Australian Banking Association

07 June 2018

General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
Level 12
1 Martin Place
SYDNEY NSW 2000
By email ADIpolicy@apra.gov.au

Dear Sir/Madam

Discussion Paper: Information security management: A new cross-industry prudential standard

The Australian Banking Association (**ABA**) appreciates the opportunity to provide the Australian Prudential Regulation Authority (**APRA**) with comments on the Discussion Paper: *Information security management: A new cross-industry prudential standard* (**discussion paper**).

With the active participation of its members, the ABA provides analysis, advice and advocacy for the banking industry and contributes to the development of public policy on banking and other financial services. The ABA works with government, regulators and other stakeholders to improve public awareness and understanding of the industry's contribution to the economy and to ensure Australia's banking customers continue to benefit from a stable, competitive and accessible banking industry.

The ABA welcomes APRA's steps to strengthen the industry's cyber resilience and also supports measures that will require all regulated entities to lift their cyber security capabilities.

The ABA notes APRA's view, based on their annual cyber security surveys, that cyber security is generally well-handled by APRA-regulated entities and that they are predominantly complying with the guidance provided by APRA in Prudential Practice Guide CPG 234 – Management of Security Risk in Information and Information Technology (**CPG 234**). A report[1] released last year by the Australian Strategic Policy Institute on cyber maturity in the Asia Pacific region placed Australia second overall, behind the United States on the back of continued investment in governance reform and implementation of the 2016 Cyber Security Strategy.

The ABA welcomes APRA's first Prudential Standard CPS 234 Information Security (**CPS 234**), and is a strong supporter of all government and regulator initiatives to strengthen the financial sector against cyber attacks. The ABA supports and echoes the comments of APRA that CPS 234 should "[increase] the safety of the data Australians entrust to their financial institutions and enhance overall system stability".

The ABA has several general comments and recommendations on the draft CPS 234 along with some further recommendations on the drafting.

Data security in context of Open Banking & comprehensive credit reporting

Australia's banks are committed to the success of open data which, if delivered properly, can empower customers to use their data across the economy to make the best choices for their circumstances and preferences.

[1] Cyber Maturity in the Asia Pacific Region 2017, Cyber Maturity in the Asia Pacific Region 2017, https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017

The ABA has welcomed[2] the Government's announcement on Open Banking which charts the way forward for this important reform. We are pleased that the Government has outlined a phased introduction that enables it to design a good system that will both benefit customers and protect their data. Open Banking will encourage competition between service providers, leading not only to better prices for customers but also more innovation of products and services.

However, security is paramount.

Developments such as mandatory comprehensive credit reporting (**CCR**)[3], Open Banking[4] and other data sharing government initiatives means that increasingly, sensitive customer data will be (at the request of the customer) transferred from APRA-regulated entities who are subject to CPS 234 and Prudential Practice Guide CPG 235 – Managing Data Risk (**CPG 235**), to financial services entities not regulated by APRA.

It is, and always has been, the ABA's firm view that customer data needs to be protected if trust in the financial system and system stability is to be maintained. The ABA strongly recommends that APRA address and mitigate potential information security risks that arise through the transfer of data to non-APRA-regulated institutions. As outlined in the ABA's submission[5] on Open Banking (Farrell Report) this can be achieved, in part, by applying the right safeguards to all Open Banking participants via a well-designed accreditation model.

Alongside a well-designed accreditation model for Open Banking, APRA must work closely with the Australian Competition and Consumer Commission (**ACCC**) who is tasked with developing the 'Consumer Data Right'[6] to ensure there are robust mechanisms to protect against sensitive customer data being passed to a non-APRA regulated entity where there are legitimate concerns regarding security of that third party.

The ABA fully appreciates the role and scope of APRA's powers, but CPS 234 sits within a broader data-sharing framework and APRA needs to ensure this government-wide data-sharing framework does not impact the ability of APRA-regulated entities to meet the objectives of CPS 234 in response to cyber risk[7]. APRA also needs to ensure government-wide data-sharing frameworks and consumer data-rights have appropriate safeguards to ensure systemic stability and allow all APRA-regulated entities to continue to protect the security of customer data.

