Regulation Impact Statement

Harmonising cross-industry risk management requirements

(OBPR ID: 2013/ 15337)

Background

This Regulation Impact Statement (RIS) addresses the Australian Prudential Regulation Authority's (APRA's) proposal to harmonise and enhance cross-industry risk management requirements and apply consistent standards to all authorised deposit-taking institutions (ADIs), general insurers and life insurers (insurers) and APRA-regulated groups.

APRA's mandate is to ensure the safety and soundness of APRA-regulated institutions so that they can in all reasonable circumstances meet their financial promises to depositors, policyholders and fund members within a stable, efficient and competitive financial system. APRA carries out this mandate through a multi-layered prudential framework that encompasses licensing and supervision of institutions. APRA is empowered under the *Banking Act 1959* (the Banking Act), the *Insurance Act 1973* (the Insurance Act) and the *Life Insurance Act 1995* (the Life Insurance Act) to issue legally binding prudential standards that set out specific requirements with which ADIs and insurers must comply. APRA also publishes prudential practice guides (PPGs), which clarify APRA's expectations with regard to prudential matters.

APRA currently supervises ADIs and insurers at two 'levels':

- Level 1 – an individual ADI or insurer
- Level 2 – a group of related ADIs or a group of related general insurers

APRA's supervision of conglomerate groups (Level 3) will extend supervision of ADIs and insurers at another 'level'. A Level 3 group is a conglomerate group that performs material activities across more than one APRA-regulated industry and/or in one or more non-APRA-regulated industries.

Key elements of APRA's current and proposed risk management requirements are based on risk management principles developed by the Financial Stability Board, the

Basel Committee on Banking Supervision and the International Association of Insurance Supervisors. APRA is a member of the latter two bodies.

Problem

The main issues with APRA's current risk management requirements are that:

- similar risks are treated in different ways depending on whether the institution is an ADI or insurer;
- the current prudential standards do not reflect recent improvements in local and global risk management practices; and
- there are two currently near-identical risk management standards for life insurers and general insurers. The equivalent of the ADI risk management standard is currently separated into a number of other ADI prudential standards. There is no consolidated group risk management standard. Absent harmonisation, APRA and industry could end up with four near-identical standards, when one cross-industry standard would be more efficient for all concerned.

The industry-specific insurance and ADI standards have been issued at different times, reflecting different stages of development of APRA's regulatory requirements for each industry. Although APRA's risk management requirements are aligned in principle, there is sufficient difference in form to create additional complexity and compliance costs. Differences between industries include, but are not limited to:

- the content of formal Board attestations regarding compliance with prudential obligations;
- the criteria for institutions to comply with risk management requirements on a group basis;
- the definition of material risks;
- a requirement for insurers but not ADIs to have a risk management strategy; and
- APRA notification requirements.

In addition, the global financial crisis exposed serious and sometimes fatal shortcomings in the governance and risk management of offshore banks and insurance companies. [1] Although the most extreme problems were associated with global financial institutions, the emergence of better practice is relevant for all Australian ADIs and insurers. Implementation of best practice will strengthen risk management at ADIs and insurers, thereby enhancing their ability to cope with stress and crisis situations.

[1] Notable writings on these shortcomings and identified best practice include the 2009 Walker report (*A Review of Corporate Governance in UK Banks and other Financial Industry Entities*), the Basel Committee's *Principles for Enhancing Corporate Governance* (2010), the Institute of International Finance's *Governance for Strengthened Risk Management* (2012), and the Financial Stability Board's *Thematic Review on Risk Governance* (2013).

The problem with maintaining the status quo is that some ADIs and insurers may choose to avoid adopting better practice, placing Australian depositors, policyholders and other stakeholders at unnecessary risk. Risk management practices are not necessarily transparent to stakeholders, so market discipline may only take effect via disruptive failures of institutions. Institutions are already largely following the proposed requirements but there are a number of institutions that need to improve their risk management practices. APRA's proposals in effect acknowledge the work already undertaken by industry, and raise minimum standards to ensure institutions that are lagging do not undermine the confidence in, and stability of, the Australian financial system.

Harmonisation

Since its establishment as an integrated prudential regulator in 1998, where appropriate APRA has sought to take a consistent, harmonised approach to the setting of prudential requirements for APRA-regulated institutions, irrespective of the industry in which the institutions operate. In this way, similar risks are treated in a similar manner. Harmonisation also creates a common language and simplifies compliance, particularly for groups that operate across more than one regulated industry. APRA has already introduced cross-industry prudential standards addressing governance, fit and proper, outsourcing, and business continuity management. APRA intends to add risk management to this list of cross-industry behavioural standards.

The main proposed changes to harmonise APRA's various risk management requirements include:

- the extension of the minimum risk management framework requirements for insurers to ADIs. These minimum requirements include that ADIs and insurers must create and maintain:
    - a risk appetite statement;
    - a risk management strategy;
    - a business plan;
    - a designated risk management function;
    - processes for reviewing the appropriateness, effectiveness and adequacy of the risk management framework; and
    - an annual and a three-year comprehensive review of the risk management framework;
- refining the definition of material risks to ensure applicability and consistency for ADIs and insurers; and
- the alignment of annual risk management declaration requirements, which currently differ between industries.

ADIs largely meet these requirements in substance as part of their existing risk management practices. For example, the proposed new requirement for ADIs to have

a risk management strategy is substantively aligned with the detailed descriptions of risk management systems required under *Prudential Standard APS 310 Audit and Related Matters*. APRA anticipates that these new requirements will not be onerous and will simply confirm accepted industry good practice. Therefore, the incremental benefit of this harmonisation is to reduce complexity and increase compliance, both resulting in lower costs to industry.

Enhancement

APRA proposes a number of enhancements to existing risk management requirements to reflect and make more explicit its heightened expectations in this area. In some respects, the enhancements will underpin the improvements that have been made in risk management practices in response to lessons learned from the global financial crisis.

