www.pwc.com.au

PwC Submission

Consultation on Draft Prudential Standard CPS 234 - Information Security

June 2018

pwc

PwC Submission: Consultation on Draft Prudential Standard CPS 234 - Information Security

Organisation:	**Business Name:** PricewaterhouseCoopers Australia (PwC) **ABN:** 52 780 433 757 **Address:** 2 Riverside Quay, Southbank, Melbourne, VIC, 3006 **Postal Address:** GPO Box 1331, Melbourne, VIC, 3001 **Phone:** +61 3 8603 1000
Contact details:	

General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
GPO Box 9836
Sydney NSW 2001

7 June 2018

Dear Sir/Madam,

PwC Submission – Consultation on Draft Prudential Standard CPS 234 - Information Security

PwC Australia ("PwC") welcomes the opportunity to provide comments on the APRA draft Prudential Standard CPS 234 – Information Security (the "Prudential Standard"). This is an important Prudential Standard for the digital economy of today and tomorrow, and specifically for Australia's Financial Services sector. APRA's regulated-entities play a key role in the fabric underpinning the Australian community – providing access to core financial mechanisms.

Worldwide, PwC employs more than 3,500 security, risk, cyber investigative and privacy professionals from a diverse range of backgrounds. Our team includes several individuals who have served in corporate roles such as Chief Information Security Officers, Chief Information Officers and Chief Compliance Officers across a variety of industries and organisations. PwC has a leading information / cyber security and privacy practice as recognised by organisations such as IDC and Forrester. We believe that our experience of working with a wide range of entities across different geographies equips us with pragmatic insights on the potential impact of the implementation of the Prudential Standard in Australia and this has informed our consultation response.

Our submission details areas where we believe the Prudential Standard would benefit from amendment or clarification to enhance its effectiveness. A summary of these areas has been provided below:

1. **Roles and responsibilities relating to information security** – The Prudential Standard defines the roles and responsibilities of Boards relating to information security. APRA may wish to include the recognition that Directors may lack the experience or knowledge to provide a credible challenge to management on cyber risk, therefore the use of skilled individuals to augment Board capabilities should be endorsed. This includes the use of independent specialists or third parties (in line with APRA's comments on external experts in the 'Board Governance Thematic Review', issued in May 2018 to all RSE Licensees). APRA should also consider including guidance on when a Board should be notified of an eventuating cyber risk / threat (for example, if there is any potential customer impact).
2. **Management of information security incidents –** It is important that information security incident response plans are defined for common and specific threats to regulated entities, and are assessed and tested to increase effectiveness. We recommend that regulated entities are required to demonstrate their incident and crisis management capabilities. APRA may also wish to consider mandating that all regulated entities participate in an industry information sharing forum to facilitate the increase in maturity across the sector, decreasing the likelihood that one type of attack will be successful against multiple market participants.

3 **Testing and measuring the effectiveness of information security controls** – We recommend that the testing of the effectiveness of information security controls would be best focused on where there have been material changes to information assets, where "material" refers to any modification or change to an information asset, including changes in the external environment, that alters or has the potential to alter the behaviour of a security control. This would provide greater value than just looking at rates of vulnerability and threat changes. Further, additional clarity should be provided on the definitions of "appropriately skilled" and what is considered a "timely" manner in regards to the reporting of security control deficiencies.

4 **Notifying APRA of information security incidents** – Consideration should be given to aligning the breach notification period of the Prudential Standard to other reporting obligations, for example disclosure of Personal Information to the Office of the Australian Information Commissioner (OAIC). APRA should also provide guidance on what constitutes a "material information security control weakness", along with the definition of "timely manner" in relation to remediation activities. APRA should further consider providing guidance as to whether the risk assessment processes of regulated entities could be relied upon to determine the level of residual risk for security incidents, and therefore negate the need to report the incident based on the above definitions.

5 **Information assets managed by a related or third party** – APRA should consider providing additional guidance on the definitions (and examples) of what constitutes a 'related party' and a 'third party', including consideration of fourth party (and similar) arrangements. The increasing use of managed services and cloud platforms presents a change in the profile of cyber risk for organisations, and our experience with regulated entities shows that a risk-based assessment process (in-line with Paragraph 19) would be practical to manage this risk. We recommend that further clarity is provided around Paragraph 21 in light of this.

Further, APRA should consider outlining their expectations of the Risk Management Declarations in the context of the proposed Prudential Standard.

