RESPONSE TO SUBMISSIONS

Information security: Cross-industry prudential standard

7 November 2018

Disclaimer and Copyright

Contents

Executive summary

On 7 March 2018, the Australian Prudential Regulation Authority (APRA) proposed a new cross-industry prudential standard for the management of information security. APRA has now released the final version of *Prudential Standard CPS 234 Information Security* (CPS 234).

The information security requirements are designed to ensure APRA-regulated entities have in place appropriate information security capabilities to be resilient against information security incidents. The new standard will apply to all authorised deposit-taking institutions, general insurers, life insurers, private health insurers, licensees of registrable superannuation entities and authorised non-operating holding companies.

APRA received a large number of submissions in response to the March consultation on draft CPS 234. While the draft prudential standard generated considerable comment, many of the issues raised were similar across submissions. APRA has addressed the key issues raised by submissions in this Response Paper. In addition, APRA will shortly be undertaking consultation on an updated cross-industry prudential practice guide on information security, which will replace the current *Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology* (CPG 234).[1]

The new CPS 234 will commence on 1 July 2019, and provides transition arrangements where information assets are managed by third party service providers. CPS 234 forms part of a broader APRA project to review and update APRA's prudential framework in respect of the qualitative management of operational risk across all APRA-regulated industries. APRA anticipates consulting on new and revised requirements and associated guidance on operational risk, outsourcing and business continuity management in 2019.

[1] The revised CPG 234 will be renamed *Prudential Practice Guide CPG 234 Information Security*.

Glossary

ADI	Authorised deposit-taking institution
APRA	Australian Prudential Regulation Authority
Availability	Accessibility and usability of information assets when required
Board	Board of directors
Confidentiality	Access to an information asset being restricted only to those authorised
CPS 231	*Prudential Standard CPS 231 Outsourcing*
CPS 234	*Prudential Standard CPS 234 Information Security*
CPG 234	Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology
Criticality	The potential impact of a loss of availability of an information asset
Entities	APRA-regulated entities including ADIs, authorised NOHCs, general insurers, life insurers, private health insurers and RSE licensees
Information asset	Information and information technology, including software, hardware and data (both soft copy and hard copy)
Integrity	Completeness, accuracy and freedom from unauthorised change or usage
NOHC	Non-operating holding company
RSE	Registrable superannuation entity as defined in s10 of the *Superannuation Industry (Supervision) Act 1993*
RSE licensee	A constitutional corporation, body corporate or group of individual trustees that holds an RSE licence granted under s290 of the *Superannuation Industry (Supervision) Act 1993*
Sensitivity	The potential impact of a loss of either confidentiality or integrity
SPS 231	*Prudential Standard SPS 231 Outsourcing*

Chapter 1 - Introduction

1.1 Background

In March 2018, APRA released a Discussion Paper *Information security: A new cross-industry prudential standard* (Discussion Paper) and draft *Prudential Standard CPS 234 Information Security* (draft CPS 234) which set out proposals on minimum standards for all APRA-regulated entities for information security. The proposals aimed to ensure regulated entities are resilient against information security incidents by requiring them to develop an information security capability commensurate with the information security vulnerabilities and threats they may be exposed to.

As APRA noted in the Discussion Paper, effective information security is increasingly critical, as information security attacks continue to increase in frequency, sophistication and impact. The approach taken in developing draft CPS 234 involved elevating key principles from *Prudential Practice Guide CPG 234 Management of Security Risk in Information and Information Technology* (CPG 234) as well as considering industry-accepted standards and the work of other Australian government agencies.

1.2 Feedback from consultation

APRA received 39 submissions in response to the March consultation from a range of interested parties, including industry bodies, regulated entities and service providers. In addition, APRA met with a number of industry bodies, entities and service providers to further discuss the proposals.

Submissions were generally supportive of the intent and direction of APRA's information security proposals; however, a number of concerns were raised, including the practical application of the proposals where information assets are managed by third parties, and issues around the timing of implementation of the standard and notification requirements. APRA has taken these matters into consideration in revising some aspects of draft CPS 234, details of which are set out in this Response Paper. Along with this Response Paper, APRA is releasing the final version of CPS 234.

