



23 March 2007

To: AMA/IRB Applicant ADIs

Data management

APRA, as part of its ongoing supervision of regulated institutions, regularly reviews various aspects of each institution's operations. Recent reviews have identified data management as an area that requires closer attention from an institution's management. This issue has also become more prominent with the impending commencement of the Basel II Capital Accord in Australia from 1 January 2008.

APRA has received specific requests from some institutions to provide guidance as to APRA's expectations with respect to data management and how institutions should be managing data.

While data management is especially significant for ADIs who are seeking to be accredited under the advanced approaches to the measurement of credit risk, it is nevertheless a critical issue for all ADIs. APRA is of the view, therefore, that data management and the need to ensure the quality and security of data are critical components of risk management and should form part of a comprehensive risk management framework.

The issue of risk management generally for ADIs is one that APRA expects to consult with industry on later this year as part of the move towards the adoption of Basel II. At present, APRA has specific risk management prudential standards in place for general insurers and is in the process of finalising similar requirements for life insurers. As part of APRA's approach to harmonising prudential requirements across regulated industries, we will be proposing the introduction of a risk management standard and associated prudential guidance for ADIs. Rather than wait until consultation commences on that standard and associated guidance, we believe it is useful to enter into informal discussions with industry now on the subject of data management and provide APRA's views as to guiding principles and practices in relation to data management to which ADIs should give consideration.

Data management is underpinned by a number of core principles: these principles and associated matters that APRA would expect ADIs to consider when developing their data management framework and architecture set out in the attachment to this letter.

APRA invites comments as to the matters set out in the Attachment for consideration in the formulation of any proposed prudential requirements. Whilst APRA will formally consult with industry on any proposed prudential standards, this information is provided at this time to facilitate discussion with industry and in the hope that you may find it beneficial when considering your data management processes.

If you have comments you would like to make please address your correspondence to:

Yours sincerely

Harvey Crapp
General Manager
Credit & Operational Risk Services

Tel: 02 9210 3289

Fax: 02 9210 3022

harvey.crapp@apra.gov.au

ATTACHMENT

Data management principles

Data management

Developments in the banking industry, such as Basel II, have heightened the significance of data to authorised deposit taking institutions (ADIs) and the necessity to maintain data quality throughout the ADI. Poor data quality can compromise decision making, have a detrimental impact on behaviour across an ADI, and ultimately result in a failure to meet business objectives.

As data is a critical and valuable asset for an ADI, there is a need to maintain data quality through an appropriate protection and control environment. Data management is the set of practices for managing data as a valuable asset. Data quality is an outcome of successful data management.

Data quality risk is the risk of data failing to meet regulatory and business requirements. APRA envisages that an ADI would normally identify, assess and manage data quality risks as part of its overall risk management framework.

In APRA's view, an ADI would typically have a risk assessment process to determine the criticality of data to its operations. This risk assessment process would typically include the classification of data according to the regulatory and operational criticality of data. The ADI's data classification and the granularity of the risk assessment would typically be aligned with regulatory and business requirements.

Data management framework

A data management framework is the documentation that outlines an ADI's approach to managing data. It embodies the data architecture and the policies, standards, guidelines and procedures that support the data quality objectives of the ADI.

APRA envisages that an ADI would normally establish and maintain a data management framework, with the elements that comprise the framework formally approved and reviewed on a regular basis. An ADI may find it beneficial to manage the development of the framework as a formal project with clearly defined timeframes and milestones.

A data management framework would typically establish clear accountability for managing data quality, including establishing specific roles and responsibilities. Roles could include Data Custodians, Data Owners and Data Users. An ADI may consider establishing governance functions to ensure a continued focus on data quality.

In APRA's view, an ADI may find it beneficial to develop a process for granting exemptions to the data management framework. Exceptions may be required where the costs of ensuring legacy systems comply with the framework are unduly large.

Data architecture

APRA envisages that an ADI would typically define and maintain a data architecture which describes how data is captured, processed and retained.

APRA envisages that the data architecture would normally align with existing corporate policies, standards and guidelines. Depending upon the complexity of the environment, the data architecture could comprise:

- (a) diagrams and detailed technical information that describe the flow of data, key systems, data repositories and interfaces;

- (b) description of the controls necessary for data capture, processing and retention based on data classification;
- (c) standards and guidelines to facilitate the development of systems, data repositories, interfaces and data controls, including information on approved technologies; and
- (d) information on the characteristics of the data, commonly referred to as metadata. This could include descriptions of data elements and a map of where data is sourced, where it is used and how it is processed.

APRA envisages the data architecture would facilitate:

- (a) assessing the consistency of data definitions across different sources;
- (b) assessing the impact of changes on data quality; and
- (c) assisting in the resolution of data quality issues by providing visibility of data flows and processing undertaken.

Where a system is not aligned to the approved data architecture, APRA envisages that the system would normally:

- (a) have an appropriate level of corporate approval; and
- (b) be assessed for adequacy by an appropriately skilled party prior to deployment.

