Level 6, 161 Collins Street
Melbourne VIC 3000
Phone 13 13 69

GPO Box 264
Melbourne VIC 3001

12 July 2018

Heidi Richards,
General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulatory Authority
GPO Box 9836
Melbourne, VIC 3001

Dear Ms. Richards

RE: IOOF's response to APRA CPS 234 discussion paper

On behalf of IOOF, we are grateful for the opportunity to respond to the Australian Prudential Regulatory Authority's (APRA) discussion paper on APRA's proposal for the new Prudential standard CPS234. Our response is as follows.

1. **General**

   a. CPS 234 seems to have a greater focus and seem to be geared towards Tier 1 and large organisations (like the Tier 1 Banks) that may have large Information security teams and substantial budgets available in the areas of security governance, compliance, management and internal audit. This is because the CPS234 seems to build on PPG234 and assumes that most organisations already comply with PPG234. This may not be the case with smaller Tier2 financial services organisations as well as start-up FinTech companies.

   b. Cybercriminals are targeting users by crafting attacks using complex social engineering techniques. They are also exploiting vulnerabilities and weaknesses in technologies left unpatched. Both these threat vectors exploit human and process weaknesses. One of the best weapons against this is cultural change and inculcating cyber-aware behaviours within all parts of the organisation. We note that there is no particular mention of "Security Culture" within the proposed CPS. The role of cyber leadership within organisations is also important and currently is lacking in the proposed CPS.

2. **Clause 20**

This clause is not detailed enough and does not provide details of controls required. It does not set out any minimum standards of any controls, making the control selection and implementation subject to interpretation. A slightly more prescriptive control-set may help entities better comply with this clause.

3. **Clause 21**

In cases where entity's information is managed by a SaaS or PaaS cloud provider (being the related third party in this case), the entity may not be able to evaluate the design and operating effectiveness of such 3rd parties. Many large cloud providers such as Google, AWS, Microsoft will not release/divulge any control information and hence the entity will not be able to evaluate the operating effectiveness of the provider and hence be in breach of this clause. Consideration should be given to clarify this clause and its applicability.

4. **Clause 26**

   Proactive and thorough controls effectiveness testing (from business perspective) will require large teams, and this will be difficult to implement in smaller organisations that have resource constraints. We would prefer such controls testing to be commensurate with risk relevance, and prioritisation based on assessment of risk versus cost.

Overall, we believe that the proposed CPS standard will add robustness and rigour to the protection of information and financial assets of Australian depositors, policyholders and superannuation fund members. We therefore welcome APRA's efforts to create and promulgate a stringent standard for protection of digital assets.

We would be keen to participate in any further consultations and discussions that APRA might like to have on this matter.

Yours sincerely

Ashutosh Kapse
Head of Cybersecurity