REGULATION IMPACT ANALYSIS — Operational risk: Information Security

(OBPR ID: 23025)

Background

APRA's development of its revised prudential framework for operational risk, covering information security risk, involved an equivalent process and analysis to that required for a Regulation Impact Statement (RIS) as set out in *The Australian Government Guide to Regulation* (the Guide).[1] Using this process, APRA has answered the seven RIS questions set out in the Guide, details of which are summarised below.

Questions 1 and 2 — Assessing the problem and objectives of government action

APRA's current prudential framework includes prudential standards for all APRA-regulated entities covering business continuity and outsourcing, and guidance covering the management of information security risks. At present, there are no prudential standards on operational risk more broadly nor information security in particular.

In a March 2018 discussion paper, *Information security management: A new cross-industry prudential standard* (March 2018 discussion paper),[2] APRA outlined the problem in relation to the need for prudential requirements on information security. In particular, the problem arising stems from:

- the rapidly evolving nature of information security threats and vulnerabilities;
- the need to outline minimum requirements for the management of information security across an entity;
- an entity's exposure to the risk of information security incidents across its extended business environment (including those managed by third parties); and
- cyber security surveys conducted by APRA in conjunction with supervisory activities which have revealed weaknesses in industry's information security management practices.

APRA is proposing to prioritise a new prudential standard on information security, *Prudential Standard CPS 234 Information Security* (CPS 234), which includes new information security requirements as well as moving existing guidance on information security into the proposed new prudential standard.

The objectives of government action include to:

- ensure APRA's prudential framework remains responsive to current thinking on measures to address information security threats and vulnerabilities and operational risks that are rapidly evolving and growing in prevalence;

---

[1] *Australian Government Guide to Regulation*, March 2014.

[2] Refer to: https://www.apra.gov.au/information-security-requirements-all-apra-regulated-entities.

- increase the resilience of the Australian financial sector through strengthening management practices for information security and operational risks; and
- ensure consistency of practices across all APRA-regulated entities.

Question 3 and 4 — Options to achieve objectives and impact analysis

The March 2018 discussion paper identified three options for changes to the prudential framework in relation to information security management, as outlined in the following table.

Options	Approach
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 institution.
Option 3: Simultaneous approach	Introduce new prudential standards on operational risk management, and information security, and revise prudential standards on business continuity and outsourcing.

Option 1: Status quo

Under this option, 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 have 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 have 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

This option prioritises information security, being a current heightened area of risk, and introduces 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 to beneficiaries and other customers.

APRA would subsequently introduce prudential requirements on the qualitative management of operational risk more broadly as well as updated requirements on business continuity and outsourcing (as set out in 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

Under this option, APRA would introduce prudential requirements at the same time on the qualitative management of operational risk, information security, business continuity and outsourcing. As this would entail implementing the full suite of requirements at the same time it is likely to be more resource intensive for industry relative to option 2.

Entities would likely be required to comply with the prudential requirements in 2020/21. 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.

Question 5 — Consultation

In March 2018, APRA undertook a three-month consultation on a proposed new *Prudential Standard CPS 234 Information Security* (CPS 234). APRA received 39 submissions from a range of interested parties, including industry bodies, 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 on 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 aspects of the prudential standard. The key changes include:

- providing a transition period for entities to meet the requirements in CPS 234 in relation to information assets managed by third parties;

- increasing the time for entities to report to APRA in relation to information security incidents and information security control weaknesses to allow time for assessment and formulation of an approach to rectification; and

- providing clarification on various aspects, including the importance of the classification of information security assets by criticality and sensitivity.

APRA will release a Response to Submissions paper outlining APRA's response to comments received by industry. In addition, APRA intends to shortly undertake 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* (May 2013). Subsequently, APRA anticipates consulting on new and revised requirements and associated guidance on operational risk, outsourcing and business continuity management. This process is expected to extend over a period through to 2020.

Question 6 — What is the appropriate option

Option 1: Status quo

Under this option, there would be no new standard on operational risk 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 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, 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

Question 7 – Implementation and review

APRA expects to release the final information security requirements before the end of 2018, with effect from 1 July 2019. One exception is that APRA is proposing a transition period where an APRA-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.