Under these circumstances, APRA envisages that the ADI would periodically review and reassess the appropriateness of the system and the associated information technology controls.

Data controls

APRA envisages that an ADI would implement controls for maintaining data quality when data is captured, processed or retained. Data controls would normally be located at key risk points in the flow of data, with the nature of the controls taking into account the data classification. This process would typically include:

- (a) protocols for data correction, including approval and review of data changes and appropriate input from the business; and
- (b) root cause analysis of data quality issues to identify the need for additional controls or weaknesses in existing processes.

In APRA's view, the correction of data at the point of capture is preferable.

APRA envisages that an ADI would review and update change management processes to assess the impact on existing data controls and data quality, including the maintenance of audit trails for tracking data changes.

In APRA's view, an ADI would typically segregate roles and responsibilities of key individuals responsible for data quality to minimise the likelihood of data quality being compromised by a conflict of interest.

An ADI may find it beneficial to develop a formal archiving strategy that covers the risks associated with inaccessible data as the result of accidental deletion, changes in technology or poor asset management. The archiving strategy would normally include mechanisms to ensure that data retention complies with regulatory requirements.

Data validation

Data validation refers to data profiling via statistical analysis, reconciliation against another data source and/or reasonableness checking.

APRA envisages that an ADI would periodically validate data and assess whether the data is within expected parameters and continues to meet the quality objectives of the ADI. The nature and frequency of validation processes will vary depending on the type of data and its classification.

An ADI would normally document data validation processes, including their nature and frequency and provide clear definition of accountabilities for the detection, investigation and escalation of data anomalies.

An ADI would also normally investigate any variances and/or anomalies, noting the reasons for differences. An ADI may also find it beneficial to monitor recurring variances and/or anomalies with the view to resolving them where possible.

Where possible, APRA envisages that an ADI would normally reconcile data to an alternative source. In APRA's view, the General Ledger is a good source of comparison for this purpose.

Where reconciliation is not possible, an ADI could consider assessing the data for reasonableness by comparing it to an appropriate data source or by subjecting it to management review.

In APRA's view, data profiling is useful for highlighting data anomalies in aggregate data, such as missing data, outliers or unexpected variances in data between time periods. This could involve the examination of data and the collection of population statistics and other relevant information.

Information technology controls

An ADI would normally maintain appropriate controls for managing its information technology environment. The control environment typically includes:

- (a) change management: how hardware and software changes are applied to the information technology environment;
- (b) security management: how the characteristics of confidentiality, integrity and availability of the information technology environment are maintained;
- (c) disaster recovery: how the information technology environment can meet business objectives in the event of a disaster;
- (d) infrastructure management: how hardware components of the information technology environment are acquired, implemented, configured, tested, problems managed and service levels met; and
- (e) life cycle processes: the requirements for project management, product development, and software development or acquisition.

In APRA's view, an ADI may find it beneficial to implement a formal exemption process for granting, registering and carrying out ongoing reviews of any deviations from information technology policies, standards and procedures.

Data quality metrics

In APRA's view, data quality metrics can be a useful mechanism for assessing data quality, particularly in complex environments. APRA envisages that the use of metrics would be

targeted towards the areas of greatest criticality determined through the risk assessment process.

Each dimension of data quality could be measured by at least one metric to enable the monitoring of progress towards set targets and the identification of trends. In APRA's view, effective metrics would be specific, measurable, business oriented, controllable, reportable and involve the inspection of data.

Common elements typically considered in the assessment of data quality include:

- (a) accuracy: the degree of confidence that can be placed on data being free of error or defect;
- (b) completeness: the extent to which data is not missing and is of sufficient breadth and depth for the task at hand;
- (c) consistency: the degree to which common data across different sources follows the same definitions, codes and formats;
- (d) timeliness: the degree to which data is up to date;
- (e) security: the degree to which data confidentiality, integrity and availability has been maintained; and
- (f) fitness for use: the degree to which data is relevant, appropriate and meets business specifications.

APRA envisages that data quality gaps would be addressed over time in a systematic way. This may involve the formulation of a data quality plan which specifies target data quality metrics, timeframes for resolution and associated action plans for closing the gaps. Action plans would normally be appropriately prioritised and tracked.

Independent assessment

APRA envisages that an independent party, such as Internal Audit, would review data quality as well as key processes and controls on a regular basis. Such reviews may encompass the:

- (a) data management framework and whether it is being complied with;
- (b) inspection of data;
- (c) data and information technology controls; and
- (d) data metrics and data quality plan(s).

APRA envisages that an ADI would typically ensure that review staff have appropriate skills in the area being assessed.

Staff awareness

In APRA's view, an ADI may find it beneficial to include data quality in training and development programs to increase staff awareness of data quality.

An ADI could also consider incorporating data management responsibilities as a component of staff performance plans.