INSURANCE COUNCIL OF AUSTRALIA

Mr Neil Grummitt
General Manager, Policy Development
Australian Prudential Regulation Authority
GPO Box 9836
SYDNEY NSW 2001

Email: datamgt@apra.gov.au

3 April 2013

Dear Mr Grummitt

DRAFT PRUDENTIAL PRACTICE GUIDE (PPG) 235 – MANAGING DATA RISK

The Insurance Council of Australia[1] (Insurance Council) welcomes the opportunity to comment on APRA's Draft PPG 235 – Managing Data Risk (the Draft PPG). Insurance Council members take data risk and data security very seriously and endorse overall the approach taken in the draft PPG which sets out a highly developed and sophisticated best practice model for data management.

There are two overarching concerns that the Insurance Council has with the Draft PPG. It may be read as being overly prescriptive and secondly, for the exercise in hand, the Draft PPG may be too ambitious in raising issues that go beyond data management.

Consistent with its role as guidance, the final PPG should explicitly acknowledge that regulated entities may decide to adopt it all or in part, using an appropriate risk based approach. Furthermore, for a variety of reasons (such as corporate mergers), regulated entities may need time to make the considerable investment in people, processes and technology in order to achieve the comprehensive data risk management framework advocated. They will need to prioritise which requirements should be progressed and when, in accordance with business needs, assessed operational risk, funding availability and resources.

Consequently, the Insurance Council recommends that APRA review the draft PPG to ensure that its language is consistent with principles-based guidance and that it does not

1) The Insurance Council of Australia is the representative body of the general insurance industry in Australia. Our members represent more than 90 percent of total premium income written by private sector general insurers. Insurance Council members, both insurers and reinsurers, are a significant part of the financial services system. December 2012 Australian Prudential Regulation Authority statistics show that the private sector insurance industry generates gross written premium of $38.7 billion per annum and has total assets of $115.8 billion. The industry employs approx 60,000 people and on average pays out about $102 million in claims each working day.

Insurance Council members provide insurance products ranging from those usually purchased by individuals (such as home and contents insurance, travel insurance, motor vehicle insurance) to those purchased by small businesses and larger organisations (such as product and public liability insurance, professional indemnity insurance, commercial property, and directors and officers insurance).

delve unnecessarily into the detail of how the principles need to be applied. Moreover, APRA should be sufficiently flexible in its supervision to recognise that, consistent with their own specific risk assessments, regulated entities may take different but equally valid approaches to complying with the final PPG.

There are indications in the Draft PPG that APRA may intend to position its guidance on data risk management within the wider context of an overall Technology and Information Management Framework. For example, paragraph 14 discusses e-commerce concepts such non repudiation and authentication and paragraphs 44 and 45 discuss End- User Computing which brings about other associated IT security and system development risks.

The Insurance Council sees advantages in APRA developing an overall IT Governance framework that, as well as Operational Risk, picked up linkages with other risks such as Strategic and Business Risks which also need to be assessed under the ICAAP. However, the final PPG on Managing Data Risk should focus on that issue alone or at least signal where elements of the PPG need to be looked at within a broader context.

Several specific issues are set out in the Attachment.

If you require further information in relation to this submission, please contact Mr John Anning, Insurance Council's General Manager Policy – Regulation Directorate by email: janning@insurancecouncil.com.au or tel: 02 9253 5121.

