ISACA®

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008-3105, USA
Web Site: *www.isaca.org*

Telephone: +1.847.253.1545
Facsimile: +1.847.253.1443
E-mail: *info@isaca.org*

5 June 2018

Heidi Richards
General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority

Dear Ms. Richards:

On behalf of the approximately 4,000 ISACA members within Australia, and the nearly 160,000 professionals who are part of ISACA's global community, we are grateful for the opportunity to respond to the Australian Prudential Regulation Authority's (APRA) discussion paper on the Authority's proposals for the new Prudential Standard CPS 234 Information Security.

In the attached document, you will find ISACA's responses to the proposals outlined in APRA's recent discussion paper. These responses encompass the insights and perspectives of leading members within ISACA's Australia community. ISACA's Australia and global communities would be pleased to continue to be a part of this important conversation, and to contribute to the Authority's ongoing efforts in this area.

If you would like additional information regarding any of the elements contained in our response, please do not hesitate to reach out to ISACA's Australia leadership at mike.trovato@isaca-melbourne.org.au, jStewartRattray@isaca.org or Adam.wood@isaca-canberra.org.au. Additionally, ISACA would welcome the opportunity to have a broader and ongoing discussion on these issues, should APRA's leadership wish to do so. Thank you in advance for your time and consideration.

Respectfully submitted,

Michael S. Trovato
ISACA Melbourne Chapter
Board Director

Jo Stewart-Rattray
ISACA International Director

Adam Wood
ISACA Canberra President

About ISACA

ISACA helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association representing approximately 160,000 information and cybersecurity professionals throughout the world, including nearly 4,000 in Australia. As part of ISACA's efforts to support the global IT professional community, ISACA offers COBIT®, a business framework to govern enterprise technology, and the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource to assist organisations in developing skilled cyber workforces and enabling individuals to grow and advance their cyber careers.

Responses to the Australian Prudential Regulation Authority Discussion Paper,
"Information Security Management: A New Cross-Industry Prudential Standard"

Australia's financial services environment relies upon adherence to the highest standards of security and data risk management. It is this insistence on high standards in risk and data management that has formed the foundations of Australia's financial services sector and created the conditions for that sector to thrive. It is that dedication to excellence that will continue to serve Australia's financial services sector well far into the future.

ISACA acknowledges the essential role of APRA in developing and enforcing a robust prudential framework that promotes prudent behaviour by ADIs, insurance companies, superannuation funds and other financial institutions it supervises, with the key aim of protecting the interests of their depositors, policyholders and superannuation fund members.

The Prudential Standard CPS 234, in ISACA's opinion, is a welcome addition to and enhancement for this foundation. It builds upon other key risk management principles, such as those offered in CPG 234 and 235, and sets the stage for future evolution in security and data risk management. Those organisations already using the principles of CPG 234 and 235 should not encounter great difficulties transitioning to the new Prudential Standard within the coming year; rather, it will likely be seen by many organisations as more 'appropriate next step' than 'transition'.

However, ISACA recognizes that this will not be the case for all organisations. Those not currently adhering to the guidance offered by existing principles will find themselves encountering real difficulty in meeting the new Prudential Standard CPS 234. Given the 1 July 2019 date for compliance, there is reasonable time for compliance, regardless of prior adherence to existing guidance, or lack thereof.

If there are increased costs for compliance—and there likely will be—those costs should be perceived as investments rather than incurrences. By strengthening risk and data management and security practices throughout Australia's financial sector, ARPA strengthens yet another pillar within Australia's innovative digital economy, making both the economy and the sector stronger and more resilient.

It is ISACA's considered opinion that any additional compliance costs would be outweighed by the overall benefits provided to Australia's financial sector and the digital economy. Likewise, ISACA believes that a 'stepped' approach to implementation of the Prudential Standard is the correct approach; it provides adequate timelines for all organisations involved, ensures compliance without the overburdening of the organisations affected by the new Prudential Standard, and minimises the immediate impact of compliance costs.