APRA will also need to engage with other regulators and Treasury to ensure appropriate and consistent information security standards are in place to facilitate mandatory CCR. In the wake of the 2017 data breach of credit bureau Equifax[8], The New York State Department of Financial Services[9] is requiring all credit reporting agencies to comply with the cyber security regulations that will apply to banks, insurance companies and other financial services institutions.

The resilient objectives of CPS 234 and the security efforts of all APRA-regulated entities could be futile if under initiatives such as Open Banking and mandatory CCR, an APRA-regulated entity is obliged under law, to share customer data with third parties where legitimate cyber and/or information security concerns exist.

---

[2] Australian Banking Association, A sensible path forward for Open Banking, (10 May 2018) https://www.ausbanking.org.au/media/media-releases/media-release-2018/a-sensible-path-forward-for-open-banking

[3] National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018

[4] Review into Open Banking in Australia – Final Report https://treasury.gov.au/consultation/c2018-t247313/

[5] Response to the Farrell Report into Open Banking, ABA submission to Australian Treasury https://www.ausbanking.org.au/images/uploads/ABA_Response_to_the_Farrell_Report_into_Open_Banking.pdf

[6] ACCC Media release, (9 May 2018) ACCC welcomes consumer data right, https://www.accc.gov.au/media-release/accc-welcomes-consumer-data-right

[7] Speech: Computer terminal velocity: APRA's response to an accelerating risk, Geoff Summerhayes, Executive Board Member - Insurance Council of Australia Annual Forum, (7 March 2018) https://www.apra.gov.au/media-centre/speeches/computer-terminal-velocity-apras-response-accelerating-risk

[8] Equifax Media Release, (2 October 2017) Equifax Announces Cybersecurity Firm Has Concluded Forensic Investigation of Cybersecurity Incident https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821

[9] Effective March 1, 2017, the New York State Department of Financial Services (NY DFS) promulgated 23 NYCRR Part 500, a regulation establishing cybersecurity requirements for financial services companies. 23 NYCRR Part 500 is very similar to APRA's draft CPS 234 – Information Security. It is designed to promote the protection of customer information as well as the information technology systems of regulated entities. The regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion

Commencement date

APRA recognises the need to provide supplemental guidance to support this standard in the form of an update to CPG 234. They intend to finalise CPS 234 and CPG 234 in the second half of 2018 with a proposed commencement date of 1 July 2019. This will be challenging for all APRA-regulated entities. Such an unreasonably short implementation timeframe will not provide those entities with sufficient time to take a strategic approach to implementing required changes, especially those that relate to third parties. The ABA will make several recommendations on how APRA can facilitate an orderly adoption of CPS 234 and CPG 234 without any risk to systemic stability or consumers.

There are a number of other upcoming regulatory changes anticipated, including the ACCC consumer data right[10], ASX Corporate Governance Principles and Recommendations[11], and updates to APRA Standards on Operational Risk Management, Outsourcing and Business Continuity. Entities need to take a holistic approach to address these requirements to avoid duplication, rework and unnecessary regulatory compliance costs. Costs associated with rework that could otherwise be deployed in broader improvements in an entity's information security control environment.

In the discussion paper, APRA outlines its preference for Option 2 and proposes a commencement date of 1 July 2019. As previously mentioned, this will be challenging for entities as they will not have clarity of APRA's final requirements and guidance until later in 2018. This will not provide entities sufficient time to take a strategic approach to implementing required changes, especially those that relate to third parties.

ABA's recommendations on commencement dates

In determining the commencement date of CPS 234 and CPG 234, the ABA recommends APRA takes a staggered implementation timeframe for certain obligations (discussed in next section). The ABA also recommends that APRA provides a period of (at least) 12 months to achieve compliance from the publication of finalised versions of CPS 234 and CPG 234 for topics other than those related to third party arrangements where the ABA is recommending a 24-month implementation (discussed below).

Wherever possible, the ABA would also encourage APRA to consider aligning the compliance date for obligations related to third party arrangements with the implementation of revised Prudential Standard CPS 231 – Outsourcing, and allow entities to update contracts with third parties at the next renewal, or at least taking a risk-based approach to contractual updates. The ABA requests this given that each entity is likely to have upwards of a thousand third party contracts to review and negotiate.

