



Implementation note

Title	Data Maintenance at TSA & AMA Institutions
Category	Capital Adequacy Requirements
Date	May 31, 2006
Sector	Banks Trust and Loan Companies
No	A & A-1

Table of Contents

Guidance to be rescinded

I. Introduction

II. Data Maintenance Principles

- 1. Senior Management and Oversight
- 2. Data Collection
- 3. Data Processing
- 4. Data Access/Retrieval
- 5. Data Storage/Retention

III. Operational Risk Data Categories

- 1. Gross Income Data
- 2. Operational Loss Data
- 3. Other Operational Risk Data

IV. Conclusion



Guidance to be rescinded

As a result of OSFI's policy review, this guidance was identified as outdated, redundant, or no longer fit-for-purpose. It will be rescinded and removed from the website by April 1, 2025.

I. Introduction

This implementation note provides key data maintenance principles for operational risk data. These principles are based on OSFI's *Capital Adequacy Requirements (CAR) Guideline A*, Chapter 6 and *CAR Guideline A-1*, Chapter 7.

This implementation note is relevant for an institution Banks and bank holding companies to which the *Bank Act* applies and federally regulated trust companies and loan companies to which the *Trust and Loan Companies Act* applies are collectively referred to as "institutions". applying for The Standardized Approach (TSA)As per the CAR Guideline, all TSA institutions must be able to track and report relevant operational risk data including material operational risk losses by significant business line. OSFI recognizes that the sophistication of an institution's tracking and reporting mechanism should be appropriate for the size of the institution, taking into account its reporting structure as well as the operational risk exposure of the institution. or the Advanced Measurement Approach (AMA) for operational risk. An institution implementing the Basic Indicator Approach (BIA) is not required to collect operational loss data. However, should a BIA institution collect operational risk data, OSFI encourages the institution to adopt the key principles set out in this implementation note as appropriate.

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. This note provides principles for specific operational risk data categories including gross income, operational loss data and other data elements of operational risk measurementThis implementation note does not provide principles for using the data elements in the quantification of operational risk capital. . Operational loss data includes internal data, external data and scenario analysis data.

II. Data Maintenance Principles

1. Senior Management and Oversight

An institution applying for TSA or AMA should establish information technology and data management processes appropriate to the nature, scope and complexity of its data maintenance requirements. Senior Management should assess the scope, plans and risks associated with timely execution of data maintenance projects, if any.

In this context, the accountabilities of Senior Management include, but are not limited to:

- Reviewing and approving organizational structure and functions to facilitate development of appropriate data architecture to support implementation of TSA or AMA,
- 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,
- Ensuring data maintenance processes provide security, integrity and auditability of the data from its inception through to its archival and/or logical destruction,
- Instituting internal audit testing, as appropriate, to provide for periodic independent assessment of the effectiveness of controls over data maintenance processes and functions, and
- Ensuring that 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

The data collection for operational risk typically involves identifying the appropriate data elements pertinent to the management of operational risk.

An institution's data collection processes should:

- Establish clear and comprehensive documentation for data definition, collection and aggregation, including data mapping to CAR business lines, data schematics where necessary, and other identifiers, if any,
- Establish standards for data accuracy, completeness, timeliness and reliability,
- Identify and document gaps and, where applicable, document the manual or automated workarounds used to close data gaps and meet data requirements,
- Establish standards, policies and procedures around the cleansing of data through reconciliation, field validation, reformatting, decomposing or use of consistent standards, as appropriate, and
- 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.

An institution's data processing should:

- Limit reliance on workarounds and manual data manipulation in order to mitigate the operational risk related to human error and dilution of data integrity,
- Ensure appropriate levels of validation, data cleansing and reconciliation for each process, as applicable,
- Establish adequate controls to ensure processing by authorized staff acting within designated roles and established authorities,
- 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

- 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 an institution's data and information. More importantly for an AMA institution, the monitoring of adherence to CAR minimum requirements will include back-testing, historical or other trend analyses.

An institution should ensure that:

- Data repositories and underlying extract, query and retrieval routines are designed and built to support the institution's own data requirements as well as ongoing needs for supervisory assessments of various data as appropriate,
- Access controls and data/information distribution are based on user roles/ responsibilities and industry sound practices in the context of effective segregation of duties, and is in conformance with the "need to know" principle, which is assessed by the institutions' internal compliance and audit functions for overall effectiveness of the internal controls designed to ensure this conformance and compliance, and
- Access to data/information is not restricted in any arrangements where data maintenance is outsourced For guidance on outsourcing, refer to OSFI's Guideline "B-10: Outsourcing of Business Activities, Functions and Processes". to external service provider(s). Notwithstanding these arrangements, an institution 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 an institution.

CAR requires an AMA institution to use internal losses as one of its data elements to measure the regulatory capital for operational risk. The measurement must be based on a minimum five-year observation period. As per CAR, when the bank first moves to the AMA, a three-year historical data window is acceptable (including parallel calculations) of internal loss data.

In addition, TSA and AMA institutions should:

- Establish documented policies and procedures addressing storage, retention and archiving, including, where applicable, the procedures for logical/physical deletion of data and destruction of data storage media and peripherals,
- Maintain back-ups of relevant data files/stores and databases in a manner that can facilitate readily available data/information to meet information calls on TSA and AMA compliance and ongoing supervisory assessments, and
- Ensure that availability of electronic versions for all relevant and material data/information is in a machine-readable format and can be made accessible.