The most important of APRA's proposed risk management enhancements are:

- the requirement that ADIs and insurers have a Board Risk Committee (BRC) that provides the Board with objective non-executive oversight of the implementation and on-going operation of the institution's risk management framework; and

- the requirement that institutions designate a person responsible for the risk management function who is involved in, and provides effective challenge to, activities and decisions that may materially affect the risk profile of the institution. For simplicity, the designated person responsible for the risk management function will be referred to as a Chief Risk Officer (CRO) in the rest of the RIS.

The basis for these proposed enhancements is to ensure there is sufficient independent oversight and management of the risk management framework, such that:

- the risk management function, headed by a designated CRO, provides effective challenge to activities and decisions that materially affect the ADI's or insurer's risk profile. The crisis abroad highlighted that there was insufficient consideration and effective challenge to the risks posed by products, business lines, and mergers and acquisitions;

- the risk management function assists the development and maintenance of the institution's risk management framework; and

- independent reporting lines appropriately escalate issues identified across the institution. The crisis highlighted instances where material risk issues were not appropriately escalated and dealt with.

APRA's requirement is that the Board of an ADI or insurer is ultimately responsible for the risk management framework of that institution. The purpose of having a BRC that is separate from the Board Audit Committee (BAC) is to ensure an appropriate level of focus on risk management. The BRC should have responsibility for oversight of the implementation of the risk management framework and advising the Board on the overall risk appetite and risk management strategy. The Board may not get this

view from the BAC which is required to look at assurance issues. Over time, many institutions have expanded the role of the BAC to effectively 'dual-hat' with the responsibilities of the BRC. Audit committees bear a heavy load in the demanding part of their role in respect to financial reporting and internal control. Where the BAC and BRC are combined, meeting priorities may result in audit issues crowding out risk management issues, or vice-versa. Further, a significant conflict of interest arises when the BAC has the same responsibilities as the BRC. In effect, the BAC would effectively be overseeing its own implementation of the risk management framework. Clear delineation of responsibilities assists the Board in overseeing the appropriateness and effectiveness of the risk management framework, rather than just check-box compliance.

Having a designated CRO that reports to the Chief Executive Officer (CEO) will elevate his or her authority within an ADI or insurer, reflect the importance of sound risk management, and facilitate candour on escalating risk management issues. The requirement for a designated CRO would ensure that there is a person who is responsible for the risk management function with sufficient skills and expertise on risk issues. Where a CRO engages in dual-hatting, a problem can occur where that person may not have sufficient time or focus to manage the risk management function or address risk management issues. Further, separation of the CEO/CRO roles and responsibilities may allow the CRO to prompt the CEO on issues or alternative actions one person may not have considered in their risk search.

APRA expects a CEO and senior executive management to always consider the impact of actions and decisions on the risk profile of the institution, and believes that the CRO would be best placed to provide such information. The CRO must also have unfettered access to the BRC. Further, the importance and the independence of the CRO should result in the Board approving his or her appointment and removal, in addition to the BRC reviewing the performance of the CRO. In some institutions, business units have been resistant to a CRO who is seen as getting in the way of their ability to undertake what they see as attractive business. APRA's proposals seek to change any residual attitudes of this kind and put beyond doubt the independent authority of the CRO in implementing the risk management framework.

Under the proposed APRA standard, a CRO may have other roles and responsibilities that do not pose a conflict of interest. That is, a regulated entity may appoint a 'designated' rather than a 'dedicated' CRO. A designated CRO is important to represent an ADI's or insurer's risk management function, and to have a comprehensive institution-wide view of all material risks, including an understanding of how risks interact to change the risk profile of the institution. Without a designated representative, the risk management function may lack the stature and authority to challenge risky business decisions. APRA's view is that a designated CRO with business line responsibilities would be subject to a conflict of interest if he or she were to oversee and challenge their own proposals and decisions.

Larger and more complex ADIs and insurers largely meet these enhancements, in substance, as part of their existing risk management practices. For the smaller and less complex institutions, APRA anticipates that these new requirements will not be onerous for the majority of them as the requirements confirm accepted industry good practice. However, there are institutions that are lagging behind industry best practice and will face a range of costs, depending on how far behind their risk management

practices are. These institutions are of sufficient size and complexity for enhancements, such as a designated CRO, to be considered a necessary element of their risk management framework. The costs faced by lagging institutions will vary but are considered necessary as these institutions have a potential medium impact on the market in the event of failure. A failure may give rise to broader economic issues given risk management practices are not transparent to stakeholders and could undermine confidence in the practices of other institutions. The global financial crisis demonstrated that where an institution fails, investors and other stakeholders are likely to withdraw support (asset and funding) for other institutions of similar size, business mix and complexity. Without requirements for enhanced risk management practices, there is no way for medium-sized institutions that meet best practice to differentiate themselves from those who do not. Market fear ultimately leads to these institutions that meet best practice being tarnished with the same brush as those who fail. Accordingly, APRA view is that the aggregate incremental benefit to confidence and stability in industry exceeds the aggregate incremental cost for those lagging behind.

Objectives

APRA's primary objective for these proposals is to harmonise and enhance risk management requirements to ensure that:

- similar risks are treated in a similar way, irrespective of whether the institution is an ADI or insurer, or stand-alone or part of a group;

- a common language is created and compliance with risk management requirements is simplified, particularly for groups that operate across regulated industries; and

- ADIs and insurers have sound risk management frameworks that reflect domestic and international best practice, ultimately to strengthen the interests of stakeholders and enhance the protection afforded to Australian depositors and/or policyholders.

Options and impact analysis

This RIS addresses two issues:

(a) Should APRA continue with multiple risk management standards across the three relevant industries and for groups, or consolidate these potential four standards into one cross-industry standard?

(b) Should APRA also take the opportunity to enhance the cross-industry requirements for effective risk management?

APRA has already demonstrated that the cross-industry approach to behavioural prudential standards works well, with four previous successful initiatives in this area. Relative to multiple industry standards, both industry and APRA can operate somewhat more effectively, and with slightly lower costs, with a single cross-industry standard.

The cost and benefit implications for APRA's intended enhancements to the industry require more substantial consideration.