Staggered implementation timeframe for certain CPS 234 obligations

Effective 1 March 2017, the New York State Department of Financial Services (**NY DFS**) promulgated 23 NYCRR Part 500, a regulation establishing cyber security requirements for financial services companies. 23 NYCRR Part 500 is very similar to APRA's draft CPS 234. It is designed to promote the protection of customer information as well as the information technology systems of regulated entities. The regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management is required to be responsible for their organisation's cyber security program and file an annual certification confirming compliance with these regulations. The regulation requires an entity's cybersecurity program to ensure the safety and soundness of the institution and protect its customers.

However, a key difference between APRA's draft CPS 234 and 23 NYCRR Part 500 is that APRA has proposed a single commencement date of 1 June 2019 for CPS 234, whereas the NY DFS has recognised that the time it will take to implement each of the requirements set out in its regulations will vary, depending on the nature of each requirement. For example, NY DFS has extended the

[10] ACCC Media release, (9 May 2018) ACCC welcomes consumer data right, https://www.accc.gov.au/media-release/accc-welcomes-consumer-data-right

[11] ASX consultation on a proposed fourth edition of the Corporate Governance Principles and Recommendations https://www.asx.com.au/documents/asx-compliance/cgc-communique-2-may-2018.pdf

implementation periods for the following requirements beyond a base regulation implementation timeframe of 180 days:

- Additional 12 months – for requirements relating to Board reporting obligations of Chief Information Security Officers, penetration testing and vulnerability assessments, risk assessments relating to information systems for the design of cyber security programs, multi-factor authentication, and the provision of cyber security awareness training;
- Additional 18 months – for requirements relating to record retention and audit trail systems, procedures to ensure in-house applications are securely developed, procedures for evaluating the security of externally developed applications utilised by the entity, policies and procedures placing limitations on data retention, and controls including encryption of non-public information; and
- Additional 24 months – for requirements relating to third party service provider security policies.

Importantly, the NY DFS has recognised that the policies and procedures designed to ensure the security of information systems that are accessible or held by third party service providers is likely to require the most time to implement and has granted an additional 24 months for entities to implement these requirements on top of the initial 180-day implementation period.

The NY DFS third party requirements echo many of the requirements set out by APRA in draft CPS 234, including the identification and risk assessment of third party service providers, minimum cyber security practices required to be met by third parties, due diligence processes to evaluate the adequacy of cyber security practices of third parties, and periodic assessment of third party providers to ensure continued adequacy of their cyber security practices.

Given this, the ABA recommends that APRA considers a similarly staggered implementation timeframe for certain CPS 234 obligations, particularly the requirements with third party considerations.

For the paragraphs listed below, the ABA recommends a 24-month implementation:

- Paragraph 15: requires that where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party.
- Paragraph 19: requires that an APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity.
- Paragraph 20: requires an APRA-regulated entity to have information security controls to protect its information assets implemented in a timely manner, including those managed by related parties and third parties.
- Paragraph 21: requires 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.
- Paragraph 27: requires that where information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, an entity must assess whether that testing is commensurate with the requirements in paragraph 26(a)-(e).
- Paragraph 31: requires that an APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties.
- Paragraph 33: requires that where information assets are managed by a related party or third party, an internal audit must assess the information security control assurance provided by that party where an information security incident affecting those information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers.

The ABA notes that to satisfy the requirements of each of these paragraphs all APRA-regulated entities must receive cooperation from relevant third parties, and in some cases a renegotiation of contractual arrangements with third parties will be required. The ultimate timing and resolution of these third party negotiations may not be within the control of APRA-regulated entities, and therefore may not be fully implemented by the proposed commencement date of 1 July 2019, hence the ABA recommendation for a best-endeavours 24-month implementation timeframe for these obligations.

The small to medium sized members of ABA would have over one thousand third party contracts that would need to be assessed and possibly renegotiated due to proposed changes to CPS 234. These contracts would also have to be reassessed once APRA finalises updates their prudential standards on operational risk management, outsourcing and business continuity. The ABA notes that for all our members the burden of continual regulatory change is very material, and more so, when the time to implement these reforms is so compressed. The impact on regional and smaller banks with more limited resources is particularly acute and the complexity facing ADIs with a large footprint is challenging.