1.3 Structure of this paper

Chapter 2 sets out APRA's response to key matters raised in submissions in response to the March Discussion Paper.

Chapter 3 sets out details of other matters where APRA has made revisions to draft CPS 234.

Chapter 2 - Response to submissions

This chapter sets out APRA's response to key matters raised in submissions to the March consultation.

2.1 Identifying and classifying information assets

In the Discussion Paper, APRA noted that consideration of criticality and sensitivity of information assets is an important step in obtaining a comprehensive understanding of a regulated entity's information assets on which its business relies, and the controls needed to ensure security of those information assets. As such, the final version of CPS 234 makes clear that a regulated entity must classify all of its information assets by both criticality and sensitivity; this applies irrespective of whether the regulated entity manages the information assets itself, or the information assets are managed by a third party or related party.

Comments received

Many submissions commented on the application of a materiality threshold to information assets as a general issue, as well as the use of the term 'material' in relation to a number of specific requirements. Issues raised in submissions included:

- that only those information assets deemed material should be covered, rather than all information assets;
- requests for a definition of material information assets aligned with *Prudential Standard CPS 231 Outsourcing* (CPS 231) so that CPS 234 only applies to information assets captured by such a definition;
- general requests for the application of some form of materiality threshold as the basis for whether a criticality and sensitivity analysis needs to be undertaken;
- various requests for the application of a materiality threshold in relation to certain requirements in CPS 234 as the basis for determining the need to apply requirements or the degree of work required in applying certain requirements in the standard. For example, some submissions argued for a materiality threshold to apply in relation to testing the effectiveness of information security controls, and in determining the need to escalate and report testing results to the Board or senior management where security control deficiencies are identified that cannot be remediated in a timely manner;
- requests for clear materiality definitions for reporting information security incidents and information security control weaknesses to APRA under the notification requirements in the prudential standard;
- comments that classifying all information assets would be unduly onerous, costly and difficult to implement;

- requests for clarification on assessment frequency and methods for information asset classification; and

- requests for application of a risk-based approach to both consideration of materiality of third party arrangements and the need to assess information assets managed under third party arrangements.

APRA response

APRA has considered the various matters raised in submissions on the question of materiality. The proposal to apply CPS 234 to all information assets was carefully considered and, as noted in the March Discussion Paper, the intention of the proposal is for regulated entities to obtain a comprehensive understanding of all information assets on which the regulated entity relies, and to focus attention on those assets that would have the greatest impact on the regulated entity in the event of an information security incident. In APRA's view, this approach is prudent and necessary if an entity is to have a properly considered view of its resilience to information security incidents and appropriate consideration of information security threats and vulnerabilities. Information assets that might on the face of it be considered 'immaterial', can provide the mechanism by which an attacker could compromise information assets with higher levels of criticality or sensitivity.

As part of this approach, it is necessary that a regulated entity's information assets managed by third parties and related parties form part of such an assessment. This reflects the fact that ensuring the information security of all information assets remains the responsibility of the regulated entity and that the Board is ultimately responsible for the information security of the regulated entity.

Rather than establishing a threshold whereby controls would only apply to information assets deemed 'material', the classification of assets by criticality and sensitivity allows a regulated entity to apply proportionate controls by assessing the impact of a loss of confidentiality, integrity and availability of each information asset. To provide further clarity around these concepts, the revised CPS 234 includes definitions of criticality and sensitivity as well as the underlying concepts of confidentiality, integrity and availability.

As noted in the March Discussion Paper, CPS 234 prescribes neither the classification method nor the level of granularity — these are left to the regulated entity to determine, as appropriate for the entity's size and complexity. It is noted that regulated entities may record information assets in various ways, sometimes at a very granular level and other times at an aggregated level. Accordingly, a regulated entity could choose to aggregate information assets which are related in some way in order to facilitate the classification process. For example, an internet banking system can be seen as an aggregation of the underlying components (such as applications, databases, operating systems and middleware) and treated as a single information asset for classification purposes. Alternatively, a regulated entity could choose to treat each of the underlying components as individual information assets in their own right. Ultimately, the level of granularity should be sufficient to enable a clear identification of the types of controls required to protect the information asset.

In APRA's view, this principles-based approach is appropriate. To assist regulated entities, APRA will be updating guidance on the classification of information assets in a revised CPG 234 in the first half of 2019.

