WHITE PAPER

DOES YOUR DATA OFFER VISIBILITY INTO ENTERPRISE RISKS?

Mitigate business risks with Basel III compliance

Infosys®
Navigate your next

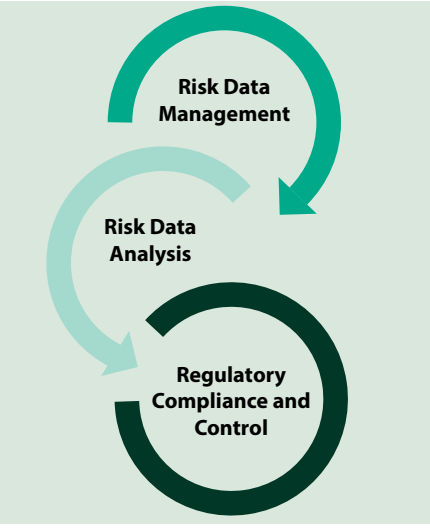
Data management transcends compliance

Basel III regulations stipulate new capital, liquidity and leverage standards for banks. It involves an increase in the amount and quality of data to be reported to regulators. More detailed data must be submitted at a higher frequency. To ensure compliance, banks may need to capture new business data to develop, validate and calculate new liquidity ratios.

The pace of technology and regulatory changes demands that the database functions are not limited to 'store, integrate and access.' The data warehouse now needs to adapt to tactical changes and strategic solutions.

Banks must mine processes such as aggregating, analyzing, and standardizing to extract high quality data for internal as well as external reporting. It involves a laser focus on data management. The quality and accuracy of data are extremely important. Data inconsistency can lead to further scrutiny that may impact the credibility of the bank. A bank's data management program must adopt a unified approach – integrated systems, a data model covering risk management, and high volume / high quality data support from a centralized data repository.

Exhibit1: The below exhibit shows the core dependency of reporting and control over the Risk Data Management.



Integrated systems

Banks tend to create data silos in the course of compliance with regulatory norms. Data silos compromise the quality of data. A majority of the existing systems capture data based on departmental or functional requirements, and are incompatible with other systems.

Banks must build integrated systems with a stable foundation to streamline data and complement the risk management data warehouse. It will safeguard the integrity of data for risk reporting.

Data standardization

Banks must standardize data in functions / divisions to achieve risk aggregation across business areas. Data standardization can be evaluated in terms of granularity, quality, consistency, completeness, and timeliness.

• Data granularity:

The data model must support the granularity level of reporting and analysis. For instance, banks must accommodate different types of provisional data (product, customer, cost center, transaction, and portfolio level) in a single model.

• Data quality:

High quality data helps banks improve capital and liquidity management. The focus on data quality must be initiated from the front office where data entry begins. The standards of data quality must be clearly articulated and implemented through systematic data checks. Inconsistent data quality results in incorrect data being used in Risk Weighted Asset (RWA) calculations. Consequently, the resulting RWAs are over estimated or under estimated.

• Data consistency:

Large banks are challenged by data inconsistency due to multiple businesses and legal entities, counterparty data, and operations in diverse regions. It is a consequence of a business having different data rules and data models. Processing inconsistent data in a central repository and using it for aggregating and reporting is a business challenge.

• Data completeness:

Data must be available in terms of transaction / business event, counterparty, product, region, and any other grouping that signifies emerging risk. Banks can manage incomplete data with more processes and controls such as data adjustments or automated data checks.

• Timelines:

Historical data is critical for banks. Maintaining sufficient data on important risk factors is crucial for analysis and risk management, while data sets of long periods provide an in-depth understanding of risks. Historical data can be maintained based on the type of data. For example, reference data requires to be stored longer than transactional data. The duration of delivery of data to be reported is a critical factor during stress testing. Reporting is difficult when the data requested is different from standard reporting formats. It may lead to manual adjustment of figures, which causes incorrect reporting.

Centralized data repository

A centralized data repository is a business imperative to address business and regulatory requirements promptly and at reduced cost. It helps banks perform mandatory regulatory reporting and fulfill analysis requirements. Significantly, a centralized data repository provides managers with a consolidated view of business and operations in terms of:

- Regulatory compliance
- Relationship banking
- Customer behavior analysis
- Wealth management
- Investment management
- Stress testing

Risk data from different units and divisions consolidated in a single repository ensures a centralized approach to collection and submission of data under Basel II and III norms. A centralized data repository addresses credit, market, operational, and liquidity risks for regulatory reporting.

A bank's centralized data repository must support data feeds from multiple systems. Generic data formats are effective to manage one type of data from multiple systems. It can be built based on the most common types of reporting and analysis to be performed such as customer behavior analysis. Basel II templates can be extended to accommodate changes for Basel III requirements, and new templates can be created for new types of data to be reported. For example, a generic template for Credit Valuation Adjustment (CVA), a new capital charge introduced by Basel III, must be created.

The centralized data repository must receive data directly from the source (front office) and not from a secondary database (data silos). Wherever possible, one type of data must originate from a single source to eliminate the risk of duplication. For example, counterparty data should be sent from one system rather than multiple systems.