Revision to CPG 234

The ABA understands that APRA is considering revised guidance for CPS 234 via an update to CPG 234. We would welcome the opportunity to engage with APRA as revisions to this guidance is being developed.

Materiality thresholds/proportional approach

The ABA understands and supports APRA's intention that CPS 234 is designed to allow for a concept of proportionality and scalability of obligations in accordance with the level of risk assessed. The ABA considers that some of the obligations in draft CPS 234 are expressed in absolute terms (example paragraphs 15, 21, 27, 28 and 31) and requests that the final CPS 234 make the intent of a proportional approach explicit as currently a strict reading of the draft standard appears not to allow such a scaled or proportionate approach.

Clarity and consistency of APRA's notification requirements with other regulators

The ABA supports the need to notify Senior Management, Boards and regulators of material incidents and control weaknesses. Regarding security breaches, numerous[12] Australian regulators, law enforcement and government agencies each provide different criteria as to:

- What they need to be notified of, i.e. different levels of materiality
- When they need to be notified, including not only the timeframe, but whether the trigger to notify is the incident itself, or the determination that the incident is material
- How they are notified, i.e. the information that is required to be submitted.

The draft CPS 234 goes further than other Australian regulators, law enforcement and Government agencies by proposing that entities must notify APRA within 24 hours of "experiencing" a "material" information security incident. There are some incident types, e.g. significant disruption to a payments system or a DDOS attack, that are immediately identifiable, enabling prompt notification. However, in the case of an information security incident, i.e. a data breach, it may take some time for an entity to identify, or be notified of, an information security incident.

[12] By way of example, in the event of a data breach which includes personal information relating to a customer or an impacted individual, financial institutions must currently notify the relevant law enforcement authority, such as the police, if the information is, for example, stolen from a vehicle (this is determined on a case-by-case basis), APRA, the OAIC and the customers and/or impacted individuals. Reporting to ASIC may be required if the breach impacts on the ability of the organisation to provide financial services efficiently, honestly and fairly, which is a Corporations Act requirement.

Where regulators have divergent incident reporting obligations it is extremely likely that the draft CPS 234 will unnecessarily encourage APRA-regulated entities to report every cyber incident they 'experience' to each, and every regulator, law enforcement and government department at the same time as reporting to APRA. A likely outcome is that APRA's obligation to report within 24 hours of experiencing an event will immediately trigger identical breach-reporting to the other stakeholders resulting in regulators, law enforcement and government departments being overwhelmed with notifications of cyber events which ultimately should not have been be reported once the appropriate assessment was completed.

The ABA recommends that APRA:

- Provides guidance on what exactly an APRA-regulated entity must provide to APRA within 24 hours. The ABA remains of the view that a 24-hour notification period (particularly since it is unclear what the purpose and intent behind the requirement) should be reviewed and aligned with industry standards and the timeframes of other regulators.
- Provides further definition, guidance and examples to enable entities to have clarity on what information APRA needs in this initial notification (see GDPR guidance[13]).
- Provides guidance on the process following this initial notification to them. APRA-regulated entities will need to understand the engagement process.
- Align timeframes and triggers for notification of incidents to that of other industry regulators. The ABA would hold that a 24-hour notification is simply too short a timeframe to provide cogent information to APRA beyond an initial report that an entity experienced an incident.
- When finalising CPS 234 considers the reporting obligations and timeframes required by other regulators such as the Office of the Australian Information Commissioner (**OAIC**) and European Union's General Data Protection Regulation (**EU GDPR**)[14].

Third party providers

The ABA's members would appreciate APRA providing guidance on CPS 234 on how to meet the obligations where an APRA-regulated entity engages a third party in a direct contractual relationship, and where a third party engages further providers, e.g. what might be referred to as fourth party/sub-contractor. While the ABA's members agree with APRA that this is not a new issue, guidance from them would be appreciated in how to satisfy them that this is being dealt with appropriately.