APRA has identified three options to enhance its current risk management framework and address the identified deficiencies in risk management for ADIs and insurers that lag current industry best practice:

- Option 1 - status quo: maintain APRA's existing prudential framework, with multiple and unchanged industry standards for risk management;

- Option 2 - voluntary adoption: outline APRA's expectations for an independent CRO and a separate BAC and BRC, such as through a new PPG, which would not create enforceable obligations for ADIs and insurers or ensure harmonisation across industries; or

- Option 3 - prudential standard implementation: implement the proposed risk management standard and updated governance standard, harmonising requirements for ADIs and insurers, and requiring ADIs and insurers to have an independent CRO, and separate BAC and BRC.

Option 1 — Status quo

Under this option, the existing risk management requirements will remain across a number of prudential standards. This would mean that ADIs and insurers would continue to apply different risk management practices.

Benefits

The primary benefit of this option is that it would impose no new requirements on ADIs or insurers. This would introduce no new immediate costs to those institutions that are lagging behind industry risk management best practice. Maintaining the status quo would allow Boards flexibility in determining whether the institution needs a designated CRO and/or separate Board Committees. This gives the Board flexibility to choose whether to delay or not implement best practice, balancing short-term performance at the detriment of prudence.

Costs

Maintaining different regulatory requirements adds to complexity and the cost of compliance, particularly for groups that operate across regulated industries. Further, it would mean that APRA's set of prudential requirements for institutions differ slightly depending on whether the institution is an ADI or insurer. APRA's industry-specific prudential standards reflect the differences in the risks faced by ADIs and insurers, and will remain separate. However, where these institutions face common risks, these requirements should be integrated in cross-industry prudential standards. Maintaining the status quo would effectively mean that similar risks to both ADIs and insurers are not treated in a similar matter.

The major costs to the do-nothing option include:

(i) the BAC will continue as a potentially less effective tool for risk management;

(ii) ADI risk management requirements will be scattered through several prudential standards, rather than centralised and harmonised in one standard. This creates operating inefficiencies and may result in less effective supervision and risk management; and

(iii) ADIs and insurers currently operating without designated CROs may suffer from failure to implement this good practice in strategic risk management.

Maintaining the status quo risks Boards not having sufficient oversight of the breadth of risk management practices, culture and issues within their institution. Further, without a designated CRO with sufficient stature and authority operating within the organisation on a day-to-day basis, there is a danger of risk issues being effectively side-lined away from the decision-making process. Further, the information provided to a Board for decision-making is substantially derived from executive management who, without appropriate independent risk views, may not integrate the level of risk involved.

Some submissions received viewed the CRO and BRC requirements to be prescriptive in nature, limiting ADIs' and insurers' ability to structure their risk management frameworks as they see fit. APRA notes that industry has largely already established these requirements as best practice and that the proposed requirements are merely enshrining this practice. APRA's view is that where best practice has been established, recognised and adopted by industry, there is a clear minimum prudential benchmark for institutions. There is no point in APRA's prudential requirements being less clear, when its view of the benchmark is clear.

As the memories of the global financial crisis fade over time, there is a danger that the enhancement of ADI and insurer capabilities in risk management may receive less management attention. This is because the benefits of enhanced risk management may only be realised over the long-term, while the costs of enhancing risk management are immediate. Further, APRA's risk management requirements would not reflect industry best practice, and may result in institutions that equate box-ticking compliance with risk management being further distanced from best practice.

Option 2 — Voluntary adoption

Under this option, the enhanced risk management requirements would be introduced to ADIs and insurers on a voluntary basis, e.g. through a new PPG. This would provide guidance but not legally enforceable obligations for ADIs and insurers to have an independent CRO and a separate BAC and BRC. Given this guidance is already provided by a range of industry bodies and other regulatory authorities, and these practices still have not been adopted, the costs and benefits of voluntary adoption largely mirror that of the status quo.

Benefits

The key benefit would be APRA's *expectations* for risk management being clear whilst maintaining the Board's flexibility in determining whether the institution needs an independent CRO and/or separate Board Committees. Additional costs that ADIs and insurers would face depend on their voluntary adoption choices and the size,

business mix and complexity of the institution. Further, the range of costs depends on how much the institution lags in regards to risk management best practice.

Costs

Voluntary adoption is expected to result in a variety of risk management practices and could result in uncertainty about quality of risk management in ADIs and insurers, given risk management practices are not transparent to the institution's external stakeholders. Further, ADIs and insurers that choose not to adopt these practices may not have an ability to properly understand, measure, manage, price and mitigate risk. This results in a lower quality of risk-based decision-making and, ultimately, leads to long-term underperformance or failure. APRA considers that the institutions most in need of enhanced risk management are also the institutions least likely to engage in voluntary adoption of these good practices.

APRA guidance is regularly misinterpreted as having the enforceability of prudential requirements. When coupled with the lack of transparency of risk management practices for stakeholders, this may provide these stakeholders with a false sense of security that all ADIs and insurers are following the practices outlined in guidance. There is a risk that stakeholders are subject to information asymmetries about the risk management practices of institutions, resulting in adverse selection where short-term performance is at the detriment to prudence.

Option 3 — Implementation through prudential standards

Under this option, a new *Prudential Standard CPS 220 Risk Management* (CPS 220) and updated *Prudential Standard CPS 510 Governance* (CPS 510) would commence from 1 January 2015.[2]

Costs

APRA specifically sought assessments of the compliance impact of the proposed changes as part of its consultation on the proposals.

No submission identified costs with the harmonisation of ADI and insurer risk management requirements. APRA expects any costs associated with harmonisation will be negligible given most ADIs and insurers are already meeting in substance the proposed CPS 220.

One submission quantified the cost of a separate BAC and BRC as $16,000 per annum, while other submissions highlighted that separation could involve administrative costs. This institution identified that their current BAC is already providing governance to the risk management function. Accordingly, APRA's view is that this indicated cost reflects its current cost of running meetings, rather than an incremental compliance cost of separating the BAC and BRC. Thus, APRA has not applied the estimated $16,000 cost across industry.

