APRA RELEASES PRUDENTIAL PRACTICE GUIDE ON MANAGING DATA RISK

By Alec Christie, Partner, and Rose Bollard, Graduate, DLA Piper

The Australian Prudential Regulation Authority ("**APRA**") has issued the final version of its new prudential practice guide, "Prudential Practice Guide CPG 235 - Managing Data Risk" ("**Data Guide**"). The Data Guide aims to assist financial institutions, general and life insurance companies and superannuation funds regulated by APRA ("**Entities**") manage their data risks. This final version of the Data Guide has few changes from the draft released in December 2012.

The Data Guide compliments APRA's earlier IT security guide, Prudential Practice Guide CPG 234 - Management of Security Risk in Information and Information Technology ("**IT Guide**").

The Data Guide focusses on common "*weak areas*" of data risk management identified by APRA through its ongoing supervisory activities of Entities. This targeted approach means the Data Guide is relevant to all Entities – whether by providing alerts to new risks or guidance to improve current practices. It also signals that APRA's current focus and efforts will be directed to monitoring and enforcement of compliance by Entities with the Data Guide.

BACKGROUND TO THE DATA GUIDE

Clearly, data plays a key role in the structure and operations of all Entities and APRA believes that such reliance on data means that it is crucial that all Entities understand and effectively manage their data quality and risks, in addition to any obligations under the IT Guide, the privacy law or otherwise.

APRA notes that a strong data risk management system protects against a range of potential risks to Entities including:

- fraud due to data theft;
- business disruption due to data corruption or unavailability;
- failure to provide deliverables due to inaccurate data; and
- breach of legal or regulatory obligations due to disclosure of sensitive data.

APRA warns that protecting against these risks (along with the matters identified in the IT Guide) is not just the task of the risk management team of an Entity but also the responsibility of senior management and technical specialists within the Entity. The Data Guide reinforces this shared responsibility approach throughout, providing guidance for all such groups within the Entity.

SUMMARY OF KEY ISSUES FOR DATA RISK MANAGEMENT BY ENTITIES

Some of the key issues identified by APRA and recommendations in the Data Guide are:

- **Take a systematic and formalised approach to data risk management** – Data risk management should not be tackled by Entities in an ad hoc or fragmented way. Rather, Entities should take a principles–based approach and put in place an overarching framework. As part of this process, Entities must consider how their framework can ensure their ongoing compliance with regulatory and legal requirements and how they can formalise roles and responsibilities within the Entity.
- **Assess and manage data quality** – Data quality is important and can be assessed through a range of factors, such as accuracy, completeness, consistency and availability of information. The relevance of each of these factors will vary depending upon the nature of the data.
- **Promote staff awareness** – Staff must have appropriate training so that they are aware of their responsibilities in relation to data risk

management and the Entity's processes and procedures.

- **Implement suitable processes for each stage of the data life–cycle** – The stages of the data life–cycle (data capture, processing, retention, publication and disposal) raise different data risk issues and so appropriate processes must be tailored by the Entity to each stage of the data life–cycle. For example, at the "data capture" stage, Entities should consider specifying data quality requirements and mechanisms in agreements with both internal and external third parties. At the publication stage (if applicable), Entities should consider validation and monitoring controls to ensure the published data continues to meet the specified requirements of users.
- **Address risks arising from outsourcing or offshoring of data** – Sending data overseas may increase data risk because the data life–cycle controls of an Entity will often be inadequate and it may be more difficult for the Entity to comply with legislative and prudential requirements. Entities should carefully assess the risks associated with transferring data overseas before entering into such an arrangement. Entities should ensure that they will still be able to meet their legislative and prudential requirements and maintain the quality and integrity of critical or sensitive data.
- **Validate data prior to further processing** – Data must be assessed against business rules to determine its "fitness for use" by the Entity prior to further processing. Data validation incorporates verification of format, type, value range, currency, consistency and completeness. The data validation process must be appropriate for the criticality of data and the risk of degradation. APRA recommends documenting the process as it can be useful for designing data quality metrics.
- **Implement monitoring processes to identify data issues** – Entities must implement monitoring processes so that data issues are identified and rectified as early as possible. Such monitoring processes must be developed and implemented to manage all stages of a data issue: detection, investigation, resolution and adjustment of controls to reduce the risk of similar issues reoccurring.

WHAT DOES THIS MEAN FOR ENTITIES?

The Data Guide, building from the foundations of the IT Guide and in addition to existing obligations under privacy law, reflects APRA's increased focus on the importance of data risk management at all stages of the data life–cycle for Entities and APRA's *"recommendation"* that Entities take a systematic and formalised approach to data risk management.

We recommend that Entities become familiar with the Data Guide (as they have with the IT Guide) and ensure compliance by taking, at least, the following steps:

- review the Entity's data risk management framework, processes and procedures to ensure they are suitable for your business objectives and provide sufficient protection to the Entity;
- assess whether existing data processes and procedures are appropriate for each stage of the data life–cycle and implement new processes if a shortfall is identified;
- consider whether any changes in the Entity's activities or procedures give rise to new data risk issues that you need to address (eg moving data to the Cloud);
- ensure that there are sufficient monitoring processes in place to identify potential data issues and that an assurance program is established to assess whether data quality is appropriate and the Entity's data risk management is effective; and
- implement ongoing monitoring of the data life-cycle within the Entity to ensure any future risks are identified and managed/minimised as soon as possible.

WE CAN HELP!

Please do not hesitate to contact the authors or any of our dedicated financial services information/ privacy team if we can assist with review of your current data risk management processes or if you have any related queries.

Alec Christie
Partner
T +61 2 9286 8237
Alec.Christie@dlapiper.com

Rose Bollard
Graduate
T +61 2 9286 8655
Rose.Bollard@dlapiper.com

CONTACT YOUR NEAREST DLA PIPER OFFICE:

BRISBANE

Level 29, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA

Level 3, 55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE

Level 21, 140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH

Level 31, Central Park
152–158 St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY

Level 38, 201 Elizabeth Street
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 4144
sydney@dlapiper.com

www.dlapiper.com

1201594299/JPS/092013