2.2 Third party arrangements

Draft CPS 234 proposed that requirements on information security capability, information asset identification and classification, implementation of controls, testing control effectiveness and internal audit would apply to information assets, including those assets managed by related parties and third parties. This recognises that there are risks that could affect a regulated entity even when information assets are managed by a related party or third party.

Comments received

A number of submissions raised issues in relation to the application of CPS 234 to information assets managed by third parties. These included:

- queries as to how the requirements would apply where a third party provider engages further service providers (e.g. fourth or fifth party providers or sub-contractors); and
- requests for materiality thresholds similar to those under CPS 231 where only material business activities are subject to the requirements.

APRA response

In APRA's view, a critical component of the framework for the management of information security is that all information assets are subject to the requirements in CPS 234. This was predicated on the view that it is necessary and appropriate that all information assets are subject to the same level of requirements, regardless of who is managing the assets.

Ultimately, information assets are subject to similar threats and vulnerabilities even if managed by another entity. Information assets, whether part of a material business activity or not, may still be subject to threats and vulnerabilities that could impact a regulated entity and the interests of depositors, policyholders, beneficiaries or other customers.

A number of submissions also raised the issue of whether CPS 234 would apply in situations where the management of information assets has been outsourced to a third party and the third party then engages other parties to manage some aspect of those information assets. APRA notes that regardless of whether information assets are managed by a third party, or a downstream provider, a regulated entity must ensure that the information assets are managed in accordance with CPS 234.

The interaction of CPS 234 with outsourcing requirements is covered further in *section 2.5.2 Information security of service providers* of this Response Paper.

2.3 Notifications to APRA

In the March Discussion Paper, APRA proposed that regulated entities would need to notify APRA of information security incidents and also material information control weaknesses that are not expected to be addressed in a timely manner. Specifically, draft CPS 234 proposed that a regulated entity would need to notify APRA as soon as possible, and no later than 24 hours after experiencing an information security incident that materially affected, or

had the potential to materially affect, the regulated entity or the interests of depositors, policyholders, beneficiaries or other customers. In addition, APRA proposed that any information security incident requiring notification to another regulator, whether in Australia or another jurisdiction, would also require notification to APRA. An entity would need to notify APRA no later than five business days after identifying a material information security control weakness that is not expected to be remediated in a timely manner.

Comments received

The proposals for notifying APRA of information security incidents and material information security control weaknesses generated significant comment. Three key concerns were raised:

- the first was in relation to the timeframes for notifying APRA which were generally viewed as potentially onerous and unachievable;
- the second was the meaning of the term 'experiencing', and the need to notify APRA within a set timeframe after experiencing an information security incident, which was considered ambiguous and potentially unachievable in some circumstances; and
- alignment with practices adopted by other regulatory bodies, both in Australia and overseas, with some submissions suggesting APRA's notification requirements would duplicate or overlap with some existing requirements of other Australian Government agencies.

Submissions argued that it is conceivable that regulated entities could experience an information security incident and not become aware of the incident until sometime later. It was argued that it is reasonably likely that in some instances it could be more than 24 hours after an incident occurs before a regulated entity becomes aware of the incident.

In addition, a number of submissions commented on the meaning of 'potential to materially affect' in terms of an information security incident, and 'material' in terms of an information security control weakness, given materiality could vary from one regulated entity to another.

Some submissions suggested that APRA would be inundated with notifications given the absence of defined notification reporting thresholds.

A number of submissions also requested that APRA set out the minimum information it would require as part of the notification requirements.

APRA response

APRA notes the concerns raised in submissions on the notification requirements. APRA remains of the view that the notification requirements are an important aspect of APRA's supervision framework and are intended to provide APRA with timely warning of such incidents.

APRA has considered submissions and made modifications to the original proposed notification requirements. These include:

- requiring a notification once a regulated entity becomes aware of an information security incident, rather than after experiencing the incident;
- increasing the time to notify APRA after becoming aware of an information security incident from 24 hours to 72 hours; and
- increasing the time to report material information security control weaknesses to APRA from five business days to ten business days.