Cloud third party providers

Guidance is sought for the treatment of information assets utilising cloud services within the standard. Large global cloud providers will usually have independent and comprehensive attestations available which typically cover a significant portion of the controls that are relevant. These providers tend to be global service providers and while designing and implementing their systems to comply with the multiple requirements across multiple jurisdictions, these large global providers tend not to allow individual customers (regardless of size or location) the right for tailored oversight or audit.

When finalising CPS 234, consideration must be given to the reasonableness of obligations placed on APRA-regulated entities in relation to the large third party providers they use. All entities, including APRA-regulated entities have limited ability to audit and influence large third party providers, and currently rely on an independent report, e.g. SOC 2.

[13] The GDPR guidelines on personal data breach notification under Regulation 2016/679, HTML version of the file http://ec.europa.eu/newsroom/document.cfm?doc_id=47741 - accessed 4 June 2018

[14] From 25 May 2018 there are also requirements to report under the European Union's General Data Protection Regulation (EU GDPR) and/or other offshore data protection regulators, where there is a nexus to that other jurisdiction

Australian Banking Association

Draft Prudential Standard CPS 234

The ABA has a number of recommendations and comments on the draft prudential standard CPS 234 which we have grouped under the headings contained within the draft standard.

Information security capability – paragraphs 14-16

When contracting with a third party provider, APRA-regulated entities specify the security standards, obligations and liabilities of each party in relation to the protection and security of information assets. The ABA agrees with the purpose and intent of paragraphs 14-16, but the proposed drafting is unclear as to what APRA expects in respect of fourth or fifth parties. For example, often the suppliers to APRA-regulated entities will subcontract parts of their operation/infrastructure to another party, i.e. utilise an IaaS/SaaS/Cloud service provider, resulting in the data of an APRA-regulated entity possibly being shared with those subcontractors (4th parties).

Whilst the APRA-regulated entity will have a contractual relationship with the third party supplier and have a "right to audit" that supplier's environment to obtain assurance, an APRA-regulated entity does not have that same contractual right to audit the 4th parties/sub-contractors. An APRA-regulated entity will impose technical standards and contractual obligations on the third party who must ensure these obligations are met by their sub-contractor. The fact remains that APRA-regulated entities may not have direct oversight of how the data is protected at the fourth party/subcontractor.

The ABA recommends that APRA clearly states the extent of responsibilities of an APRA-regulated entity for data held at fourth/fifth, etc parties. We recommend that the scope of these assessments be limited to those parties in which the bank has a direct contractual relationship and that assurance over data held at 4th parties will be obtained via assessing the (direct) supplier's own subcontracting assurance process.

The ABA would welcome clarification whether the assessment is only at contract initiation or whether APRA expects a continuous or regular assessment. If it is to be a regular assessment, then contracts with third parties will need to be negotiated and amended to include "right to audit" clauses. It is highly probable that it would be impossible to negotiate such a clause into a contract for large global organisations such as Google and Amazon, and it will also be impossible to renegotiate the "right to audit clause" for all other existing contracts by July 2019, as each APRA-regulated entity will have thousands of suppliers.

The ABA would also recommend that APRA makes it clear that regulated entities can rely on the independent attestations such as SOC 2[15] reports which are a global industry standard[16]. SOC reports are an independent assessment on "Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy". These reports are intended to meet the needs of a broad range of users that require detailed information and assurance about the controls at a service organisation relevant to security, availability, and processing integrity of the systems the service organisation uses to process users' data, and the confidentiality and privacy of the information processed by these systems. These reports play an important role in:

- Oversight of the organisation
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

There are two types of SOC reports:

- A type 1 report on management's description of a service organisation's system and the suitability of the design of controls.

[15] SOC 2 - SOC for Service Organizations: Trust Services Criteria
[16] The American Institute of CPAs https://www.aicpa.org/about.html

- A type 2 report on management's description of a service organisation's system and the suitability of the design and operating effectiveness of controls.

Information asset identification and classification – paragraph 19

Industry standards refer to criticality and sensitivity of information being the "Confidentiality, Integrity and Availability" of information. Many organisations have historically only classified information assets according to 'Confidentiality' and rely on business continuity management to drive an assessment of availability. The ABA acknowledges that APRA may not want to be prescriptive on the assessment process of criticality and sensitivity, but given cost implications of any rework, the ABA recommends that APRA clarifies whether it expects ADIs to classify information assets across all these dimensions.

