

<b>Part A</b>	<b>OVERVIEW .....</b>	<b>1</b>
1.	Introduction.....	1
2.	Applicability .....	2
3.	Legal Provision .....	2
<b>Part B</b>	<b>SOUND DATA MANAGEMENT AND MIS PRACTICES .....</b>	<b>3</b>
4.	Guiding Principles .....	3
<b>Part C</b>	<b>IMPLEMENTATION.....</b>	<b>13</b>
5.	Implementation Requirements .....	13

BNM/RH/GL_018_1	Prudential Financial Policy Department	Guidelines on Data Management and MIS Framework	Page 1 / 13
-----------------	----------------------------------------	-------------------------------------------------	-------------

## **PART A OVERVIEW**

### **1. Introduction**

- 1.1 In an increasingly competitive and fast-paced environment, appropriate and easily accessible information provides critical support to financial institutions in the decision making process and day-to-day operations. In this regard, a framework to manage data and disseminate information throughout an organisation effectively and efficiently provides a strong foundation for well-run financial institutions. Principally, such a framework should support a high level of assurance regarding data quality that would facilitate data mining, analysis and reporting by financial institutions for the purposes of risk management and conduct of significant business activities.
- 1.2 Bank Negara Malaysia expects financial institutions to establish and maintain a sound data management and management information system (MIS) framework. Senior management, with appropriate oversight by the board, must play a key role in the development of the framework to ensure the proper allocation of resources, effective planning and coordination across the organisation and alignment to the organisational strategic objectives, and a corporate culture that reinforces the importance of data integrity. Of importance, considerations around resources, technology and infrastructure issues need to be addressed in the context of the organisation's overall corporate objectives and the evolution of its business model over time.
- 1.3 The Guidelines on Data Management and Management Information System (the Guidelines) sets out high level guiding principles on sound data management and MIS practices that financial institutions should observe when developing internal data management capabilities. Financial institutions should structure and implement data and management information systems in a manner that is consistent with the principles set out in the Guidelines and appropriate to each institution's specific business needs.

<b>BNM/RH/GL_018_1</b>	<b>Prudential Financial Policy Department</b>	<b>Guidelines on Data Management and MIS Framework</b>	<b>Page 2 / 13</b>
------------------------	-----------------------------------------------	--------------------------------------------------------	--------------------

## **2. Applicability**

- 2.1 These guidelines are applicable to all institutions licensed under the Banking and Financial Institutions Act 1989 (BAFIA), Islamic Banking Act 1983 (IBA), Insurance Act 1996 (IA) and Takaful Act 1984 (TA), hereinafter referred to as “financial institutions”. Other institutions which are part of a financial group are also encouraged to adopt the principles contained in these guidelines, where appropriate.
- 2.2 These guidelines should be read together with other specific risk guidelines as well as other relevant guidelines or circulars issued by the Bank.

## **3. Legal Provision**

- 3.1 These guidelines are issued pursuant to section 126 of the BAFIA, Section 53A of the IBA, Section 201 of the IA and Section 69 of the TA.

BNM/RH/GL_018_1	Prudential Financial Policy Department	Guidelines on Data Management and MIS Framework	Page 3 / 13
-----------------	----------------------------------------	-------------------------------------------------	-------------

## PART B SOUND DATA MANAGEMENT AND MIS PRACTICES

### 4. Guiding Principles

**Principle 1: Financial institutions should develop and implement an effective data management and MIS framework that is aligned with the institution's business and risk strategies. The roles of the board and senior management in relation to the oversight, design and operationalisation of the framework should be clearly defined.**

4.1 A data management and MIS framework defines the operating framework for meeting a financial institution's data and MIS requirements to support its strategic, operational and risk management functions. It should set out policies, systems and procedures relating to:

- (i) data governance (refer Principle 2);
- (ii) data architecture (refer Principle 3); and
- (iii) internal controls and reviews (refer Principles 4 and 5).

4.2 The board must maintain effective oversight over the data management and MIS framework and ensure that the framework is aligned with the business and risk strategies of the institution. This includes providing direction to senior management on broad expectations of the framework in supporting strategic and operational decision-making. These expectations should be documented in formal policy statements on data management and should address the institution's organisational needs in terms of acceptable system performance levels, operational reliability, data quality, security and transparency of data management processes. The board is also responsible to ensure that expectations are met on a continuing basis and approve strategic resource allocations towards data management and MIS enhancement initiatives.