For all the benefits provided by the draft Prudential Standard CPS 234, however, there are still areas to consider:

- **Overall**—Even though the Prudential Standard CPS 234 establishes minimum standards to apply to all industries, by elevating key principles from CPG 234, and previously PPG234, which have been applied since 2010, a closer examination appears to present a focus on larger, group-structured, Tier-1 banks that can afford more protective and preventive resources (e.g. larger teams of information security professionals; adequate resources to undertake thorough testing of controls; internal audit functions with information security audit capabilities, etc.). For smaller organisations — and even some FinTechs — such resources are not easily obtained without some significant budgetary increases as they have not been on this journey or have avoided it all together.

- **Overall**—There could be a greater focus on guidance related to security culture, and the role of leadership in the establishment of an effective security culture that would result in more resilient organisations. The guidance presented is limited in scope and depth.
- **Overall**—Some vendors and FinTech organisations are significantly invested in digital transformation, product innovation and rapid development, yet there is limited guidance on development approaches (such as DevOps) and innovation activities; ISACA believes this to be a missed opportunity to assist the sector.
- **Clause 12**— To strengthen this clause, we believe it should be re-prioritised as "*and which enables the interests of depositors, policyholders, beneficiaries, or other customers and the sound operation of the entity and maintaining trust*". Essentially, putting customer interests first. Often boards focus too much on their personal risk and entity profit versus the impact on customer interests and resilience.
- **Clause 15**—The Prudential Standard places its primary focus on information hosted within the regulated entities' perimeter. However, many organisations utilise external service providers. In relation to this, there is a lack of clarity on what is expected in relation to Clause 15 as a result of the capability assessment. We suggest adding the words "*and its related party or third party*" to Clause 16 for clarity.
- **Clause 19—**ISACA believes that classification is useful for facilitating the effective handling and protection of information, particularly personal information. To strengthen this clause, we believe it should be re-prioritised as "*interests of depositors, policyholders, beneficiaries, or other customers or the entity*". Essentially, putting customer interests first, as mentioned earlier in the suggested amendments to Clause 12.
- **Clauses 20 and 21**—There is a lack of detail about the components expected in the control model. Inclusion of those details would provide additional clarity.
- **Clause 20**—The Review into Open Banking which was commissioned by the Treasurer to make recommendations on the most appropriate data-sharing model in order to facilitate competition and innovation in the banking sector offers some exciting opportunities and threats to customers. It was recommended that ADIs should consider the Review carefully and assess what internal processes and policies need to be updated or created to prepare for Open Banking generally. The Review suggests that the four major banks should be required to implement Open Banking from the intended commencement date (1 July 2019), with all other ADIs to follow within 12 months. ISACA believes that the complex and complicated nature ADIs and challenges of implementing Open Banking and the CPS 234 will be difficult for many entities to do on the scheduled timetable. The potentially toxic combination of big data, Cloud, APIs, and third-party apps via Open Banking should be called out in this clause, such as by adding "or those used for Open Banking" to following "third parties,". Regardless, ISACA is concerned about the risks of Open Banking and its impact on trust and the potential of increasing fraud.
- **Clause 21**—It is not clear how what is outlined in Clause 21 can be undertaken by a smaller regulated entity, especially the evaluation of control effectiveness. It is also unclear how this is applicable to SaaS providers. Clause 21 may work for traditional outsourcing but may be difficult in a Cloud environment. Specifying that the regulated entity should evaluate related party or third party use of a Service Organization Control (SOC 2®) Report on Controls Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy, or similar independent audit would offer additional clarity on what is expected as a minimum.
- **Clause 26**—The activities outlined in Clause 26 should be further described to include both business process and technical controls, i.e. penetration testing.

- **Clause 34**— To strengthen this clause, we believe it should be re-prioritised as "*interests of depositors, policyholders, beneficiaries, or other customers or the entity*". This would align with earlier suggested amendments to Clauses 12 and 19 and keep a focus on putting customer interests first.

In the discussion paper for this consultation, APRA notes that "*there is no 'end-state' for information, therefore (it requires) a continuous cycle of investment in sound practices*".[1] The ISACA community in Australia—and globally—agrees, but with one addition to that sentiment; it requires an equally strong and continuous cycle of commitment to improvement and investment as well.

We believe this discussion paper and consultation is indicative of ARPA's commitment, in both regards, and are grateful to have the opportunity to share ISACA's views on the new Prudential Standard.

[1] Australian Prudential Regulation Authority Discussion Paper; *Information Security Management: A New Cross-Industry Prudential Standard*; 7 March 2018