Implementation of controls - paragraphs 20-21

CPS 234 states "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." The ABA recommends that this paragraph be reviewed and amended to allow for 'scaling' of the obligation, e.g. to specify that this evaluation process must be commensurate with various factors (such as those in paragraph 20 of the draft CPS 234).

Regarding paragraph 20, the ABA seeks clarification as to whether this includes the availability of the asset as the controls for this may be different to those in respect of confidentiality and integrity.

The ABA would welcome guidance on paragraph 20 (c) in respect of the information asset lifecycle. The lifecycle is perhaps best aligned with Information Security standard ISO 27002 (paragraph 8.1.1) which states "the lifecycle includes creation, processing, storage, transmission, deletion and destruction".

Paragraph 20 requires an assurance commensurate with the inherent risk, whereas paragraph 21 appears to require complete assurance regardless of the risk. The ABA recommends that paragraph 21 be updated such that assessments (or request for assurance) are commensurate with the criticality or sensitivity of the information asset, or commensurate with the potential consequences of an information security incident affecting those assets.

Incident management - paragraphs 22-25

The ABA agrees with the intent of paragraphs 22-25, however further clarification and/or guidance is sought regarding the interrelationship between CPS 234 (in particular paragraphs 23-25) and CPS 232 - Business Continuity Management (**CPS 232**), as strictly by the definitions under paragraph 11 Definitions (b)(iii) an incident also incorporates the availability/accessibility and usability of information. Within CPS 232 critical processes are considered through the business impact analysis, of which availability/accessibility would be considered.

Paragraph 23 is drafted in very broad terms and is therefore open to a number of interpretations. The ABA would recommend guidance in regards to materiality which would be useful to understand what APRA considers a 'plausible incident'. Without further guidance, implementation of the standard, as it stands, is likely to generate substantial and unnecessary regulatory costs and unintended consequences. Should APRA's view be that information security response plans do not require a 'deep dive' in every case, then this obligation should be appropriately scaled in the final standard.

Testing control effectiveness - paragraphs 26-30

Paragraph 26 requires an entity to "test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with [a number of factors]." Given that some vulnerabilities and threat can change daily or even more frequently, and assuming APRA does not require systematic testing to be done at the same rate (daily/ more frequently), the ABA recommends that the paragraph be redrafted to read:

> "The nature and frequency of the systematic testing must be ~~commensurate with~~ appropriate, having regard to [a number of factors]."

Paragraph 27 requires that "where information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, an entity must assess whether that testing is commensurate with paragraph 26 (a)-(d)". The ABA seeks confirmation that APRA intends for this paragraph to require supplier security assessments to be performed at a service-level instead of at an entity-level to comply with this requirement.

Paragraph 28 states that an entity "*must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner, to enable an assessment and potential response by the Board or senior management to mitigate the exposure, as appropriate."* The ABA would recommend further guidance from APRA so that APRA-regulated entities can determine what kind of information security control deficiencies need escalation to Board or senior management. The ABA would suggest the inclusion of a materiality threshold on this escalation and reporting obligation.

Internal audit - paragraphs 31- 33

The ABA seeks clarification in respect of the responsibilities of internal audit for testing the controls at third parties, particularly given that most third party contracts only have the 'right to audit' just once per year. Under draft CPS 234 APRA proposes (in paragraph 21), that APRA-regulated entities test the design and operating effectiveness of third party controls. The ABA would welcome clarification whether APRA expects this to be completed by internal audit or would they accept that where there is a first line function assessing the controls at third parties, that an internal audit can satisfy the requirement by reviewing the effectiveness of the first-line process and coverage.

Regarding third party oversight and assessment, the ABA would highlight to APRA that the impact of the requirements in paragraph 33 have a disproportionate impact on smaller ADIs where functions like internal audits are outsourced, and as such meeting the requirements of paragraph 33 would be a significant financial cost.

APRA notification – paragraphs 34-35

Timeframe for reporting an information security incident (24Hrs)

As discussed in the early part of this submission, the ABA has several concerns with the proposed timeframes for reporting to APRA within 24 hours of an entity 'experiencing' an information security incident that materially affects, or has the potential to materially affect, the entity or interests of depositors, policyholders or other customers.