4.3 Senior management has operational responsibility for the design of the data management and MIS framework. Senior management should advise the board on the key features of the framework and any subsequent changes made thereto in a timely manner. In certain situations, the board may consider

<b>BNM/RH/GL_018_1</b>	<b>Prudential Financial Policy Department</b>	<b>Guidelines on Data Management and MIS Framework</b>	<b>Page 4 / 13</b>
------------------------	-----------------------------------------------	--------------------------------------------------------	--------------------

it appropriate to require senior management to obtain its specific approval (either directly or through a board-delegated committee) of key features of the framework prior to implementation. This is relevant where the features have significant or wider implications for the institution's internal decision-making processes, timeliness and controls of information flows, privacy policies, and interfaces within and outside the organisation.

- 4.4 Senior management should periodically review and advise the board on the effectiveness of the data management and MIS framework. Such reviews should serve to ensure that the framework remains responsive to changes in business activities and processes, and is able to support expanding needs of risk management and business functions over time. This includes ensuring the scalability of system infrastructure and processes to accommodate developments (such as business acquisitions) that have major data implications, the introduction of new financial products and services, and changes in the regulatory environment. The framework, including the technology employed, should be able to support new data requirements in these situations economically and effectively.
- 4.5 The data management and MIS framework and governance structure should be subject to independent reviews by an external party or the internal audit function. Such reviews should provide senior management and the board with an overall assessment of:
- (i) the adequacy of data management and MIS framework in relation to the nature, complexity and scale of the financial institution's operations;
  - (ii) appropriateness of data standards and adequacy of policies and procedures established to meet those standards<sup>1</sup>;

---

<sup>1</sup> Where appropriate, the external party or internal auditor should:-

- participate as observers in data cleansing exercises to further enhance the integrity of the process; and
- assess the quality of data (e.g. completeness and accuracy) to ensure that it is preserved throughout the end-to-end processes.

BNM/RH/GL_018_1	Prudential Financial Policy Department	Guidelines on Data Management and MIS Framework	Page 5 / 13
-----------------	----------------------------------------	-------------------------------------------------	-------------

- (iii) the risks inherent in the institution's data management and MIS environment and effectiveness of controls in place to mitigate those risks; and
- (iv) whether adherence to established policies, procedures and controls has been effectively maintained.

**Principle 2: Financial institutions should establish a sound data governance structure that ensures the effective control of data quality.**

- 4.6 Data governance refers to the overall management of the availability, usability, reliability, integrity and security of the data employed in an organisation.
- 4.7 Senior management should establish appropriate governance structures that support a clear accountability framework for the effective implementation of the financial institution's data management policies and standards. The governance structures must be well integrated across business units, and between business units and the IT functions.
- 4.8 Functions responsible for data management must have a formal status at senior management level within the institution with the appropriate authority to implement approved data management policies and standards in the organisation. The specific responsibilities associated with data management should be clearly defined, and should generally include:
- (i) identifying the institution's data needs on an ongoing basis. This includes taking proactive steps to anticipate changing data needs in the light of organisational or external developments, thereby pre-empting business disruptions due to inadequate data support;
  - (ii) ensuring that the institution's data needs are effectively incorporated in documented data policies and procedures for the creation, capture, maintenance, reporting, distribution and retention of data;
  - (iii) translating data quality expectations set by the board into specific goals for significant data systems and owners, and defining the metrics for measuring data

<b>BNM/RH/GL_018_1</b>	<b>Prudential Financial Policy Department</b>	<b>Guidelines on Data Management and MIS Framework</b>	<b>Page 6 / 13</b>
------------------------	-----------------------------------------------	--------------------------------------------------------	--------------------

quality with respect to its accuracy, completeness, consistency and currency (i.e. up-to-date for the intended purpose);

- (iv) ensuring that data control functions are operating effectively to preserve the integrity of the institution's data, including financial information reported to the Bank. This includes ensuring that adequate controls are in place to safeguard the security of the institution's data repositories and the transmission of confidential and mission critical data. The controls should also specifically address procedures to be observed for the deletion/destruction of logical or physical data;
- (v) monitoring trends (e.g. increasing frequency of data inconsistencies or data security breaches) which may be symptomatic of fundamental weaknesses within the data systems and controls or indicative of heightened risks of larger system failures; conducting regular reviews and assessments of the overall operation of the data management and MIS framework; and recommending enhancements or corrective measures to senior management to address gaps and deficiencies in the framework; and
- (vi) providing continuous development support, including training, updated user guidelines or manuals, and technical support to users to ensure smooth business operations.

4.9 For larger and more complex institutions, consideration may be given to the establishment of a dedicated data stewardship function which reports to and supports senior management in discharging its responsibilities for effective data management as outlined in paragraph 4.8. Such a function should interact closely with relevant line functions. In other cases, financial institutions may identify existing roles within the organisation to discharge these responsibilities.