[2] The consultation package proposed a commencement date of 1 January 2014. On 14 August 2013, APRA proposed to delay the commencement to 1 January 2015 to provide industry with sufficient time to comply fully with the proposed enhancements.

In considering implementation costs, APRA can identify three potential requirements that may lead to one-off and/or ongoing costs.

(i) ADIs will need to ensure that they meet the documentation requirements under the new consolidated standard. These requirements include maintaining a risk management strategy, a risk appetite statement and a business plan. APRA notes that insurers already operate under this documentation regime, so would have no additional costs. ADIs must already operate an effective risk management regime, including effective documentation. APRA's documentation requirements standardise what are already industry-accepted good practices. Therefore, APRA considers that the conversion and ongoing costs of adopting standard risk management documentation practices are negligible relative to good industry practice, and near-zero for the current ADI industry;

(ii) APRA has explicitly provided that the new BRC may comprise, in its entirety, the current BAC. APRA's expectation is that larger and more complicated institutions will adopt separate board committees, and many have already done so of their own accord. Smaller entities will often choose to continue with a combined subcommittee, so any incremental costs will be negligible and zero in most cases. In summary, any increased costs arising from the BRC requirement will come from entities incurring these costs as a business decision, not as an APRA requirement; and

(iii) institutions lacking a designated CRO will need to create this position, in some cases by formally designating persons who currently perform the function informally, in some cases by allocating the time of a current employee away from other functions in favour of risk management, and in some cases by creating and staffing a new position, either from an internal transfer (with associated training) or an external hire. The first of these practices creates no new costs; the other two practices may create material costs.

Submissions received quantified the cost of a dedicated full-time CRO for smaller and less complex ADIs and insurers to be $50,000-$300,000 per annum. One submission identified that the cost of a CRO for a larger and more complex institution may reach $2 million. APRA notes, however, that nearly every large entity already employs such a person or persons. The CRO position is established industry practice for large and many medium-sized institutions.

At the other end of the scale, APRA supervises a number of very small institutions, which lack multiple management layers and may only employ a few professional staff. The proposed prudential standard will allow these entities to designate a dual-hatted CRO, ensuring that the function is covered without the need to add people.

The incremental cost of the CRO requirement is therefore likely to fall upon an unknown number of medium-sized institutions that are big enough to need a CRO, but for some reason have yet to create this role. APRA's view is that medium-sized institutions already have personnel who have, or are close to possessing, the necessary skills to be responsible for the risk management function. The $300,000 per annum figure is considered to be a maximum cost of hiring a new full time 'dedicated' employee rather than promoting existing risk management personnel. As APRA is not requiring a 'dedicated' CRO but rather a 'designated' CRO, APRA assumes a

conservative *incremental* cost estimate of a person becoming responsible for of the risk management function would be $100,000 per annum. This cost would reflect any potential additional salary adjustment to existing personnel to reflect the importance of the role.

No submission identified specific start-up costs; however, APRA has assumed that existing personnel at these medium-sized institutions would require some training to head the risk management function and be aware of their prudential responsibilities. Accordingly, APRA has assumed the *incremental* cost of training would, on average, be $500 per annum. This assumption is based on a sample of development courses on financial risk management offered by industry associations and professional education providers. The amount of this expenditure depends on the skills of existing personnel and the size, business mix and complexity of the institution. However, training is considered to be a long-term investment to enhance the skills and expertise of existing staff.

APRA's view is that its pragmatic approach will enable aggregate compliance costs for ADIs and insurers under this option to be minor. As no submission quantified the number of smaller and less complex institutions that will seek alternative arrangements, APRA has assessed the aggregate compliance cost to industry on a best endeavours basis.

There are 356 ADIs and insurers subject to the proposed prudential standard. APRA considers that CRO practices will be sized based:

- the 77 institutions holding more than $5 billion in assets are all assumed to already employ a CRO, or a person or persons fulfilling that function. Any incremental costs for this group will be nominal;

- the 163 institutions holding less than $500 million in assets are assumed to meet the CRO requirements, with APRA's approval, by redeploying their current risk management staff;

- of the remaining 116 institutions with assets from $500 million to $5 billion, APRA's supervisory understanding is that approximately half these institutions already deploy resources at least equivalent to the proposed risk management standards, though in many cases the new standard will require more formalisation of the CRO arrangements;

- this leaves approximately 58 entities that may need to spend material amounts to create a CRO role. Based on submissions, APRA assumes that the cost of this role will amount to $100,000 per institution, resulting in an annual cost across all three relevant industries of $5.8 million. APRA's view is that $100,000 per annum is a very conservative estimate of the incremental costs of compliance for a head of the risk management function as it need not be a dedicated resource and it need not be called a CRO.

Benefits

The benefit of harmonising risk management requirements is to reduce complexity and associated compliance costs by requiring standardised risk documentation,

particularly for ADIs. Harmonisation will result in similar risks being treated in similar ways, whether the institution is an ADI or insurer. Further, this will provide a foundation for sound risk management frameworks and principles that support a level playing field between ADIs and insurers. The alignment across industries enhances the consistency of risk management, particularly for groups that operate in both industries. There is an incremental benefit of homogeneity across industries that leads to a reduction in complexity and increase in compliance, both resulting in lower costs to industry. APRA recognises that homogeneity should only be done where appropriate, namely where there are shared principles and practices across industries. These are usually associated with governance of certain activities and ensuring appropriate due diligence supporting decision-making. APRA maintains industry-specific standards that address risks that are primarily associated with banking or insurance. These standards fall within the overarching cross-industry standards that address principles of governance. From a quantitative perspective, the benefits of harmonisation are small. Therefore, APRA has not estimated the dollar value.

The benefits of enhancing risk management requirements are that all ADIs and insurers will enjoy better risk governance, both at the management and board levels. This means that unexpected losses to shareholders and other stakeholders will reduce. More relevantly for APRA, the failure rate of APRA-regulated institutions will fall over time, as the internal lines of defence against overly aggressive management become stronger. This collective improvement in industry risk management and governance means that systemic risk is likely to fall, because there is an accepted collective approach to good risk management practices.