The APRA 24-hour reporting timeframe after 'experiencing' an information security incident is unreasonably short and wholly impractical. A likely outcome is that all APRA-regulated entities will report each matter to APRA as 24 hours is not enough time to complete an assessment on materiality. APRA will be flooded with reports as every incident, prior to an appropriate assessment and investigation, has 'the potential to materially affect' the entity. The APRA obligation is inconsistent with the obligations to report data breaches to the OAIC under the Privacy Act, both in terms of timeframe and reporting threshold (criteria for reporting).[17]

Recommendation: The ABA's view is that consistent with Prudential Standard CPS 220 Risk Management (**CPS 220**) (para 53), APRA-regulated entities should be required to notify APRA "as soon as practicable, and no more than 10 business days, after it becomes aware…" [that an incident has occurred].

Timeframe for reporting a material internal control weaknesses

APRA proposes that entities notify it within five business days of identifying material internal control weaknesses that the entity is not able to remediate in a timely manner. The ABA would hold that the specified timeframe is unreasonably short and wholly impractical to allow for adequate identification,

[17] The Office of the Australian Information Commissioner (OAIC), Notifiable Data Breaches scheme, https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#which-data-breaches-require-notification

investigation and the development of cogent plans to rectify such matters. The ABA questions the logic behind the five-day notification period and notes that the timeframe differs substantially with the existing statutory requirements currently in place in relation to the Notifiable Data Breaches (**NDB**) scheme regulated by the OAIC which allows time for an entity to complete an appropriate investigation and rectification plan.

Recommendation: The ABA would recommend that the reporting process for CPS 234 be aligned with the process under the OAIC's NDB scheme. This will allow APRA-regulated entities time to develop and execute cogent plans to rectify the weakness which goes to the purpose and intent of CPS 234. Conscious of APRA's focus on systemic and entity stability, the ABA suggests that APRA-regulated entities notify them within 10 business days of assessing that there is a material information security control weakness which cannot be remediated in a timely manner. This allows a more appropriate timeframe as the clock only starts once an assessment has been carried out, which is an approach aligned with (but with a much shorter notification timeframe) the OAIC's NDB scheme regime.

Thresholds for reporting

Paragraph 34 in the draft CPS 234 states "after experiencing an information security incident". However, the earliest an entity could report an incident to APRA is after it becomes aware an incident has occurred. The ABA recommends that consistent with CPS 220, the timeframe for reporting should instead start from when the entity "becomes aware that a material incident has occurred.

Paragraph 34(b) of the draft CPS 234 states that an APRA-regulated entity must notify APRA after experiencing a security incident that "has been notified to other regulators, either in Australia or other jurisdictions." The ABA is concerned that paragraph 34(b) is drafted too broadly. For example, the reporting to OAIC under the mandatory data breach notification regime is quite different, i.e. is one where "a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates." That is, the reporting threshold focuses on harm to an individual, in contrast to the intent of CPS 234 which is to address information security incidents that could affect the stability of an APRA-regulated entity or the financial system. The ABA would welcome confirmation of our understanding that APRA does not intend for every incident reported to a regulator to also be reported to APRA. If this is the case, then it seems paragraph 34(b) is not required – since 34(a) already requires the reporting of any information security incidents that "materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers."

Should APRA retain paragraph 34(b) the ABA recommends that they consider amending the drafting such that events reported to regulators in other jurisdictions are only reported to them if they are material, which they will need to further define. The GDPR guidelines on personal data breach notification under Regulation 2016/679 gives insight to the excessive number and frequency of irrelevant reports APRA could expect from their regulated population under paragraph 34 as currently drafted.

Conclusion

The ABA welcomes APRA's first prudential standard on information security and remains a strong advocate and partner of all government and regulator initiatives to strengthen the financial sector against cyber attacks. The ABA looks forward to working collaboratively with APRA in the finalisation of CPS 234. If you would like any further information, please contact me on 02 8298 0408.

Yours faithfully

Signed by

Aidan O'Shaughnessy
Policy Director - Industry & Prudential Policy
02 8298 0408
aidan.oshaughnessy@ausbanking.org.au