DISCUSSION PAPER

Information security management: A new cross-industry prudential standard

7 March 2018

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY | WWW.APRA.GOV.AU

Disclaimer and Copyright

While APRA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

Contents

Executive summary

The Australian Prudential Regulation Authority (APRA) proposes to implement a cross-industry framework for the management of information security.

Information security management requires ongoing vigilance, improvement, investment and oversight. Technological developments continue to expand the scope and sophistication of potential malicious activity against financial institutions. The conclusions from APRA's two cyber surveys remain valid—there is no 'end-state' for information security, therefore requiring a continuous cycle of investment in sound practices among APRA-regulated entities.[1]

APRA's proposed requirements are set out in a new cross-industry prudential standard, draft *Prudential Standard CPS 234 Information Security* (draft CPS 234), which APRA proposes to apply to authorised deposit-taking institutions (ADIs), general insurers, life insurers, private health insurers, licensees of registrable superannuation entities (RSE licensees) and authorised or registered non-operating holding companies.

Draft CPS 234 covers the following areas:

- roles and responsibilities;
- information security capability and policy framework;
- information assets and controls, including incident management;
- testing and internal audit;
- APRA notifications.

Draft CPS 234 forms part of a broader APRA project to update the prudential framework in respect of the qualitative management of operational risk across all APRA-regulated industries.

[1] See *APRA Insight* Issue Four 2017 at http://www.apra.gov.au/Insight/Pages/default.aspx; *APRA Insight* Issue Three 2016 http://www.apra.gov.au/Insight/Pages/insight-issue3-2016.html; and Information Paper *2015/16 Cyber Security Survey Results*: http://www.apra.gov.au/adi/Publications/Pages/other-information-for-adis.aspx.

Chapter 1 – Introduction

1.1 Background

Sound risk management is a cornerstone of APRA's prudential requirements across all APRA-regulated industries, and includes the management of information security. Effective information security is increasingly critical as information security attacks are increasing in frequency, sophistication and impact, with perpetrators continuously refining their efforts to compromise systems, networks and information worldwide. This was clearly evident from the results of APRA's two cyber surveys, which indicated that incidents varied in nature, sophistication and impact.

All APRA-regulated entities (entities) must operate on the basis that information security attacks are and will continue to remain a significant threat. Accordingly, the management of information security should be based on the expectation that significant cyber security incidents will be experienced. While to date, no entity has suffered material losses from an information security incident, and security controls have protected against past attacks, APRA strongly believes that past experience is not grounds for complacency. In APRA's view, preparedness is vital.

APRA action to date has included the introduction of *Prudential Practice Guide CPG 234 Management of security risk in information and information technology* (CPG 234), increased on-site supervision and an increased expectation for entities to secure themselves against information security attacks and implement improved mechanisms to quickly detect and respond to attacks when they occur. The introduction of a new cross-industry information security prudential standard addresses the need to establish minimum standards across all industries.

The proposals in draft CPS 234 were informed by discussions with industry bodies and service providers during 2017. The proposals in draft CPS 234 reflect the following:

- the need to address a clear gap in APRA's prudential framework and outline minimum requirements for the management of information security across an entity;
- an entity's exposure to the risk of information security incidents exists across its extended business environment, including information and information technology managed by third-party providers (e.g. cloud providers);
- the rapidly evolving nature of information security threats and vulnerabilities; and
- cyber security surveys conducted by APRA, and other supervisory activities, have revealed weaknesses in industry's information security management practices.

For private health insurers, the proposals in this paper form part of Phase one of the private health insurance prudential policy roadmap. The roadmap outlines APRA's intention to review aspects of the prudential framework relating to operational risk, including business continuity management and outsourcing, as part of a broader APRA project to refresh those requirements across all APRA-regulated industries. As this work has progressed, and in light of the increasing prevalence of cyber risk, APRA has decided to prioritise the delivery of the information security component of the review.

1.2 Current framework

To date, APRA has supervised and communicated the management of information security in two key ways. Firstly, through the application of centralised key risk management principles in *Prudential Standard CPS 220 Risk Management* and *Prudential Standard SPS 220 Risk Management* (CPS/SPS 220). These principles include key Board requirements and cover all material risks that impact the entity. Secondly, through the introduction of cross-industry guidance on information security in CPG 234. CPG 234 was introduced in 2010 to communicate best practices and identified industry weaknesses.