Specifically, the primary benefit of a designated and independent CRO is to ensure ADIs and insurers have a risk management function with sufficient stature, authority and resourcing to support sound risk-based decision-making. APRA proposes that the risk management function needs to be led by a designated CRO who is appropriately skilled, unencumbered by conflicts of interest with their risk management role, and can speak with candour to the CEO, the Board and relevant committees. APRA considers the CRO to be clearly conflicted if he or she were to dual-hat with business lines or assurance roles and responsibilities. APRA proposes to prohibit the CRO from being also the CEO, the CFO, the Appointed Actuary, and the Head of Internal Audit. The CRO is a key element in developing and maintaining a sound risk management culture, as his or her stature and authority enhances the importance of risk management in an organisation.

APRA expects institutions that currently have a risk management function without an appropriate head, to provide training for a person to ensure they have the skills and expertise to head the function. Where a head exists, the Board of that institution would consider the level of influence he or she has within the organisation.

It is important that the CRO can provide objective and effective challenge to actions and decisions that may have a material impact on the risk profile of an ADI or insurer, to support sound risk-based decision-making. APRA's proposals intend the CRO to be engaged with business units, reinforcing the value of risk-based decision-making and minimising the potential for resistance from business units which see the CRO as a barrier to undertaking what they see as attractive business. The required level of involvement and effective challenge provided by the CRO will overcome the risk that the CRO is sidelined in the decision-making process. The stature and authority of the

CRO, supported by the BRC, ensures that he or she has a seat at the senior executive table when discussing the risks associated with business decisions. This seat at the table supports the CRO having sufficiently detailed involvement in day-to-day management of the institution's affairs and supports information flows to the CRO. Access to information is enshrined in the CRO's authority as they are also a conveyor of risk information from and to the Board. The requirements for a CRO simply enshrine best practice, and ensure that the Board has sufficient oversight and influence on the risk management. Enhanced risk governance is of paramount importance to the stability and profitability of institutions. This benefit is particularly acute for a small number of institutions that are currently large enough to have this functionality, but do not currently deploy it.

The benefit of a separate BAC and BRC is that each has a clearer focus on fulfilling its responsibilities. The BAC is responsible for oversight of the independent assurance provided by internal and external auditors. In contrast, the BRC is responsible for oversight of the implementation of the risk management framework. APRA's experience is that where ADIs and insurers have a separate BAC and BRC, both audit and risk management issues are subject to greater Board oversight. Enhanced focus results from Boards being able to allocate sufficient time to consider audit and risk management issues, rather than audit issues potentially crowding out risk management issues, or vice-versa. Further, the non-executive membership of the BRC allows it to maintain objective oversight of the risk management function, given the inherent conflict of interest that arises from executive directors effectively overseeing their own proposals and decisions.

The BRC's role in advising the Board on the institution's current and future risk appetite and risk management strategy will allow members of the Board to have a greater level of engagement and interaction with executive management, before the decision is presented to the whole Board. This interaction in the lead-up to the full Board decision will grant the non-executive directors sufficient time and knowledge of material proposals, such as mergers and acquisitions, to support risk-based decision-making. The BRC also provides a regular audience for risk management matters to be communicated to directors, and a forum for the Board to challenge senior management's proposals and decisions and have a holistic view of risks across the organisation. This is supported by the three-year comprehensive review that identifies how the risk management framework is operating, and includes recommendations on enhancing risk management practices. The provision of this review by an independent third party allows the Board to have an objective view of the institution, enhancing its engagement in overseeing the appropriateness of managerial actions and decisions. The crisis highlighted that enhancing Board engagement and oversight of risk management can assist in ensuring performance is not at the detriment of prudence.

The Board's oversight of the appointment, dismissal, performance and objectives of the CRO empowers the CRO to raise risk issues with candour, given they are ultimately responsible to the Board. These structural requirements would deal with the risk of the CRO becoming subservient to a dominant CEO, remuneration practices or other group behavioural pathologies. Further, APRA proposes to require the CRO to be invited to all relevant sections of BRC meetings. This supports the opportunity for the BRC members to meet with the CRO individually, away from the influence of the

CEO, to support candour. APRA's guidance will identify that regular meetings with the chairperson of the BRC reflects the normalisation and importance of risk in decision-making. It is important to note that the BRC's role is oversight of the implementation whilst the CRO's role is day-to-day implementation of the risk management framework. This distinction ensures that the Board remains focused on the strategic side of risk management and is not caught up with the day-to-day practices.

This proposal has been assessed by the OBPR as likely to be relatively less significant, and therefore has assigned it a D rating (on a scale of A to D, with 'D' being the lowest impact).

Consultation

APRA has specifically consulted on option 3. This policy development and consultation process complied with the then applicable OBPR requirements.

In May 2013, APRA released a discussion paper, *Harmonising cross-industry risk management requirements*. It was accompanied by draft prudential standards relating to these components.

In its August 2013 letter to all ADIs, general and life insurers and Level 2 Heads, APRA confirmed that, in response to industry requests, it proposed to move the implementation date of CPS 220 to 1 January 2015.

Submissions received

APRA received 44 formal submissions following the release of the May 2013 discussion paper from a wide range of stakeholders including ADIs and insurers, industry bodies and professional bodies. In addition to written submissions, APRA has received feedback via industry workshops and meetings with institutions and other stakeholders. Submissions broadly supported the introduction of CPS 220.

The main concerns submissions raised were:

- resourcing constraints faced by smaller ADIs and insurers if they are required to have a dedicated CRO, although submissions generally supported the principle of the CRO;

- the separation of the BAC and the BRC appeared to reflect form over substance, although submissions agreed that there should be a Board Committee that has the responsibilities of the BRC; and

- the applicability of CPS 220 on Australian branch operations of foreign institutions, although submissions agreed that branch operations should, in principle, meet CPS 220.

