



Shutterstock: 1110248891

Sep 04, 2020 22:21 BST

Australian Prudential Regulation Authority (APRA) updates four-year plan

by Joss Howard, Senior Advisor, NCC Group

2020 has been a tumultuous year for all, the Australian Prudential Regulation Authority (APRA) included. This week they released an update of their four year plan, acknowledging the significant impact of not only COVID-19, but also the devastating bushfires and storms that occurred since

their last plan.

APRA has a new focus on what they dub 'immediate priorities' for the next 12-18 months when the future and economy is still adjusting to the new normal. *"APRA is cognisant that it plays an important role in protecting the financial wellbeing of the Australian community in these times of unprecedented adversity. It has been necessary for APRA to rapidly adapt to a volatile external environment and respond as events unfold in close coordination with Government, peer regulators and industry,"* Wayne Byres stated in his Chair's Foreword.

In the longer term, APRA's 2020-2024 Corporate Plan continues its commitment to delivering four key community outcomes:

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

In relation to the last outcome APRA recognised that, *"Cyber-attacks are increasing in frequency, sophistication and impact both domestically and globally. All indications are that the risk will continue to grow, requiring a continuous cycle of investment in sound practices."*

Building on the release of their CPS 234 Information Security standard (NCC Group's CPS 234 [on-demand webinar can be viewed here](#)), they have been developing their 2020-2024 Cyber Security Strategy. APRA says that it plans to expand its cyber approach by applying a broader set of tools and techniques across the industry. It's also expected the strategy will broaden its scope to include the broader eco-system of suppliers and providers that financial institutions rely upon, like it has done in the second phase of CPS 234.

The Plan went on to state that the end-state of cyber security is still unclear, there are a number of actions that can be taken to limit the impact of cyber incidents in the community. Over the longer-term, APRA will:

- establish a baseline of cyber controls by reinforcing embedding of non-negotiable cyber practices, facilitating sharing of relevant and timely cyber information and enabling effective incident response for the financial system;
- enable the Board and executives of financial institutions to oversee and direct correction of cyber exposures by formulating sound practice guidance and stepping up APRA's scrutiny of cyber oversight practices;
- identify and focus on work to address weak links within the broader financial eco-system and supply chain by fostering maturation of provider cyber-assessment and assurance and harmonising the

- regulation and supervision of cyber across the financial system; and
- innovate using impactful regulatory tools and approaches by actively harmonising regulatory cyber efforts and dialling-up supervision scrutiny and intensity.

What does this mean for the financial services industry and its suppliers?

We expect that organisations will get notification of new prudential standards from APRA in the near-mid future, and for APRA to be firmer in their scrutiny and supervision of entities cyber resilience. APRA has clearly stated that it will “establish a baseline of cyber controls by reinforcing embedding of non-negotiable cyber-practices.

It goes without saying that cyber-risks have increased due to the escalation in working from home, cloud usage for anywhere services (which may present data privacy and sovereignty issues) and APRA acknowledge these risks in their plan.

It is therefore, very important for businesses to remain agile, focused on reducing their internal and external cyber-risk, especially in supply chains. Boards need senior management to ensure that they are well-informed of any changes so that the business takes the appropriate action.

While this is a challenge during this current time, compliance with any new regulations, protecting member information and implementing robust controls is a priority for the safety of the business, its customers and the finance industry.

You can view the full plan on [APRA's website here](#).

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant

market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts



NCC Group Press Office

Press Contact

All media enquires relating to NCC Group plc

press@nccgroup.com

+44 7824 412 405

+44 7976 234 970