Industry has by and large appropriately applied the above risk management principles and guidance to strengthen its information security management practices. However, APRA is concerned that industry needs to better address the evolving nature of information security matters. APRA is taking steps to strengthen the information security resilience across all APRA-regulated industries through the proposed new cross-industry standard on the management of information security.

1.3 Development of proposed requirements

The proposals in draft CPS 234 focus on the minimum requirements for an entity's management of information security. The approach taken to develop the proposed requirements has involved elevating key principles from CPG 234.

When developing the proposed requirements, APRA also considered the work of other Australian government agencies and industry-accepted standards to ensure that industry-accepted practices and language are leveraged where appropriate.

1.4 Link to risk management practices

APRA's prudential framework is structured with key risk management principles set out in CPS/SPS 220. While CPS/SPS 220 are intended to cover all risks, not all prudential standards within the prudential framework contain links back to CPS/SPS 220. Similarly, draft CPS 234 is designed to be part of the broader CPS/SPS 220 framework but does not explicitly link to CPS/SPS 220 risk management principles. Also, the notion of 'vulnerabilities and threats' is used in place of 'risk' to reflect the nature of information security.

Although there is no specific CPS/SPS 220 linkage, APRA expects that information security risks will have the same visibility as other risks contained in an entity's Risk Management Framework and other required elements of CPS/SPS 220. Moreover, the standard does not preclude an entity from having risk management staff involved in information security management. APRA believes that information security management necessitates the involvement of various staff and a number of proposals are drafted so as to allow an entity to identify the most appropriate staff to meet the requirements.

1.5 Balancing financial safety and other considerations

APRA's mandate includes balancing the objectives of financial safety and efficiency, competition, contestability and competitive neutrality, and, in balancing these objectives, promote financial system stability in Australia. APRA considers that, on balance, the proposals in this discussion paper will strengthen the resilience of the Australian regulatory financial framework, improve financial safety and promote financial system stability.

PRIMARY OBJECTIVES	
Financial safety ⬆	Financial system stability ⬆
Improved: Financial safety is supported by improved risk management practices through a set of minimum requirements.	**Improved:** Financial system stability is expected to improve through stronger and more consistent management of information security risks across all APRA-regulated industries.

OTHER CONSIDERATIONS	
Efficiency ↔	**No material change:** the proposals in this paper have no material impact on efficiency.
Competition ↔	**No material change:** prudential requirements on information security reflect existing guidance and industry practice, and are not expected to affect the ability of entities to compete with one another or with unregulated entities.
Contestability ↔	**No material change**: the proposals in this paper have no material impact on contestability.
Competitive neutrality ↔	**No material change:** the proposals in this paper have no material impact on competitive neutrality.

Chapter 2 – Scope of application

This chapter sets out key considerations when applying the proposals in draft CPS 234. APRA seeks industry views on any implementation issues that could arise.

2.1 Security of customer data

APRA's core prudential role is to establish and enforce prudential standards and practices designed to ensure that, under all reasonable circumstances, entities meet the financial promises made to depositors, policyholders and beneficiaries. However, more generally, APRA promotes soundness in business behaviour and risk management on the part of the entities it supervises, and expects those entities to ensure the security of all customer data including, for example, borrower data.

2.2 Information security of service providers

Some APRA–regulated entities either wholly or predominantly outsource their material business activities, particularly in the superannuation industry. APRA's prudential framework therefore requires that any outsourcing arrangements involving material business activities are subject to appropriate due diligence, approval and ongoing monitoring.[2]

In light of these overarching requirements, APRA expects such entities would apply the requirements of draft CPS 234 in a manner commensurate with the nature of their business operations and their service provision arrangements. Moreover, the management of outsourcing-related risks is expected to form a significant aspect of the entity's information security control framework. This means that, in complying with prudential requirements in respect of risks arising from outsourcing material business activities, an entity's due diligence and ongoing monitoring should include an assessment of the information security capability of the outsourcing provider. Draft CPS 234 extends these requirements to include an assessment of the information security capability of all other outsourcing providers, commensurate with the potential consequences of an information security incident. In respect of outsourced arrangements, additional requirements in draft CPS 234 include:

- classifying information assets by criticality and sensitivity;
- adopting processes to detect and respond to information security incidents;
- assessing the control testing frameworks and audit assurance of outsourcing providers; and
- notifying APRA of information security incidents and control weaknesses.