In addition to the areas outlined above in relation to the Prudential Standard, to support a broader cyber risk mitigation approach for the Financial Services industry, APRA may wish to consider the two following ideas to mitigate systemic sector wide risks that could damage the Australian economy as a whole:

- That APRA-regulated entities include, as part of their enterprise wide cyber risk assessment, analysis of digital shared infrastructure versus traditional infrastructure for back-up solutions and services where a systemic disruption to critical components of the financial system could occur (i.e. payments).
- Supporting the classification of the internet as critical infrastructure in Australia, bringing additional resilience through increased oversight by the appropriate Federal Government Department or Agency.

Our practitioners are available for further discussions or consultations in relation to the submission, and we welcome further opportunities to have ongoing conversations about legislation and issues impacting information security in Australia.

Yours sincerely,

Peter Malan
Partner

Andrew Gordon
Partner

PwC submission

We support the introduction of APRA's draft Prudential Standard CPS 234 - Information Security ("Prudential Standard") in Australia.

Information assets and their protection are front of mind for many Australian organisations. In 2017 alone, organisations locally and globally experienced a number of significant cyber security related incidents. Security incidents, such as Petya and WannaCry, which exploited vulnerabilities in external and internal systems, have magnified the importance of managing these emerging and growing risks. Within the Financial Services sector, effective management of information security is paramount to retaining and building trust within the community.

The increasing cross industry trends of cloud platform use, managed services, adoption of agile methodologies and big data / data insights all provide large amounts of value to organisations, but they also change the information security risk profile. The World Economic Forum's 2018 Global Risks Report ranked large-scale cyberattacks and major data breaches among the top five most likely to occur global risks in the next decade. Given these trends are common to most organisations, we agree that it is prudent for APRA to issue a formal standard to mandate that all regulated entities establish appropriate information security controls, ongoing assurance, monitoring and reporting.

As part of our research we have leveraged our "Global State of Information Security® Survey 2018" which surveyed more than 9,500 Chief Executive Officers, Chief Financial Officers, Chief Information Officers, Chief Information Security Officers, Vice Presidents and Directors of IT and security practices from more than 122 countries.

This submission details a number of areas where we believe the Prudential Standard requires amendment or clarification to effectively meet its objectives of requiring regulated entities to improve their information security capabilities. These areas are as follows:

1. **Roles and responsibilities relating to information security**
2. **Management of information security incidents**
3. **Testing and measuring the effectiveness of information security controls**
4. **Notifying APRA of information security incidents**
5. **Information assets managed by a related or third party**

Contents

1 Roles and responsibilities relating to information security

We agree with the intent of the Prudential Standard to define the roles and responsibilities of APRA-regulated entities Boards in relation to information security. Our experience is that Boards typically delegate accountability and responsibility to their security teams with little or no consideration of the broad ownership of information risk across the organisation, and the shared responsibility required to ensure the continued sound operation of the entity.

Recommendations

Our view is that to ensure the accountability of Boards, they need to have the relevant training and insight to understand information security threats and issues. We recommend that Boards are trained to deal with these events before they materialise. Without this, they may be unprepared to question the validity of any information security program that the entity executes. This also extends to the nature of information provided to the Board of an APRA-regulated entity - ensuring that this information is at an appropriate level of detail to inform and drive decision making related to these threats and issues.

Given that Directors may lack the experience or knowledge to provide a credible challenge to management on cyber risk, APRA should consider endorsing the use of skilled individuals to augment the information security capabilities of regulated entities Boards. This should be done in alignment to APRA's recommendations (i.e. Recommendations 1.1 and 2.1) in the Board Governance Thematic Review, issued in May 2018 to RSE Licensees). In addition, in conjunction with Paragraphs 26 and 30 of the Prudential Standard, we recommend that Boards of regulated entities should receive the outputs from information security assurance / testing activities performed and APRA may consider whether mandating periodic independent assessments is warranted.

APRA should also consider including guidance on when a Board of a regulated entity should be notified of an eventuating cyber risk / threat (for example, any customer impact / potential breach of regulatory or legal requirement / movement outside cyber risk residual risk appetite).

Further, when assessing the size of threats, a valid threat model is needed to understand the likelihood of, and potential loss from, information security incidents so that any decision-making and investment oversight is properly informed. To this extent, the Prudential Standard or supporting guidance, should include, or reference, a set of scenarios or threats with a defined level of granularity to allow an APRA-regulated entity and their Board to properly understand the size and extent of the threats that they face.