III. Operational Risk Data Categories

Operational risk capital measurement, whether TSA or AMA, is highly dependent on an institution's ability to maintain a reliable operational risk dataset(s) for various operational risk data categories. The operational risk data categories include gross income data, operational loss data and other qualitative data representing business environment and internal control factors.

As per paragraph 653 of CAR, a TSA institution is required to calculate its capital based on three years of gross income. In addition, for effective operational risk management, a TSA institution is required to track and report its material losses.

Comprehensive data are important for the successful implementation of AMA, especially in the measurement of operational risk capital and the management of an institution's operational risk exposures. An AMA institution is

required to incorporate four data elements in its capital measurement methodology. These include internal losses, external losses, scenario analysis and business environment and internal control factors.

In addition to the key data maintenance principles outlined earlier in this implementation note, specific principles for TSA and AMA operational risk data categories have been set out below.

1. Gross Income Data

As per paragraph 653 of CAR, a TSA institution is required to use gross income to determine the operational risk capital charge. To maintain reliable gross income data for the calculation of capital, and in alignment with the implementation of CAR requirements relating to gross income, an institution should consider the following:

- Documenting the mapping process to provide for the consistent mapping of gross income data,
- Establishing a system or process that facilitates the reconciliation of gross income reported in CAR reporting forms to the firm's reported financial results, and
- Ensuring that the robustness is commensurate with the complexity of the gross income mapping process.

2. Operational Loss Data

(i) Internal Loss Data

All TSA institutions must be able to track their material internal losses and related data elements by business line. OSFI recognizes that the industry practices for collecting internal operational losses are emerging. It is expected that tracking systems will vary across TSA institutions. As outlined in CAR, the sophistication of an institution's tracking system should appropriately reflect the size, reporting structure and the operational risk exposure of the institution. Accordingly, an institution's tracking system will be assessed against its ability to comprehensively capture its material operational losses.

Accountabilities assigned to the data maintenance of internal loss data (and its related data elements) should consider:

- Ensuring that the maintenance of internal loss data aligns with the established enterprise-wide data management framework As outlined under the accountabilities of Senior Management on page 3 of this document. ,
- Determining and documenting the scope of internal loss data to be collected according to its operational risk management needs,
- Establishing and documenting processes for mapping internal loss data to business lines,
- Developing and documenting standards to ensure a consistent process for the collection of internal loss data,
- Incorporating internal loss data as part of its operational risk reporting to effectively support the ongoing management of operational risk,
- Ensuring periodic independent reviews of the processes involved in the collection of loss data.

An AMA institution is also expected to adhere to certain CAR requirements (paragraphs 670 to 673) as relevant to the data maintenance of its internal losses. In order to facilitate the implementation of these minimum requirements, an AMA institution should consider:

- Identifying and documenting the scope of loss data collected for the purposes of calculating capital,
- Establishing and documenting standards for the use of internal loss data in the measurement of operational risk capital. This may include the use of internal loss data in a quantification model as well as any use of internal loss data in scenario analysis,
- Ensuring that the organizational structure and processes (e.g. centralized functions, decentralized functions) supports the data collection process, including timeliness and integrity,
- Documenting data field definitions to ensure consistency and completeness in the data collection,
- Separately flagging loss events (e.g., opportunity costs, credit losses relating to operational risk losses) that are collected in the dataset but are not used for the purposes of regulatory reporting, and

- Incorporating the internal loss data, in a complete and timely manner, into the operational risk reporting for both operational risk management purposes and capital impact analysis.

(ii) External Loss Data

As per paragraph 674 of CAR, an AMA institution is required to incorporate relevant external data, whether it is in the form of public data and/or pooled industry data. External data can be useful additional information especially when an institution has limited internal loss data.

In order to facilitate the implementation of these minimum requirements, AMA institutions should consider:

- Identifying and documenting a consistent process for determining the scope of external data used, ensuring that the data is appropriate for assessing infrequent, yet potentially severe losses,
- Establishing and documenting standards for a systematic process that incorporates external data into measurement methodologies,
- Ensuring that external data is used to measure operational risk appropriately, reflecting its operational risk exposure and is used to represent of tail-end losses,
- Incorporating external data as part of its operational risk reporting to effectively support the ongoing management of operational risk exposures, and
- Conducting periodic independent reviews of the processes involved in the use of external loss data.

3. Other Operational Risk Data

Other operational risk data (quantitative or qualitative elements) may include scenario analysis, risk assessments of business environment and internal control factors that underscore an operational risk profile (e.g. risk and control self-assessment results, key risk indicators), and audit scores. For AMA institutions, minimum requirements related to scenario analysis and business environment and internal control factors have been set out in paragraphs 675 and 676 of CAR. An institution should consider the following for the maintenance of other operational risk data:

- Establishing standards and processes for determining the scope and criteria for these data,
- Documenting the use of these data in its operational risk methodology,
- Incorporating these data, in a complete and timely manner, into operational risk reporting, as appropriate, and
- Ensuring that the processes of collecting these data are subject to periodic independent review.

IV. Conclusion

This implementation note has focused on principles to guide an institution in maintenance of operational risk data. Accordingly, the focus is on the TSA and AMA institutions to ensure that the operational risk data is consistent and provides a sound, reliable and a representative basis for management of institution's operational risk exposure.

OSFI has specifically not prescribed requirements for deploying the operational risk data in the measurement of operational risk capital charges for an AMA institution. OSFI recognizes that the scope of operational risk data, and the methodologies of collecting and incorporating such data in the quantification process, will evolve; and with this development the range of acceptable of practices will emerge within the industry, OSFI expects that further guidance on the use of operational risk data in capital measurement process will follow, as appropriate.