Enterprise logical data models

The bank's risk data warehouse must have a data model covering all risk management requirements:

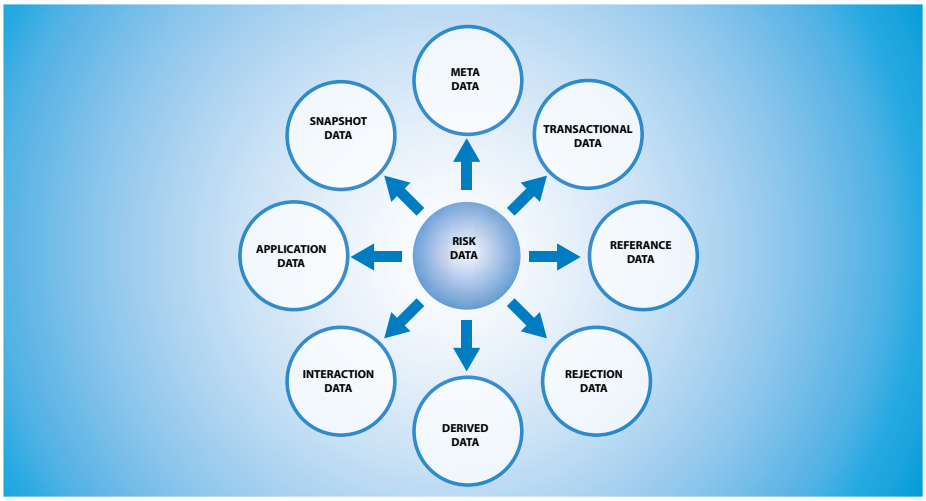
- It must be proven and support all risk factors, counterparties / legal entities, instruments, and organizational hierarchies required for regulatory reporting.
- The data model must cover credit, liquidity, market, concentration, and operational risks.
- The data model must support data at the granular level required by regulations. If existing models are re-used, they must be re-examined for new risk appetites.

Types of data in the risk data warehouse

The types of data must be built based on the transactions, counterparties and products of the bank:

- Meta data:
  Provides summarized data leading to detailed data.
- Transactional data:
  Covers data related to business events. It is dynamic and voluminous in nature.
- Customer data:
  Covers data related to counterparties with whom banks perform business events. It is semi-static, i.e., it may change but not frequently.
- Reference data:
  Covers data about products and cost centers that are related to a transaction. Such data has a low volume and does not change. Banks must have a single golden source of data to avoid duplication of reference data. For example, banks cannot have two product ids for one product.
- Rejection data:
  Covers data that fails business defined validations. Analysis of rejected data ensures that data quality standards are maintained.
- Derived data:
  Covers data derived from source data such as generated payments (non-retail).
- Intersection data:
  Creates a sequential number for each record during processing based on the unique identifier of the record in the source file. Such data helps downstream users track the source of records.
- Application data:
  Involves applications that may require reporting for some data, but not from the core repository. These applications may require processing of core data to meet specific requirements.
- Snapshot data:
  Covers data for which no history is maintained.

Exhibit 2: The below exhibit shows the snapshot of type of data in warehouse



Data sourcing, validating and storing

1. Data sourcing

In the sourcing process, the core risk data warehouse receives automated data feeds from various systems of the bank. The warehouse must switch from conventional, static batch to real-time, dynamic batch processes. Data must be sourced in real time and not at the end of the day. An integrated approach of unifying front office systems with the ability to transfer data whenever it changes will ensure that real-time data is available in the repository to meet regulatory and analysis requirements. The frequency of reporting increases manifold with new regulations. As a result, sourcing the data from the point of capture resolves delays that banks face due to data adjustments.

2. Data validation

Validation is important to maintain the quality of data. Business rules must be established based on appropriateness, completeness and accuracy of data. Requisite alerts must be triggered at the data source on completion of validations for analysis and control. Rejected data must be analyzed for deficiencies, and a mechanism established for oversight in the areas of:

- Technical data checks:

  Address technical constraints for fields in the data model. For example, the country name in the field must be a valid country name in the reference data table.

- Business data checks:

  Applied based on business requirements. For example, the value of a field can only be 'ABC' or 'XYZ'. Any other value including 'NULL' must not be accepted.

- Functional data checks:

  Address functional constraints for fields in the data model. For example, the date of birth of the counterparty must be before 'AS AT DATE' of record in the data warehouse.

3. Data storing

Only data that conforms to the criteria of quality will be accepted in the centralized repository. The history of data must be determined based on the type of data. The customer and reference data must be stored for a longer period (5-6 years) compared to transactional data (2-3 years).

A Basel III data agenda

Mere regulatory compliance is an opportunity lost. Banks must invest in processes to make operations more efficient. Banks must implement a robust data management framework for consolidating, loading and processing risk data in a centralized repository, and report from a centralized reporting platform. Significantly, banks must explore innovative ways of creating operational efficiencies and market differentiation. Data and IT infrastructure must fully support risk aggregation capabilities and risk reporting practices. The bank's existing model will determine whether it needs to enhance the existing environment or implement a new environment. Banks must use the Basel III compliance regulatory imperative to improve business processes and achieve business goals.

About the Author

Poonam is a Risk and Compliance Consultant with the Financial Services practice at Infosys. She has more than six years of experience in the financial services and healthcare industries. Her areas of expertise include risk and compliance, healthcare regulatory mandates, and credit risk database management. She has worked on requirements gathering, analysis and validations for transitional programs including database management for Basel III regulations and compliance, healthcare mandates (ICD-10), and clinical changes. Poonam completed her Master of Business Administration (MBA) from the University Business School, Punjab University, Chandigarh. She can be reached at poonam01@infosys.com