[2] APRA's prudential standards governing outsourcing risk are *Prudential Standard CPS 231 Outsourcing* and *Prudential Standard SPS 231 Outsourcing* (CPS/SPS 231).

In addition, draft CPS 234 requires an entity to implement information security controls over its information assets. For an entity that wholly or predominantly outsources its material business activities, APRA expects this would include controls over the assets it directly controls and information security aspects of its outsourced arrangements directly within its control, such as the data interface between the entity and outsourcing provider.

An entity may choose to outsource the activities associated with meeting the requirements detailed above. However, regardless of an entity's business model, draft CPS 234 reinforces that the Board of an entity is ultimately responsible for information security, and requires the entity to clearly set out roles and responsibilities with respect to information security.

2.3 Group application

CPS/SPS 220 requires an entity that is the head of a group to comply with the respective standard in its capacity as a regulated entity as well as on a group basis. CPS/SPS 220 also requires that risk management requirements are applied appropriately throughout the group including entities that are not APRA-regulated. CPS 220 also includes additional requirements for the head of a group with respect to group risk management frameworks, group functions and APRA notifications.

APRA believes draft CPS 234 is consistent with this broader CPS/SPS 220 group approach, while not applying any additional requirements specific to information security. While the CPS/SPS 220 group approach is considered to be sensible and appropriate for the proposals set out in draft CPS 234, APRA seeks industry feedback on this group application and whether there should be any distinctions for information security management.

Chapter 3 – Requirements for managing information security

3.1 Roles and responsibilities

The proposals in the 'roles and responsibilities' section of draft CPS 234 cover both Board responsibilities and those of the entity. APRA believes that information security management necessitates the involvement of all personnel as well as specific roles for information security specialists.

Although key Board requirements are covered in CPS/SPS 220, draft CPS 234 includes a proposed Board requirement specific to information security. It is therefore considered to be an extension of those outlined in CPS/SPS 220.

Paragraph 12 of draft CPS 234 articulates that the Board is ultimately responsible for information security. This proposal seeks to highlight the Board's responsibility to ensure a level of information security that not only addresses the rapidly evolving industry but links to the broader strategic objective for continued sound operation of the entity. Also, the proposal reflects the need to close an observed gap in Board engagement on information security. During informal consultation with industry, feedback indicated that introducing prudential requirements to focus Board attention on information security could improve current practices and the delegation of information security management and incident management to information security specialists.

In paragraph 13, APRA proposes that an entity clearly define the formal roles and responsibilities that are involved in the management of information security. This proposal seeks to ensure that all functions necessary to manage information security are specified and designated to personnel, including the Board. The degree to which a Board chooses to engage on information security matters varies considerably from entity to entity, and the proposal seeks to enable the Board to stipulate the degree of engagement that it wishes to have with regard to information security matters in light of its responsibility in paragraph 12. In implementing this requirement, an ADI will need to have regard to the recently enacted Banking Executive Accountability Regime (BEAR) legislation, which requires an ADI to nominate a senior executive with responsibility for 'information management, including information technology systems for the ADI'.[3]

3.2 Information security capability and framework

The concept of 'information security capability' is intended to describe the resources, skillset and controls necessary to maintain information security. The concept of 'capability' is a generally accepted industry term and reflects the need to access appropriately skilled resources and have a set of controls that keeps in step with the evolving threat landscape.

[3] Refer to section 37BA(3)(f) of the *Banking Act 1959*.

In establishing an information security capability, draft CPS 234 proposes that an entity link its capability to the Board's role to ensure that information security is commensurate with the size and extent of threats, and which enables the continued sound operation of the entity. Through this proposal, APRA seeks to reinforce the significance of information security and the need to address its impact on the entity more broadly.