Yours sincerely

Robert Whelan
Executive Director & CEO

INSURANCE COUNCIL OF AUSTRALIA

ATTACHMENT

PPG 235 – MANAGING DATA RISK: INSURANCE COUNCIL COMMENTS

Introduction

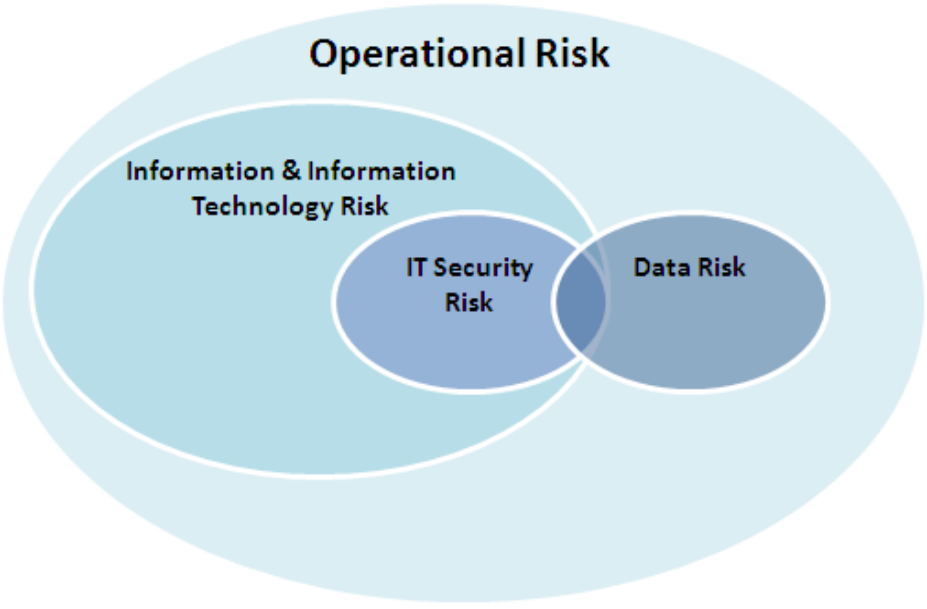
Para 3: The Insurance Council agrees that data needs to be treated as an asset in its own right. We believe it would be helpful to position data as a strategic organisational asset as this will prompt a more effective and complete response to managing data risk within organisations. If data risk management is considered as a strategic organisational issue, there is an increased likelihood that senior management will address and drive organisational change, with support and guidance from IT.

The Insurance Council therefore submits that the final sentence of this paragraph be amended to read: "This trend has enhanced the importance of treating data as an organisational asset in its own right"

Definition

Para 12: In line with the above comment, the Insurance Council suggests that data risk should be seen as a subset of operational risk with overlaps with IT and IT Security risk.

The Insurance Council suggests that the opening sentence of this paragraph be changed to: "*For the purposes of this PPG, data risk is considered to be a subset of operational risk with overlaps with Information and Information Technology Risk and IT Security Risk (refer to the diagram below):"*



While the realisation of data risks can have adverse effects, it is uncertain that the existence of data risk in itself could adversely affect a regulated institution.

Consequently, the Insurance Council suggests that the second sentence of this paragraph be altered to read: '*Realisation of data risks can adversely affect…'*

INSURANCE COUNCIL OF AUSTRALIA

Data and data risk

Para 13(c): The Insurance Council agrees with the range of dimensions set out as constituting data risk but proposes the replacement of 'Consistency' with 'Validity' as we believe it to be a more familiar term for data practitioners. Validity within a single data set may be considered as the basis for consistency across all data sets. For example, in recording customer data, duration of policy in years could be expressed as '4' or 'four'. Both are accurate and complete but only one should be valid as per internal business/system rules. If this data is captured in more than one data set, enforcing validity rules should ensure consistency - for example, business/system rules stipulating that 'duration of policy' in years is expressed as '4' across all systems that record this information.

The Insurance Council suggests that 'Validity' be substituted for 'Consistency' in 13(c).

A systematic and formalised approach

Para 20: The Insurance Council considers that the overarching framework would be enhanced by organisations having an enterprise data management strategy that addresses the end to end data management lifecycle. Without an enterprise strategy, data risk management could only occur in pocket/silos across the organisation, if at all. We acknowledge that elements of an enterprise strategy are covered in section 21, but feel that it is beneficial to emphasise this earlier in the document.

The Insurance Council suggests that a new (20)a be added along the lines of: "has an overarching enterprise data management strategy to manage the lifecycle of data across its business value chain".

Ongoing compliance

Para 25: The Insurance Council suggests that this paragraph could be usefully expanded to explain how APRA expects that the exemption policy and process it advocates would operate. For example, how would exemptions be applied for and to whom and what criteria will be used in the granting of exemptions?

Data Architecture

Para 28(d): The Insurance Council considers that defining the data life cycle will help ensure that organisations consider data risks in a more consistent manner.

The Insurance Council suggests that a definition of the data lifecycle should be inserted into footnote 9 as follows: 'The data lifecycle is considered to be the end to end lifecycle of data through the stages of data identification, definition, capture, storage, processing, publishing, usage, retention and destruction'

Processing

Para 35(c): The reference to "identify and address" could potentially be misinterpreted to literally mean 'identifier' and 'address' records having data quality issues rather than the process of identifying and responding to data quality issues.

The Insurance Council therefore recommends the revision of paragraph 35(c) to read "exception handling to identify and respond to data quality issues in a timely manner".

Destruction

Para 42: The Insurance Council suggests the following amendment in order to provide additional context as to why destruction management is important:

"*The destruction strategy would normally include mechanisms to ensure that data destruction complies with business requirements, including regulatory and legal requirements.*"