Regulated entities are required to notify APRA as soon as possible of the notifiable events in CPS 234. However, APRA has modified the maximum time for a regulated entity to notify APRA from within 24 hours to within 72 hours of the entity becoming aware of an information security incident. This will provide regulated entities with appropriate time to properly assess an information security incident and determine how to deal with the issue. This change in timeframe also aligns with the breach notification timeframes of other regulators.

For material information security control weaknesses, APRA is of the view that it should be made aware of control weaknesses that are not expected to be remediated in a timely manner as this could be indicative of broader issues with a regulated entity's information security capability. For example, where control assessment activities (e.g. internal audit, disaster recovery testing, penetration testing) identify that a number of key controls are either ineffective or not present.

APRA has, however, amended the time to report such matters to APRA from five business days, as originally proposed, to 10 business days.

The requirement to notify APRA of information security incidents in cases where a regulated entity has notified another regulator, either in Australia or other jurisdictions, is an important mechanism that could identify potential information security issues that may be relevant from a prudential regulation perspective. This requirement will assist APRA in forming a complete picture of information security incidents that could impact regulated entities, including identification of potential trends or correlations evident in reported information security incidents.

APRA notes that submissions generally requested clarity as to the nature and form of notifications required to be provided to APRA. To assist regulated entities, APRA will provide further guidance on the nature and form of notification requirements. APRA expects to do this via revisions to CPG 234. At a minimum, APRA would expect an entity to advise APRA of the regulators who have been informed and the nature of the incident.

2.4 Transition matters

In the March Discussion Paper, APRA indicated that it anticipated releasing the final CPS 234 in late 2018, with a commencement date of 1 July 2019. At that time, APRA also noted that it would consult on a revised CPG 234 once the final CPS 234 was released.

Comments received

A number of submissions noted that, assuming the final CPS 234 was released as anticipated, they would have difficulty complying with the standard from 1 July 2019. Various reasons were identified for the expected difficulties in complying with the standard; the most material were in relation to information assets managed by third parties. Submissions that commented on this matter noted that it would be difficult, if not impossible, to comply without the need to break or renegotiate contracts with third parties; this was deemed impractical, time consuming and potentially costly.

Some submissions also noted that APRA's expected review of other prudential standards regarding operational risk, notably CPS 231, would also likely result in the need to review third party contracts. Submissions argued that APRA should delay the commencement of CPS 234 or provide some sort of transition period recognising the various practical issues involving the management of information assets by third parties.

A number of submissions commented that aspects of CPS 234 would be difficult to implement in the absence of guidance anticipated to be included in the revised CPG 234.

Some submissions from the private health insurance industry noted that the proposed CPS 234 would require significant change for that industry and this supported the need for a longer timeframe for entities to be able to comply.

APRA response

APRA acknowledges the issues raised in submissions concerning the practical difficulties in complying with CPS 234 from 1 July 2019. In response, a transition period has been included for those aspects of CPS 234 that apply to information assets managed by third parties. In this respect, regulated entities will have until the earlier of the next contract renewal date or 1 July 2020 to ensure such arrangements comply with the prudential standard.

As noted above, APRA expects to release a revised CPG 234 in the first half of 2019 to provide guidance on the implementation of CPS 234.

2.5 Scope of application

In the March Discussion Paper, APRA sought industry views on a number of matters concerning the scope of application of the proposals in CPS 234. Details of these matters and responses from submissions are set out below.

2.5.1 Security of customer data

While APRA's prudential role is to ensure that, under all reasonable circumstances, regulated entities meet the financial promises made to depositors, policyholders and beneficiaries, CPS 234 places focus on ensuring the security of all sensitive data, including customer data. This reflects the fact that the information security of an entity, and all customer data, is critical for the continued prudent and sound operation of the regulated entity.

Comments received

A small number of submissions commented on the reference to customers in draft CPS 234. Two submissions questioned why the prudential standard referred to customers and suggested the reference be removed or that it be clarified.

APRA response

APRA considers that the reasons for extending aspects of information security to customer data are prudent and appropriate. The final CPS 234 retains references to customers and, as noted in the March Discussion Paper, APRA expects regulated entities to ensure the security of customer data, including, for example, borrower data.