Draft CPS 234 proposes an entity's policy framework that underpins information security correspond to exposures to information security vulnerabilities and threats. This requirement is intended to emphasize the expectation that an entity's framework be adaptive.

3.3 Criticality and sensitivity

CPG 234 provides guidance to entities on the consideration of criticality and sensitivity of their information assets. APRA is of the view that this assessment is an important step in obtaining a comprehensive understanding of the entity's information assets on which its business relies and the controls needed to ensure their security.

As such, draft CPS 234 proposes that an entity classify its information assets by criticality and sensitivity. In addition this this, an entity must ensure information security controls are implemented over those assets, commensurate with their criticality and sensitivity, irrespective of whether the information asset is managed by a related or third party. Given the existing guidance, APRA believes that further prescription on the assessment process is unnecessary.

The intention of this provision is for entities to obtain a comprehensive understanding of the information assets on which the business relies, and, focus attention on those assets that would have the greatest impact on the entity in the event of a security incident. APRA strongly believes that 'you are only as strong as your weakest link' and the proposed scope will enable entities to consider information assets that may expose those with higher criticality or sensitivity. Finally, draft CPS 234 does not prescribe the information asset classification method and granularity, leaving the entity to determine the appropriate scaling.

This approach differs from other areas of APRA's prudential framework, which generally limit particular risk management requirements to material risk exposures. However, materiality typically requires a degree of judgement and APRA believes techniques are not yet available for a materiality concept to be readily applied to information security.

3.4 Testing

APRA's ongoing supervisory activities have identified variability and weaknesses in the industry's control testing. APRA is of the view that the testing of controls is paramount to ensure that information security controls are commensurate with an entity's information security exposures.

Through the proposed testing requirements in draft CPS 234, APRA seeks to address a crucial minimum expectation that testing be orderly, structured and comprehensive. While the proposals do not stipulate timeframes for testing, the key objective of the proposals is to ensure that the testing conducted is commensurate with the entity's exposures to vulnerabilities and threats and the rate at which these exposures evolve.

3.5 Internal audit

Internal audit requirements are predominantly covered in *Prudential Standard CPS 510 Governance* and *Prudential Standard SPS 510 Governance*. For ADIs, there are also requirements covering the scope of internal audit in *Prudential Standard APS 310 Audit and related matters*.

Draft CPS 234 includes proposed internal audit requirements specific to information security. APRA considers internal audit as a critical function to provide the Board with assurance on information security controls protecting an entity's information assets. However, many entities do not have sufficient in-house information security expertise within the internal audit function, and will need to engage external experts. Draft CPS 234 proposes that the internal audit function have access to persons appropriately skilled in information security in order to provide adequate assurance. Under the proposal, an entity may use staff employed internally or engaged externally to provide this assurance.

As internal audit could have limited access (if any) to directly audit the controls on information assets managed by third parties (e.g. cloud services), draft CPS 234 proposes that internal audit assess the third party assurance of controls over such assets. APRA expects the Board and senior management would be informed if internal audit has no visibility of third party assurance over information assets managed by third parties or was uncomfortable with the robustness of that assurance.

3.6 APRA Notifications

APRA proposes that entities notify APRA of information security incidents and material internal control weaknesses that may not be addressed in a timely manner.

The need to notify APRA of material internal control weaknesses is an extension of the requirement to notify APRA of an actual disruption or incident. Through this notification, APRA will be made aware of circumstances when the likelihood of a material information security incident impacting an entity is heightened. APRA will provide examples in guidance as to the underlying expectations of this requirement.

Where an entity is required to notify APRA of information security incidents under more than one prudential standard, the entity would only be required to notify APRA once.

APRA seeks industry feedback on the feasibility of the notification requirements.

Chapter 4 – Revisions to CPG 234

APRA will update CPG 234 to reflect the final version of CPS 234. APRA will also update CPG 234 to communicate APRA's current expectations on information security, taking into account issues identified through ongoing supervisory activities and the results of the cyber security surveys.