2 Management of information security incidents

We concur with the objective of the Prudential Standard to ensure that APRA–regulated entities have robust mechanisms in place to detect and respond to information security incidents. However, it is our view that the proposed requirements do not sufficiently empower APRA to effectively assess a regulated entity's handling of an information security incident, or require the regulated entity to demonstrate the effectiveness of their process.

Recommendations

The Incident Management Paragraph of the Prudential Standard (Paragraphs 22 to 25) should be enhanced, or supporting guidance provided, to be specific and set the appropriate expectation for APRA-regulated entities, i.e. that their process must be robust and demonstrable. A regulated entity should be required to demonstrate their incident and crisis management capabilities to APRA (including an agreed definition of when an incident becomes a crisis). Evidence should be provided that an entity's processes are robust and timely from real-world information security incidents and simulations against their response plans.

We recommend that an APRA-regulated entity should demonstrate to APRA on a regular basis how they evaluate the effectiveness of these processes against planned and real-world incidents and how they have been adapted over time. This should include situational crisis management with relevant internal escalation during an incident and any necessary external notifications. It should then describe the information reporting requirements, including post incident review and notifications to Boards and governing bodies.

The Prudential Standard, or supporting guidance, should also explicitly support an entity's external engagement with relevant authorities, depending on the nature of the security incident and the extent of any security breach. This could include situational based engagements with the national Australian Cyber Security Centre (ACSC) and CERT Australia, which should be included in any plans or playbooks developed for Paragraph 23 of the Prudential Standard. This also presents an opportunity for APRA and APRA-regulated entities to establish a common framework for the classification of information security incidents and the sharing of this information across industry so that all participants benefit from the potential threat intelligence.

To ensure that an APRA-regulated entity understands their obligations, the Prudential Standard, or supporting guidance, should include a limited set of examples such as denial of service, ransomware/extortion, theft of IP or disclosure of PII, so it is clear that plans are required for common and specific threats to the APRA-regulated entity. The entity should also have a credible threat model that describes its common and specific information security threats and associated response plans for Paragraph 23.

Further, APRA may wish to consider mandating that regulated entities participate in an information sharing forum to facilitate the increase in cross sector maturity.

3 Testing and measuring the effectiveness of information security controls

In our view, there is limited value in requiring an annual assessment of the security of information assets where a material change has not occurred. Suggesting that control testing be commensurate with the rate at which vulnerabilities and threats change potentially fails to address appropriate control validation and revalidation for weaknesses introduced through change and potential misconfiguration.

The escalation and reporting requirements of the Prudential Standard should be progressive enough to support new ways of working, specifically considering agile environments where there is a need to define what is material to make risks related to changes more manageable. This is especially important when considering compensating controls and rapidly changing environments. In environments with high rates of change, the reporting requirements may be overly burdensome where the control deficiency is short lived.

Further, there is no definition provided on what is meant by "appropriately skilled" in relation to the testing of information security controls.

Recommendations

We believe that the Prudential Standard should focus on two aspects of the testing of information security controls:

1) In the short to medium term, establishing a foundation level of testing to assess the effectiveness of security baseline controls.

2) Once the baseline is established and meets defined residual risk levels, focussing on "material" changes to information assets, where "material" refers to any modification or change to an information asset, including changes in the external environment, that alters or has the potential to alter the behaviour of an information security control. APRA may also want to consider if it is appropriate to comment on what is commensurate with rates of vulnerability and threat change, and only require Clauses (b) to (d) of Paragraph 26.

Further, we believe that the Prudential Standard, or supporting guidance, should clearly define what is meant by "appropriately skilled" in practice relating to the testing of security controls. There is also a need to define APRA's expectations for reporting of security control deficiencies that cannot be remediated in a "timely" manner to senior management or the Board.

In our view, external validation and testing of controls by industry accredited individuals and organisations is desirable. Clarity should also be provided on the expectations of the External Auditor to consider cyber risk as part of an audit.

For Paragraph 30, it should be outlined whether the use of independent assessments for entities providing services to APRA-regulated entities negates the need for testing described in Paragraph 26 (a) to (d).

4 Notifying APRA of information security incidents

A definition of what constitutes a "material information security control weakness" and what is considered to be “a timely manner” for remediation has not been included in the Prudential Standard.

As noted above in ‘2.Management of Information Security Incidents’, external engagement with relevant authorities, depending on the nature of the security incident and extent of any security breach, should be a mandatory obligation for an APRA-regulated entity.