2.5.2 Information security of service providers

Many regulated entities outsource some aspect of their business activities, particularly in the superannuation industry where outsourcing material business activities is common. Where outsourcing involves a material business activity, as defined in CPS 231 and *Prudential Standard SPS 231 Outsourcing* (SPS 231), the outsourcing arrangement must comply with CPS 231/SPS 231, including being subject to appropriate due diligence, approval and ongoing monitoring of the outsourced activity.

The March Discussion Paper noted that, in complying with prudential requirements in respect of risks arising from outsourcing material business activities, a regulated entity's due diligence and ongoing monitoring should include an assessment of the information security capability of the outsourcing provider. Importantly, the proposals in draft CPS 234 would extend these requirements to cover all service providers who manage information assets for a regulated entity, regardless of whether the outsourcing arrangement in question covers a material business activity or not. That is, all information assets of a regulated entity, whether managed in-house or by a service provider, whether to a related party or third party, would be subject to the requirements of CPS 234.

Comments received

Two submissions commented on the proposed application of CPS 234 to cover all information assets managed by service providers. Both recommended that CPS 234 should only apply to material outsourcing arrangements involving information assets, consistent with the application of CPS 231/SPS 231 to outsourcing of material business activities only.

APRA's response

As APRA noted in the March Discussion Paper, given the importance of information security and the potential consequences of an information security incident, APRA remains of the view that the requirements in CPS 234 should apply to all outsourcing of information assets, whether or not those assets form part of the outsourcing of material business activities. This reflects that the criticality and sensitivity of information assets managed under any outsourcing arrangement may mean that a compromise of those assets could have material consequences for a regulated entity and its customers. In this regard, APRA considers that

the application of CPS 234 to all information assets managed by a third party or related party as part of an outsourcing arrangement remains appropriate.

Other matters related to the application of requirements in respect of third parties and related parties are covered in *section 2.2 Third party arrangements* of this Response Paper.

Chapter 3 - Other issues

This chapter sets out details of other minor matters where APRA has made revisions to CPS 234, in addition to those matters set out in Chapter 2.

3.1 Other amendments to CPS 234

In response to submissions, APRA has made a number of minor amendments to CPS 234 to clarify and assist with the interpretation of the prudential standard. The key additional changes are:

- clarification of the Board's responsibilities for information security;
- clarification that CPS 234 applies to all information assets managed by related parties and third parties, not only those captured under outsourcing agreements involving material business activities;
- clarification of the life-cycle of information assets;
- clarification that regulated entities must annually review and test their information security response plans;
- a new requirement for the nature and frequency of testing the effectiveness of information security controls to be commensurate with the materiality and frequency of change to information assets;
- modifications to the requirement for testing control effectiveness where information assets are managed by a related party or third party and the entity relies on its information security control testing; and
- clarification of the role of internal audit where information assets are managed by a related party or third party.

Attachment A - Regulatory costs

This Attachment sets out the steps taken in finalising the new CPS 234, including details of compliance cost estimates for implementation of the standard.

In March 2018, APRA released for public consultation a Discussion Paper which outlined three options for the future implementation of the information security standard as well as a broader project to review and update all existing prudential standards and guidance across regulated entities on operational risk, including updating standards on outsourcing and business continuity management. Those three options were:

- Option 1 — status quo — continue with existing standards and guidance, relying on supervisory discretion to address any deficiencies in the risk management practices of entities;

- Option 2 — stepped approach — prioritise information security management and first introduce prudential requirements on information security. Subsequently, introduce the remainder of the proposal. This option will focus industry's attention on the highest priority risk; APRA considers that an information security event could have a material impact on an entity; and

- Option 3 — simultaneous approach — introduce new prudential standards on operational risk management, and information security, and revise prudential standards on business continuity and outsourcing.

Assessment of regulatory costs

As part of its public consultation, APRA sought information from stakeholders on the compliance impacts of the proposed changes set out in the Discussion Paper, including associated substantive costs. Respondents were asked to use the Australian Government's Regulatory Burden Measurement Tool (RBMT) to assess regulatory costs.

None of the submissions provided regulatory cost estimates using the RBMT. However, some respondents provided high-level cost estimates of the expected cost impacts of the proposed options. APRA has taken these cost estimates into account in developing its own cost estimates for each option.