APRA has considered these views and made the following refinements to the proposals:

- some submissions incorrectly interpreted that APRA was requiring a dedicated person to head the risk management function and for that role to be called the CRO. CPS 220 has been clarified to ensure the reader interprets this requirement as a dedicated person heading the risk management function;

- CPS 220 now clearly identifies that APRA may approve alternative arrangements for an ADI and insurer to have a dual-hatting CRO if, in APRA's opinion, these will achieve the objectives of this standard. Further, APRA has reiterated in the response paper and draft PPG that it expects alternative arrangements that may be appropriate to smaller and less complex institutions;

- the response paper and draft PPG clearly outline APRA's intent of a separate BAC and BRC, which includes guidance on the composition and focus of responsibilities, and clarifies that the BAC and BRC may be made up of the same directors;

- CPS 220 now clearly identifies that a reference to a Board is equivalent to a reference to a senior officer outside of Australia or Compliance Committee (as applicable). This considerably reduces incremental costs that might otherwise apply to some branches. Further, the response paper and draft PPG outline APRA's expectations for Australian branch operations, identifies instances where APRA expects branch operations would seek alternative arrangements.

In addition, submissions sought additional guidance on APRA's expectations for compliance with CPS 220. The main clarifications will be incorporated in a draft *Prudential Practice Guide CPG 220 Risk Management* (CPG 220). Draft CPG 220 will be released together with the response paper and outline a number of clarifications on good risk management and risk governance practices.

Compliance with Best Practice Regulation Handbook

As consultation for these proposals commenced before the implementation of the revised Best Practice Regulation Handbook (which began on 8 July 2013), APRA has opted to complete a single-stage RIS. APRA has endeavoured to address the OBPR's feedback on an earlier version of this RIS. APRA has undertaken best endeavours to meet the OBPR's requirement to include detailed compliance costs and compliance cost offsets via the business cost calculator (BCC) and Regulatory Burden and Cost Offset Table. Of the 44 submissions received from industry, only one estimated costs via the BCC. This submission was from a small regulated institution which assumed a CRO had to be a dedicated resource and appeared not to have distinguished existing costs and incremental compliance costs with a separate BRC. As a result, this submission is not appropriate as a basis for estimated compliance costs for the rest of the industry. Overall, due to the lack of submissions containing the completed BCC, APRA has provided limited but conservative cost estimates via the BCC.

A final decision from the OBPR on whether this RIS complies with the Best Practice Regulation Handbook has not yet been taken on this matter.

Regulatory compliance cost offsets

A regulatory offset has been identified and agreed with by the OBPR from within the Treasury portfolio.

Conclusion and recommended option

APRA has harmonised and consolidated a number of its behavioural prudential standards relating to outsourcing, business continuity management, governance, and fitness and propriety. APRA proposes to continue this process of harmonisation with a consolidated risk management prudential standard – CPS 220. Following the finalisation of CPS 220, APRA will revoke two insurance prudential standards – *Prudential Standard GPS 220 Risk Management and Prudential Standard LPS 220 Risk Management* – and will revise a number of ADI prudential standards to remove any duplication or inconsistencies. The proposed harmonisation of risk management requirements will create a common language and also simplify compliance, particularly for groups that operate across regulated industries.

APRA considers the proposed enhancements to CPS 220 and CPS 510 as necessary to reflect and make more explicit its and industry's heightened standards in this area. These enhancements will strengthen APRA's existing risk management requirements and align them with current domestic and international best practice. The proposed requirements for a CRO and a BRC will enhance the stature and authority of risk management functions and will strengthen risk-based decision-making within ADIs and insurers.

Maintaining the status quo or duplicating industry guidance is not expected to result in industry laggards adopting risk management enhancements, given short-term performance may be at the detriment of prudence. Further, market discipline is not expected to be effective given the lack of transparency of risk management practices. The lack of transparency may result in overconfidence in the risk management of those institutions that are materially affected by the proposals.

APRA's view is that these risk management proposals will have a minor cost impact as industry has already substantially invested in risk management capacity, at both the management and Board levels. Further, APRA's principles-based application will accommodate alternative arrangements for ADIs and insurers according to their size, business mix and complexity. The institutions that are materially affected are the minority of industry that are of sufficient size to need these enhancements and have yet to implement them on their own accord. Therefore, it is recommended that APRA implement Option 3, i.e. implementation via prudential standard, from 1 January 2015.

Implementation and review

The harmonised and enhanced risk management requirements are proposed to commence on 1 January 2015. This proposed date provides industry with sufficient time to request, where appropriate, alternative arrangements from APRA before the standards commence.

APRA will release a final CPS 220 and CPS 510, accompanied by a response to submissions on the proposals, and consultation on CPG 220.

Attachment A: Business Cost Calculator report (variable ongoing cost by size of business)

Proposal name	Harmonising cross-industry risk management requirements
Reference number	2013/15337
Problem and objective	
Problem	

The main issues with APRA's current risk management requirements are that:
• similar risks are treated in different ways depending on whether the institution is an ADI or insurer;
• the current prudential standards do not reflect recent improvements in local and global risk management practices; and
• there are two currently near-identical risk management standards for life insurers and general insurers. The equivalent of the ADI risk management standard is currently separated into a number of other ADI prudential standards. There is no consolidated group risk management standard. Absent harmonisation, APRA and industry could end up with four near-identical standards, when one cross-industry standard would be more efficient for all concerned.

The industry-specific insurance and ADI standards have been issued at different times, reflecting different stages of development of APRA's regulatory requirements for each industry. Although APRA's risk management requirements are aligned in principle, there is sufficient difference in form that this creates additional complexity and compliance costs. Differences between industries include, but are not limited to:
• the content of formal Board attestations regarding compliance with prudential obligations;
• the criteria for institutions to comply with risk management requirements on a group basis;
• the definition of material risks;
• a requirement for insurers but not ADIs to have a risk management strategy; and
• APRA notification requirements.

In addition, the global financial crisis exposed serious and sometimes fatal shortcomings in the governance and risk management of offshore banks and insurance companies. Although the most extreme problems were associated with international financial institutions, the emergence of better practice is relevant for all Australian ADIs and insurers. Implementation of best practice will strengthen risk management at ADIs and insurers, thereby enhancing their ability to cope with stress and crisis situations.

