IMPLEMENTATION NOTE

Subject: Data Maintenance at IRB Institutions

Category: Capital

No: A-1 Date: January 2006

I. Introduction

This implementation note elaborates on the data management requirements for institutions[1] adopting the internal ratings-based (IRB) approach as outlined in OSFI's *Capital Adequacy Requirements* (CAR) Guideline A-1, Chapter 5. All relevant and material quantitative and qualitative data used to assess and manage credit risk should be adequately maintained. Institutions will need to maintain comprehensive historical data across legal entities and geography. This data will include, but not be limited to, borrower information, credit transaction details, portfolio risk characteristics, ratings, rating migration, default, and collateral.

Data management and timely execution of underlying information technology initiatives are major challenges that institutions need to address in order to successfully implement the IRB methodology under CAR. CAR outlines the scope and certain characteristics of data maintenance; however, there is limited description of expectations on the data maintenance (or generic "data management") process itself.

This note provides general guidance on data maintenance and principles for institutions to apply when establishing an enterprise-wide IRB framework. These principles are not intended to be prescriptive or limiting in any manner. Adherence to the broad principles outlined in this implementation note will be an important consideration in OSFI's initial IRB approval and for monitoring ongoing compliance.

The term "data maintenance" incorporates the key components of the data management process, including data collection, data processing, data access/retrieval and data storage/retention.

[1] Banks and bank holding companies to which the *Bank Act* applies and federally regulated trust or loan companies to which the *Trust and Loan Companies Act* applies are collectively referred to as "institutions".

Table of Contents

II. Data Maintenance Principles

1. Senior Management and Oversight

Institutions seeking IRB approval should adopt an approach to managing their information technology initiatives and data management processes appropriate to the nature, scope and complexity of their data maintenance requirements.

Institutions should have appropriate processes and procedures in place supported by effective Senior Management oversight to ensure successful completion of their programs related to IRB data maintenance for IRB approval and ongoing compliance with the IRB approach.

In particular, institutions' Senior Management should assess the scope, plans and risks associated with timely execution of data maintenance projects, and take effective measures to mitigate these risks. The accountabilities of Senior Management will include, but are not limited to:

a) Reviewing and approving organizational structure and functions to facilitate development of appropriate data architecture to support implementation of CAR;

b) Establishing an enterprise-wide data management framework defining, where appropriate, the institution's policies, governance, technology, standards and processes to support the data collection, data maintenance, data controls and distribution of processed data, i.e., information;

c) Ensuring data maintenance processes provide security, integrity and auditability of the data from its inception through to its archival and/or logical destruction;

d) Instituting internal audit programs, as appropriate, to provide for periodic independent audits of data maintenance processes and functions; and

e) Ensuring the appropriate policies, procedures and accountabilities are in place to monitor the enterprise-wide observance of the data management framework, including ongoing updates to procedures and documentation, as necessary.

2. Data Collection

In the context of CAR, the data collection component (also referred to as data acquisition or data capture) would typically involve determining requisite data elements in various internal/external source systems, and their validation and extraction to appropriate operational data stores or data repositories.

Institutions' data collection processes should:

a) Establish clear and comprehensive documentation for data definition, collection and aggregation, including data mapping to source/aggregation routines, data schematics where necessary, and other identifiers, if any;

b) Establish standards for data accuracy, completeness, timeliness and reliability;

c) Ensure that data elements collected encompass the necessary scope, depth and reliability to substantiate rating definitions, rating assignment, rating refinement, risk parameters, overrides, back-testing and other processes, capital ratio computations, and relevant management and regulatory reporting;

d) Identify and document data gaps and, where applicable, document the manual or automated workarounds used to close data gaps and meet data requirements;

e) Establish standards, policies and procedures around the cleansing of data through reconciliation identifiers, field validation, reformatting, decomposing or use of consistent standards, as appropriate, and;

f) Establish procedures for identifying and reporting on data errors and data linkage breaks to source, downstream and/or external systems.

3. Data Processing

The data processing component covers a wide range of data management tasks, including its conversion through multiple systems (or manual) processes, transmissions, source/network authentication, validation, reconciliation, etc.

Institutions' data processing should:

a) Limit reliance on workarounds and manual data manipulation in order to mitigate the operational risk related to human error and dilution of data integrity;

b) Establish standards and data processing infrastructure for life-cycle tracking of credit data including, but not limited to, relevant history covering borrowers, obligors, credit facilities, transactions, repayments, rollovers, restructuring, and sale and error trails, as appropriate;

c) Ensure appropriate levels of front-end validation/data cleansing for each process and reconciliation to related processes as applicable, e.g., accounting and general ledger, line of business management information system;

d) Establish adequate controls to ensure processing by authorized staff acting within designated roles and established authorities;

e) Institute appropriate change control procedures for changes to the processing environment, including, where applicable, change initiation, authorization, program modifications, testing, parallel processing, sign-offs, release, library controls; and,

f) Provide appropriate levels of disaster back-up, process resumption and recovery capabilities to mitigate loss of data and/or data integrity.

4. Data Access/Retrieval

From OSFI's supervisory perspective, a key component of data maintenance is the continued availability of institutions' data and information for the purpose of IRB approval and ongoing monitoring of IRB compliance, such as back-testing, replication, historical or other trend analyses.

Institutions should ensure that:

a) Data repositories and underlying extract, query and retrieval routines are designed and built to support the institutions' own data requirements as well as ongoing needs for supervisory assessments of various data as appropriate, including credit portfolios, history, borrower/industry profiles, exposures, process quality, asset class analyses;

b) Access controls and data/information distribution are based on user roles/responsibilities and industry best practices in the context of effective segregation of duties, "need to know", as validated by institutions' internal compliance and audit functions; and

c) Access to data/information is not restricted in any arrangements where data maintenance is outsourced to external service provider(s). Notwithstanding these arrangements, institutions should be able to provide data/information at no additional cost.

5. Data Storage/Retention

The data storage/retention component of data maintenance addresses the dual expectations of electronic data retention and archival to meet the minimum historical retention criteria established under CAR, as well as the requirements of institutions and OSFI to ensure ongoing IRB compliance and credit risk management data/information calls.

CAR requires institutions to use all relevant data in the development of IRB internal estimates. In order to support internal estimates and ensure that all relevant risks are considered, data may be needed for a long period of time. For corporate, sovereign and bank exposures, a minimum of

five years of underlying history for PD[2] estimates, and a minimum of seven years underlying history for LGD and EAD estimates should be maintained. For retail exposures, a minimum of five years of underlying history for PD, LGD and EAD estimates is required. On implementation, institutions may not be able to meet this standard, but they should have IRB data going back to at least October 31, 2004.

In addition, institutions should:

a) Establish documented policies and procedures addressing storage, retention and archival, including, where applicable, the procedures for logical/physical deletion of data and destruction of data storage media and peripherals;

b) Maintain back-ups of relevant data files/stores and data bases in a manner that can facilitate ready availability of the data/information to meet information calls on IRB-compliance and ongoing supervisory assessments; and

c) Ensure that availability of electronic versions for all relevant and material data/information is in a machine-readable format and can be made accessible.

[2] Probability of default ("PD"), loss given default ("LGD") and exposure at default ("EAD").

Appendix I: Data Life Cycle Management