APRA intends to consult on revised guidance once the final CPS 234 is released. In the meantime, APRA seeks industry views on guidance topics that would assist with understanding and implementation of the proposed requirements. Currently, APRA proposes to cover the following topics in the revised CPG 234:

- information security capability – including context, link to Board's responsibility for entity's information security and considerations when investing in information security capability;
- role of the Board – context, outline level of engagement;
- information asset classification – considerations in classifying information assets by criticality and sensitivity;
- information security of service providers - how to assess controls implemented by third and related parties;
- incident management – examples of plausible information security incidents, examples of incident stages;
- information security control testing – what is meant by systematic, how to assess testing by third or related parties and sound practice testing approaches;
- internal audit – what is meant by 'designed and operating effectively', how to assess assurance provided by third parties; and
- APRA notification – examples of information security incidents and material information security control weaknesses.

In revising CPG 234, APRA will review the need to update other prudential practice guides relevant to information security.

Chapter 5 – Consultation and next steps

5.1 Request for submissions and cost-benefit analysis information

APRA invites written submissions on the proposals set out in this discussion paper. Written submissions should be sent to PolicyDevelopment@apra.gov.au by 7 June 2018 and addressed to:

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

Important disclosure notice—publication of submissions

All information in submissions will be made available to the public on the APRA website unless a respondent expressly requests that all or part of the submission is to remain in confidence.

Automatically generated confidentiality statements in emails do not suffice for this purpose.

Respondents who would like part of their submission to remain in confidence should provide this information marked as confidential in a separate attachment.

Submissions may be the subject of a request for access made under the *Freedom of Information Act 1982* (FOIA).

APRA will determine such requests, if any, in accordance with the provisions of the FOIA. Information in the submission about any APRA-regulated entity that is not in the public domain and that is identified as confidential will be protected by section 56 of the *Australian Prudential Regulation Authority Act 1998* and will therefore be exempt from production under the FOIA.

APRA asks that all stakeholders use this consultation opportunity to provide information on the compliance impact of the proposals, and any other substantive costs associated with the changes. Compliance costs are defined as direct costs to businesses of performing activities associated with complying with government regulation. Specifically, information is sought on any changes to compliance costs incurred by businesses as a result of APRA's proposals.

Consistent with the Government's approach, APRA will use the methodology behind the Commonwealth Regulatory Burden Measure to assess compliance costs. This tool is designed to capture the relevant costs in a structured way, including a separate assessment of upfront costs and ongoing costs. It is available at https://rbm.obpr.gov.au/.

APRA requests that respondents use this methodology to estimate costs to ensure the data supplied to APRA can be aggregated and used in an industry-wide assessment. When submitting their costs assessment to APRA, respondents should include any assumptions made and, where relevant, any limitations inherent in their assessment. Feedback should address the additional costs incurred as a result of complying with APRA's requirements, not activities that institutions would undertake due to foreign regulatory requirements or in their ordinary course of business.

5.2 Implementation and next steps

Following the close of this consultation on 7 June 2018, APRA anticipates that the finalised prudential standard CPS 234 will be released in the fourth quarter of 2018 and come into effect on 1 July 2019.

In determining an implementation date, APRA has been mindful of other regulatory changes underway across each regulated industry. APRA believes that the potential impact of material information security incidents and impending need to strengthen practices warrants a relatively short implementation timeframe.

APRA invites feedback about the intended implementation timeline.

Next Steps

The proposed information security standard is part of a broader APRA project to update its existing prudential standards and guidance across all APRA-regulated industries regarding operational risk, including updated standards on outsourcing and business continuity management.

The objective of this project is to align prudential requirements to sound industry practice, and community expectations for a high degree of resilience to material operational risk incidents. APRA's intention is to also outline broad-based expectations for operational risk and resilience that aligns to the overarching risk management framework.

This discussion paper prioritises the consultation on information security management, given that APRA does not have existing requirements in this area. APRA intends to consult on broader operational risk requirements later in 2018.