APRA has considered relevant compliance costs (e.g. administration, substantive and financial compliance costs as applicable) in estimating the regulatory cost of each option.

Option 1: Status quo

Under this option, there would be no new standard on operational risk management or information security and existing standards on outsourcing and business continuity management would continue without change. This approach would be problematic as it would mean APRA's prudential framework in this area would be outdated and not require proper consideration of an area of rapid change with new and emerging technologies in

information technology and information security nor reflect developments in operational risk. There would, however, be no initial compliance costs given no change to the status quo.

Table 1—Average annual regulatory costs

Sector	Business	Community organisations	Individuals	Total change in costs
Total change in cost by sector ($ million)	0	0	0	0

Option 2: Stepped approach

Under this option, APRA would adopt a staged implementation of prudential requirements on operational risk, information security, business continuity management and outsourcing. As information security is considered a current heightened area of risk, releasing a new information security prudential standard would be prioritised. Subsequently, APRA would introduce an operational risk management prudential standard and revise the business continuity management and outsourcing prudential standards.

Where submissions commented on the three options, option 2 was preferred as it would allow industry to focus on information security as a priority, provide adequate time for entities to adopt information security requirements, ensure compliance without overburdening affected entities and minimise the immediate impact of compliance costs.

A few submissions estimated that there will be significant one-off and recurrent costs in changing oversight, monitoring, reporting and other systems. While submissions highlighted the considerable compliance costs that may be incurred, they were balanced by other comments that any additional compliance costs would be outweighed by the overall benefits provided to the financial sector and digital economy, that any increase in costs should be perceived as investments rather than incurrences, and that proposals will ensure resilience and strength in the financial sector as a whole. Also, some costs provided relate to changes to systems as part of other programmes of work which are not only related to changes needed to address the information security proposals.

APRA expects costs to vary depending on the size of entities, the extent to which entities have already incorporated existing information security guidance into their policy frameworks and operations and resourcing available to facilitate compliance with information security requirements.

APRA has considered costs involved in the implementation of the information security proposals, including costs involved with contractual changes, information asset identification and classification, risk management, compliance and operational costs. Estimated costs have been projected for all affected industries, taking into account various factors such as the size of entities and estimates of staff involvement. APRA expects costs in the first year to be greatest and then taper off as entities embed the information security proposals into their business. Consequently, the average costs estimated below are lower than the expected costs in the early implementation period.

Table 2—Average annual regulatory costs

Sector	Business	Community organisations	Individuals	Total change in costs
Total change in cost by sector ($ million)	6.7	0	0	6.7

Option 3: Simultaneous approach

APRA estimates that the costs for option 3 will be similar to, or the same as, option 2 as entities will be required to implement the same information security requirements, however the costs will emerge in later years and the burden may be greater at that time due to the deferral of implementation until other operational risk related requirements are determined.

The average annual cost estimate below replicates the costs for option 2; APRA would expect these costs to occur in later years when the information security prudential standard would be released in conjunction with the other new and revised prudential standards.

Table 3—Average annual regulatory costs

Sector	Business	Community organisations	Individuals	Total change in costs
Total change in cost by sector ($ million)	6.7	0	0	6.7

Summary assessment of options

Considering each option and the associated costs and benefits, as well as feedback from industry, APRA's preferred approach is option 2; the stepped approach. Implementation of the full proposal in stages allows industry to focus attention on information security first, which is considered to be an area of current industry weakness.

Table 4—Summary of net benefits of each option

	Option 1	Option 2	Option 3
Compliance cost	No change	Moderate cost	Moderate cost
Reduces system-wide risk relating to information security incidents	No change	Meets this criteria	Meets this criteria
Considers local conditions	Does not meet this criteria	Meets this criteria	Meets this criteria
Overall	Low net cost	Moderate net cost	Moderate net cost

Implementation and review

The new requirements will take effect from 1 July 2019. APRA will allow a transition period where a regulated entity's information assets are managed by a third party; in this case, requirements will apply from the earlier of the next renewal date of the contract with the third party or 1 July 2020.

APRA's prudential framework is regularly reviewed, including consideration of whether the requirements continue to reflect good practice, remain consistent with international standards and remain relevant and effective in facilitating sound risk management practices.

APRA