The problem with maintaining the status quo is that some ADIs and insurers will choose to avoid adopting better practice, placing Australian depositors, policyholders, and other stakeholders at unnecessary risk. Risk management practices are not necessarily transparent to stakeholders, so market discipline may only take effect via disruptive failures of institutions. Institutions are already largely following the proposed requirements, but there are a few institutions that need to materially improve their risk management practices. Ultimately, APRA's proposals acknowledge the work already undertaken by industry, and raise minimum standards to ensure laggards do not undermine the confidence in, and stability of, Australia's financial institutions.

Objective	

APRA's primary objective of these proposals is to harmonise and enhance risk management requirements to ensure that:
• similar risks are treated in a similar way, irrespective of whether the institution is an ADI or insurer, or stand-alone or part of a group;
• a common language is created and compliance with risk management requirements is simplified, particularly for groups that operate across regulated industries; and
• ADIs and insurers have sound risk management frameworks reflect harmony in domestic and international best practice, ultimately to strengthen the interests of stakeholders and enhance the protection afforded to Australian depositors and/or policyholders.

Explanatory information

APRA's requirement is that the Board of an ADI or insurer is ultimately responsible for the risk management framework of that institution. The purpose of having a BRC that is separate from the Board Audit Committee (BAC) is to ensure an appropriate level of focus on risk management. Where the BAC and BRC are combined, meeting priorities may result in compliance or audit issues crowding out risk management issues, or vice versa. The BRC should have responsibility for oversight of the implementation of risk management framework and advising the Board on the overall risk appetite and risk management strategy. The Board may not get this view from the BAC which is required to look at compliance and assurance issues. Overtime, many institutions have expanded the role of the BAC to effectively "dual-hat" with the responsibilities of the BRC. Audit committees bear a heavy load in the demanding part of their role in respect to financial reporting and internal control. Where the BAC and BRC are combined, meeting priorities may result in compliance or audit issues crowding out risk management issues, or vice versa. In regards to composition of the BRC, a conflict of interest arises where executive Board members are effectively overseeing his or her own implementation of the risk management framework. Mirroring the existing BAC requirements, APRA proposes that membership of the BRC is limited to non-executive directors so that independent oversight can be maintained. The potential or actual overload of the BAC and the need for closely-related but separate capability to focus on risk in future strategy leads to the conclusion that best practice is for the establishment of a BAC and BRC. Clear delineation of responsibilities assists the Board in overseeing the appropriateness and effectiveness of the risk management framework, rather than just check-box compliance.

A designated CRO that reports to the Chief Executive Officer (CEO) elevates his or her authority within an ADI or insurer, reflects the importance of sound risk management, and facilitates candour on escalating risk management issues. A designated CRO would ensure that there is a person who is responsible for the risk management function with sufficient skills and expertise on risk issues. Where a CEO engages in dual-hatting with a CRO, the problem can occur where that person may not have sufficient time or focus to manage the risk management function or addressing risk management issues. Further, separation of the CEO/CRO roles and responsibilities may allow the CRO to prompt the CEO on issues or alternative actions one person may not have considered in their risk search.

APRA expects a CEO and senior executive management to always consider the impact of actions and decisions on the risk profile of the institution, and considers that the CRO would be best placed to provide such information. The CRO must become and remain a member of the senior executive management of the institution. The CRO should report to the BRC and have direct access to the chairperson of that committee to ensure that all risk views are considered, for instance, when a CRO has a different view than the CEO or Chief Financial Officer (CFO). Further, the importance and the independence of the CRO should result in the Board approving his or her appointment and removal, in addition to the BRC reviewing the performance of the CRO. Historically, business units have been resistant to a CRO who is seen as getting in the way of their ability to undertake what they see as attractive business. Any residual attitudes of this kind must be changed and the independent authority of the CRO put beyond doubt.

Under the proposed APRA standard, a CRO may have other roles and responsibilities that do not pose a conflict of interest. That is, a regulated entity may appoint a 'designated' rather than a 'dedicated' CRO. A designated CRO is important to represent an ADI's or insurer's risk management function, and to have a comprehensive institution-wide view of all material risks, including an understanding of how risks interact to change the risk profile of the institution. Without a designated representative, the risk management function may lack the stature and authority to challenge risky business decisions. APRA's view is that a designated CRO with business line responsibilities would be subject to a conflict of interest if he or she was to oversee and challenge their own proposals and decisions.
Larger and more complex ADIs and insurers largely meet these enhancements, in substance, as part of their existing risk management practices. Smaller and less complex institutions are APRA anticipates that these new requirements will not be onerous for the majority of institutions, simply confirming accepted industry good practice. However, there are a number of institutions (identified below) that are lagging behind industry best practice and will face a range of costs, depending on how far behind their risk management practices are. These institutions are of sufficient size and complexity for enhancements, such as a designated CRO, to be considered a necessary element of their risk management framework. The costs faced by lagging institutions will vary but are considered necessary, given these institutions have a potential medium impact on the market in the event of failure. The failure of one of these institutions may result in broader economic issues given risk management practices are not transparent to stakeholders, and would, at least, undermine confidence in the practices of other institutions. The aggregate benefit to confidence and stability in industry is considered to exceed the aggregate incremental cost for those lagging behind.

Option 1			
Option name			Maintain the status quo
Option description			

Under this option, the existing risk management requirements will remain across a number of prudential standards. This would mean that ADIs and insurers would continue to apply different risk management practices.

For more information on the costs and benefits of this option, please see the options and impact analysis above.