Attachment A – Policy options and estimated comparative net benefits

APRA has considered three options for enhancing the framework for the qualitative management of operational risk by entities:

Option	Approach
Option 1: Status quo	Continue with the existing standards and guidance, relying on supervisory discretion to address any deficiencies in the risk management practices of entities.
Option 2: Stepped approach	Introduce prudential requirements on information security ahead of other requirements on the qualitative management of operational risk.
Option 3: Simultaneous approach	Introduce a prudential standard on the qualitative management of operational risk, which includes revised content on business continuity and outsourcing, and new content on information security.

The above options are discussed further below, together with a preliminary analysis of the costs and benefits of each. The analysis of costs associated with each option focuses on compliance costs, that is, the direct administrative, substantive (business) and financial costs incurred by entities in complying with government regulation. Indirect costs for entities and other stakeholders arising as a consequence of regulation (or not applying regulation) are also considered.

Any information provided in response to APRA's request for cost-benefit analysis information (see Chapter 6 of this discussion paper) will be used by APRA to quantify the change in regulatory burden using the Regulatory Burden Measurement Tool, and inform calculations of the net benefits of the proposal.

Option 1: Status quo

Under option 1, the management of operational risks would continue to be addressed through existing standards and guidance, as well as through APRA's supervision activities. Maintaining the status quo would not cause any immediate additional compliance costs for entities. However, if steps are not taken to address the heightened operational risk exposures through strengthening of prudential requirements, there are a range of indirect costs and implications that could result.

1. Vulnerability to risks – APRA's current requirements and guidance on subsets of operational risk were developed some time ago. Significant developments in industry practices in recent years has resulted in an evolution and growing prevalence of operational risks, including those associated with information security. As a result, APRA-regulated entities remain vulnerable to a range of such risks, ranging from low impact to potentially material. APRA's current requirements and guidance contain dated language and have incomplete coverage as they do not address current industry

weaknesses. If prudential requirements are not introduced to strengthen the management of operational risks, particularly regarding information security, the threat to the ongoing viability of entities, and financial stability more broadly, is likely to increase significantly.

2. Inconsistencies within industry and across jurisdictions – variable management of operational risks, particularly information security risks, across APRA-regulated entities would result in continued uncertainty about the resilience of the Australian financial sector, particularly in comparison to other jurisdictions. Without new prudential requirements, entities may be viewed by stakeholders as falling behind international standards, with potential detrimental impacts.

APRA believes the *status quo* will result in a negative net impact as the costs associated with this option would become more significant over time; that is, as industry practices and risks continue to rapidly evolve but risk management by entities does not keep pace.

Option 2: Stepped approach

Option 2 is to prioritise information security, being a current heightened area of risk, and introduce a prudential standard containing a minimum set of key principles to manage information security. APRA considers that an information security incident could have a material impact on an entity's capacity to operate as a going concern and fulfil its obligations.

APRA would subsequently introduce prudential requirements on the qualitative management of operational risk more broadly that includes updated requirements on business continuity and outsourcing (update CPS 231 and CPS 232)

Entities would be required to comply with the information security prudential standard by 1 July 2019. This timeframe would allow industry sufficient time to make changes to comply with the new requirements. The subsequent introduction of prudential requirements on operational risk more broadly would be implemented over a longer timeframe.

Once all requirements are finalised, entities would benefit from strengthened operational risk management practices that address the growing range of operational risks and incidents. For APRA, inconsistencies within industry and across jurisdictions would be addressed.

APRA expects that implementing prudential requirements on information security initially and then other operational risk requirements later, would result in compliance costs, however these would be outweighed by the benefits of having strengthened risk management practices in place.

Finally, given that entities are already operating in an environment of regulatory and industry change, the stepped approach would alleviate the impact of the entire proposal for industry.

Option 3: Simultaneous approach

Option 3 is to introduce prudential requirements on the qualitative management of operational risk, including requirements on information security, business continuity and outsourcing. This would entail implementing the full suite of requirements at one time which is likely to be more resource intensive for industry relative to option 2.

Entities would be required to comply with the prudential requirements by 1 January 2020. However, this longer timeframe could leave industry vulnerable to operational risk incidents for an extended period of time that may be mitigated through faster implementation as proposed under option 2.

APRA's preferred approach is option 2; the stepped approach. Implementation of the full proposal in two stages allows industry to focus attention on information security, which is considered by APRA to be an area of industry weakness.