In our view, the notification requirement may be difficult for APRA-regulated entities to comply with as it will be influenced by the maturity of development and testing practices at each individual entity and may generate a significant number of notifications (e.g. agile development that releases a material security control weakness into production that is not remediated for five or more days). In addition, a material security control weakness may be inherent by design (e.g. an application does not operate with least privilege) and treated through mitigating controls (e.g. access to the application is restricted through the use of a filtering proxy). APRA should consider providing guidance as to whether they would still expect to be notified if compensating controls or mitigations are in place, or whether regulated entities risk assessment processes could be relied upon to determine the level of residual risk, and therefore the need to report the security incident, based on the above definitions.

Recommendations

The Prudential Standard, or supporting guidance, should include a definition of a "material information security control weakness" in addition to the definition of "remediate in a timely manner." It is noted that in other APRA standards, breach reporting requirements are determined on the basis of a “significance test”. APRA should consider whether consistency is required amongst these standards with regards to terminology.

We believe that the security incident notification period should be determined and aligned to other reporting obligations, such as for the disclosure of Personal Information to the Office of the Australian Information Commissioner (“OAIC”). APRA should also consider providing specific guidance to regulated entities on their expectations for being notified for material information control weaknesses as noted above in ‘3. Testing and measuring the effectiveness of information security controls’.

In relation to Paragraph 36, clarity should be provided for when APRA may adjust or exclude any requirement in this Prudential Standard in relation to a particular APRA-regulated entity. This includes specifying what circumstances can be applied, or why an APRA-regulated entity may be excluded or have a reduced set of requirements. In addition, if any of these apply, how long an exclusion or reduction may be in place and what, if any, process is required to evaluate and/or terminate the exclusion or reduction of this Prudential Standard.

5 Information assets managed by a related or third party

The terms “related party” and “third party” have not been defined within the Prudential Standard to articulate the types of arrangements that are expected to fall within these categories (e.g. technology providers, non-technology suppliers, individual contractors and joint-ventures). Further, it is not clear whether these terms extend to ‘fourth party’ (and beyond) arrangements within the supply chain.

In our view, risks pertaining to fourth party (and similar type) arrangements are continuing to evolve as the business environment becomes increasingly intertwined and the number and nature of new service providers (e.g. cloud providers, managed service providers and start-ups) continue to enter and disrupt the market. It is key that regulated entities build a related party / third party risk management process which considers the full span of their critical data flows.

With reference to Paragraph 21 which stipulates that “where information assets are managed by a related party or third party, an APRA-regulated entity must evaluate the design and operating effectiveness of that party’s information security controls”, further clarity is required around the scope of this requirement. Specifically, instances where a regulated entity has classified their information assets in terms of sensitivity and criticality (as per Paragraph 19) and has defined a risk-based related / third party assessment approach that aligns to this classification, this does not appear to meet the requirements of Paragraph 21. At present, the draft wording infers that all related / third parties are subject to both design and operating effectiveness testing, which is likely to pose a significant challenge to entities, particularly those with a large vendor base, who currently execute risk-based assessment programs.

In practice, many regulated entities currently undertake stratification activities to assign their related / third parties to different tiers according to their risk profile, and perform assessment activity commensurate with their perceived risk. This typically entails a range of activities being performed, from self-assessment questionnaires (for lower risk suppliers) through to onsite assessments (for higher risk suppliers), which includes design and operating effectiveness testing. The resource / effort implications of performing design and operating effectiveness testing over all related / third parties is likely to require significant investment and uplift for many regulated entities, while not focusing on key risk areas.

Recommendations

We recommend that the Prudential Standard is expanded, or supporting guidance provided, to include definitions (and examples) of what constitutes a related party and a third party, and that these definitions extend to the consideration of fourth party (and similar) arrangements.

In addition, we suggest that further guidance is provided around the scope of Paragraph 21, to provide clarity as to whether a risk-based approach for conducting related / third party assessments would be deemed acceptable, assuming the basis of the framework is of sufficient rigor. If a risk-based approach is acceptable, guidance around the levels of risk that would require detailed assessment activities (i.e. design and operating effectiveness testing) would help to ensure consistency in classification across regulated entities. We suggest that similar to CPS 231 where “material business activity” is defined, further clarity is provided in CPS 234 around APRA’s expectations of managing information security risks associated with APRA-regulated entities’ third / related parties.

www.pwc.com.au

At PwC Australia our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.au