Businesses affected			0
Timeframe (years)			10
	Size of business	**Cost per business**	**Total cost for all businesses**
Start up cost	Small	0	0
	Medium	0	0
	Large	0	0
	All	0	0
Average ongoing compliance cost per year	Small	0	0
	Medium	0	0
	Large	0	0
	All	0	0

Option 2			
Option name			Voluntary adoption
Option description			

Under this option, the enhanced risk management requirements would be introduced to ADIs and insurers on a voluntary basis, e.g. through a new PPG. This would provide guidance but not legally enforceable obligations for ADIs and insurers to have an independent CRO and a separate BAC and BRC. Given this guidance is already provided by a range of industry bodies and other regulatory authorities, and these practices still have not been adopted, APRA envisages that the divergence between industry and those materially lagging will increase.

For more information on the costs and benefits of this option, please see the options and impact analysis above.

Businesses affected			0
Timeframe (years)			10
	Size of business	**Cost per business**	**Total cost for all businesses**
Start up cost	Small	0	0
	Medium	0	0
	Large	0	0
	All	0	0
Average ongoing compliance cost per year	Small	0	0
	Medium	0	0
	Large	0	0
	All	0	0

Option 3	
Option name	Implementation through prudential standards
Option description	

Under this option, a new Prudential Standard CPS 220 Risk Management (CPS 220) and updated Prudential Standard CPS 510 Governance (CPS 510) would commence from 1 January 2015.

The main proposed changes to harmonise APRA's various risk management requirements include:

• the extension of the minimum risk management framework requirements for insurers to ADIs. These minimum requirements include that ADIs and insurers must create and maintain:

o a risk appetite statement;

o a risk management strategy;

o a business plan;

o a designated risk management function; and

o processes for reviewing the appropriateness, effectiveness and adequacy of the risk management framework; and

o an annual and a three-year comprehensive review of the risk management framework;

• refining the definition of material risks to ensure applicability and consistency for ADIs and insurers; and

• the alignment of annual risk management declaration requirements, which currently differ between industries.

ADIs largely meet these requirements in substance as part of their existing risk management practices. For example, the proposed new requirement for ADIs to have a risk management strategy is substantively aligned with the detailed descriptions of risk management systems required under Prudential Standard APS 310 Audit and Related Matters. APRA anticipates that these new requirements will not be onerous and will simply confirm accepted industry good practice. Therefore, the incremental benefit of this harmonisation is to reduce complexity, increase compliance, both resulting in lower costs to industry.

APRA proposes a number of enhancements to existing risk management requirements to reflect and make more explicit heightened expectations. In some respects, the enhancements will underpin the improvements that have been made in risk management practices, locally and globally, in response to lessons learned from the global financial crisis.

The most important of APRA's proposed risk management enhancements are:

• the requirement that ADIs and insurers have a Board Risk Committee (BRC) that provides the Board with objective non-executive oversight of the implementation and on-going operation of the institution's risk management framework; and

• the requirement that institutions designate a Chief Risk Officer (CRO) who is involved in, and provides effective challenge to, activities and decisions that may materially affect the risk profile of the institution.

The basis for these proposed enhancements is to ensure there is sufficient independent oversight and management of the risk management framework, including:

• the risk management function, headed by a designated CRO, providing effective challenge to activities and decisions that materially affect the ADI's or insurer's risk profile. The crisis highlighted that there was insufficient consideration and effective challenge to the risks posed by products, business lines, and mergers and acquisitions;

• the risk management function assisting the development and maintenance of the institution's risk management framework; and

• having independent reporting lines to appropriately escalate issues identified across the institution. The crisis highlighted instances where material risk issues were not appropriately escalated and dealt with.

Businesses affected			58 (Small = 0, Medium = 58 and Large = 0)
Timeframe (years)			10
	Size of business	**Cost per business**	**Total cost for all businesses**
Average training cost per year	Small	0	0
	Medium	$500	$29,000
	Large	0	0
	All	$500	$29,000
Average ongoing compliance cost per year	Small	0	0
	Medium	$100,000	$5,800,000
	Large	0	0
	All	$100,000	$5,800,000

Note: An assessment of compliance costs in itself do not provide an answer to the most effective and efficient regulatory proposal.

Rather, it provides information that needs to be considered alongside other factors when deciding between policy options.

Attachment B: Regulatory Burden and Cost Offset Estimate Table

Average Annual Change in Compliance Costs (from BAU)				
Sector/Cost Categories	**Business**	**Not-for-profit**	**Individuals**	**Total by cost category**
Administrative Costs (training)	$29,000	$0	$0	$29,000
Substantive Compliance Costs (wage)	$5,800,000	$0	$0	$5,800,000
Delay Costs	$0	$0	$0	$0
Total by Sector	$5,829,000	$0	$0	$5,829,000

Annual Cost Offset				
	Agency	**Within portfolio**	**Outside portfolio**	**Total**
Business	$0	$5,829,000	$0	$5,829,000
Not-for-profit	$0	$0	$0	$0
Individuals	$0	$0	$0	$0
Total	$0	$5,829,000	$0	$5,829,000

Proposal is cost neutral? ☑ **yes** □ **no**
Proposal is deregulatory □ **yes** ☑ **no**
Balance of cost offsets $___0_____

Attachment C: Regulatory Burden and Cost Offset Estimate Table

Regulatory Offset

A regulatory offset has been identified and agreed with by the OBPR from within the Treasury portfolio. This offset relates to the Future of Financial Advice (FOFA) reforms and is outlined in the table below.

Average Annual Change in Compliance Costs (from BAU)				
Sector/Cost Categories	**Business**	**Not-for-profit**	**Individuals**	**Total by cost category**
Administrative Costs	($140,780,756.58)	$0	$0	($140,780,756.58)
Substantive Compliance Costs	$0	$0	$0	$0
Delay Costs	$0	$0	$0	$0
Total by Sector	($140,780,756.58)	$0	$0	($140,780,756.58)

Annual Cost Offset				
	Agency	**Within portfolio**	**Outside portfolio**	**Total**
Business	$5,829,000	$0	$0	$5,829,000
Not-for-profit	$0	$0	$0	$0
Individuals	$0	$0	$0	$0
Total	$5,829,000	$0	$0	$5,829,000

Proposal is cost neutral? ☑ **yes** □ **no**
Proposal is deregulatory ☑ **yes** □ **no**
Balance of cost offsets $__($134,951,756.58)_____