA%20Capability%20Review.pdf>

[13] Australian Prudential Regulation Authority 2019, APRA releases 2019-2023 Corporate Plan, viewed 4 September 2019, <https://www.apra.gov.au/news-and-publications/apra-releases-2019-2023-corporate-plan>

[14] Australian Prudential Regulation Authority 2006, Prudential Practice Guide – CPG 230 – Operational Risk, viewed 3 September 2019, <https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-GPG-230-Operational-Risk_0.pdf>

[15] Australian Prudential Regulation Authority 2019, APRA's response to the Capability Review report, viewed 9 September 2019, <https://www.apra.gov.au/apras-response-capability-review-report>

[16] Eyers, J 2019, “Westpac fined $1.5m by APRA for late data”, The Financial Review, viewed 10 September 2019, <https://www.afr.com/companies/financial-services/westpac-fined-1-5m-by-apra-for-late-data-20190808-p52f9g>

[17] Australian Prudential Regulation Authority 2019, APRA fines Westpac for failing to meet legal reporting requirements, viewed 10 September 2019, <https://www.apra.gov.au/media-centre/media-releases/apra-fines-westpac-failing-meet-legal-reporting-requirements>

[18] Byers, W 2019, “Reflections on a changing landscape”, transcript, Australian Prudential Regulation Authority 26 August, viewed 5 September 2019, <https://www.apra.gov.au/media-centre/speeches/reflections-changing-landscape>

References

[19] Eyers, J 2019, “Banks must share cyber threat intel: Byres”, The Financial Review, viewed 13 September 2019, <https://www.afr.com/companies/financial-services/banks-must-share-cyber-threat-intel-byres-20190516-p51o1z>

[20] Summerhayes, G 2019, “Buy now or pay later”, transcript, Australian Prudential Regulation Authority 21 June, viewed 4 September 2019, <https://www.apra.gov.au/media-centre/speeches/buy-now-or-pay-later>

[21] Eyers, J 2019, “Banks must share cyber threat intel: Byres”, The Financial Review, viewed 13 September 2019, <https://www.afr.com/companies/financial-services/banks-must-share-cyber-threat-intel-byres-20190516-p51o1z>

[22] Bank of International Settlements 2017, Sound Practices: Implications of fintech developments for banks and bank supervisors, viewed 10 September 2019, <https://www.bis.org/bcbs/publ/d415.pdf>

[23] Byers, W 2018, “Peering into a cloudy future”, transcript, Australian Prudential Regulation Authority 21 September, viewed 2 September 2019, <https://www.apra.gov.au/media-centre/speeches/peering-cloudy-future>

[24] Byers, W [2018], “Peering into a cloudy future”, transcript, Australian Prudential Regulation Authority [21] September, viewed [2] September [2019], <https://www.apra.gov.au/media-centre/speeches/peering-cloudy-future>

[25] Bank of International Settlements 2017, Sound Practices: Implications of fintech developments for banks and bank supervisors, viewed 10 September 2019, <https://www.bis.org/bcbs/publ/d415.pdf>

[26] Byers, W [2019], “Building resilience in three dimensions”, transcript, Australian Prudential Regulation Authority [26] March, viewed [4] September [2019], <https://www.apra.gov.au/media-centre/speeches/building-resilience-three-dimensions>

[27] Byers, W 2019, “Building resilience in three dimensions”, transcript, Australian Prudential Regulation Authority 26 March, viewed 4 September 2019, <https://www.apra.gov.au/media-centre/speeches/building-resilience-three-dimensions>

[28] Byers, W 2019, “Opening Statement - 9 August 2019”, transcript, Australian Prudential Regulation Authority 9 August, viewed 5 September 2019, <https://www.apra.gov.au/news-and-publications/opening-statement-9-august-2019>

[29] Moullakis, J 2019, “APRA looks to boost staff numbers”, The Australian, viewed 12 September 2019, <https://www.theaustralian.com.au/business/apra-looks-to-boost-staff-numbers/news-story/20339824b6f05a686ef3b2a76865cc95>

[30] Ferguson, A 2019, “APRA's capability review will shake up culture”, The Financial Review, viewed 25 September 2019, <https://www.afr.com/companies/financial-services/apra-s-capability-review-will-shake-up-culture-20190714-p5270f>

Figure References

Figure 1: Australian Prudential Regulation Authority 2013, Prudential Practice Guide CPG 235 – Managing Data Risk, viewed 3 September 2019, <https://www.apra.gov.au/sites/default/files/CPG-235-Managing-Data-Risk.pdf>

Figure 2: Summerhayes, G 2019, “Buy now or pay later”, transcript, Australian Prudential Regulation Authority 21 June, viewed 4 September 2019, <https://www.apra.gov.au/media-centre/speeches/buy-now-or-pay-later>

Figure 3: Bullock, M 2017, “Big Banks and Financial Stability”, transcript, Reserve Bank of Australia 21 July, viewed 4 September 2019, <https://www.rba.gov.au/speeches/2017/sp-ag-2017-07-21.html>