4.10 Policies and procedures, including the appropriate approving authority, for effecting changes to data systems should be clearly defined. The policies and procedures should appropriately reflect the significance of specific data systems to critical business functions, with more rigorous controls entrenched for mission-critical systems.

4.11 The deployment of alternative systems which are not aligned to the institution's approved data architecture (see Principle 3) should be subject to specific authorisation at an appropriate senior management level. A technical

BNM/RH/GL_018_1	Prudential Financial Policy Department	Guidelines on Data Management and MIS Framework	Page 7 / 13
-----------------	----------------------------------------	-------------------------------------------------	-------------

assessment by a suitably skilled and objective party should be considered to fully understand the risks to the institution associated with the deployment of such systems.

4.12 Where data is managed by third party vendors under outsourcing arrangements, senior management must ensure that effective oversight, review and reporting arrangements are established to ensure that service level agreements regarding standards on data quality, integrity and accessibility are observed at all times.

**Principle 3: A financial institution's data management and MIS framework should be supported by a comprehensive data and systems architecture that is appropriate to the scale and complexity of the institution's operations.**

4.13 The data and systems architecture defines how data is captured, processed, stored and utilised within the overall data management and MIS framework.

4.14 A comprehensive data and systems architecture should facilitate the proper integration of data and systems across the institution and should generally address the following elements:

- (i) standards<sup>2</sup>, guidelines or common criteria and data definitions<sup>3</sup> to be applied in the development of systems, data repositories and interfaces, and controls over data flows. Such protocols should be designed to ensure that common data and MIS systems are implemented consistently, thereby mitigating the increased cost and risk of fragmented and disconnected flows of data within the organisation;
- (ii) major types and sources of data necessary to support the organisation and a description of the systems in place to capture such data;

<sup>2</sup> E.g. standards applied for fair valuations of collateral and recognition of defaulted loans.

<sup>3</sup> E.g. consistent use of codes and formats for common data items such as customer records and product codes.



BNM/RH/GL_018_1	Prudential Financial Policy Department	Guidelines on Data Management and MIS Framework	Page 8 / 13
-----------------	----------------------------------------	-------------------------------------------------	-------------

- (iii) the database technology employed to support the desired data architecture (see paragraph 4.15 below);
- (iv) administrative structures and protocols for processing and disseminating data throughout the organisation, having regard, among other things, to the organisational objectives, volume of data handled, reporting and management information needs;
- (v) processes and systems for data repository management. The institution should consider relevant legal and regulatory requirements, privacy protection policies or standards, and the need to retain sufficiently detailed information for a defined period to support the institution's internal models and processes used for analysis and decision making; and
- (vi) appropriate data storage and back-up processes that optimise the functioning of data systems and enable efficient and timely access to data for the purpose of business continuity management.

4.15 Financial institutions should ensure that the technology employed for its data systems is capable of transmitting and integrating data across multiple platforms and systems in an efficient manner. This should include the ability to link and aggregate common data records (e.g. specific customer, counterparty, investment rating or product) residing in multiple sources as needed to support the business and risk management functions. In addition, the technology should also allow for the efficient integration between internally developed and external software applications.

**Principle 4: Financial institutions should maintain adequate data quality at all times. Data quality should be assessed and monitored against the institution's data policy statements and objectives on an ongoing basis.**

4.16 Measures and controls put in place by financial institutions should ensure that data generated is accurate, complete, current (i.e. up-to-date for the intended

<b>BNM/RH/GL_018_1</b>	<b>Prudential Financial Policy Department</b>	<b>Guidelines on Data Management and MIS Framework</b>	<b>Page 9 / 13</b>
------------------------	-----------------------------------------------	--------------------------------------------------------	--------------------

purpose)<sup>4</sup>, consistent across systems and the organisation, and supported by clear and unambiguous data descriptions. Senior management, or the data stewardship function where one exists, should define metrics for measuring data quality. The metrics and target performance standards should reflect the institution's desired data objectives as enumerated in the data policy statements endorsed by the board (see paragraph 4.2).

4.17 Processes should be established to support the effective monitoring of data quality on an ongoing basis. This may include, among other things:

- (i) the conduct of data quality assessments at regular intervals, and whenever material changes are made to data systems, architecture or processes;
- (ii) roles assigned to perform the monitoring functions;
- (iii) timely reporting on the outcome of data quality assessments to senior management; and
- (iv) scheduled data quality maintenance activities to enable defects and deteriorations in data quality to be detected and rectified promptly. This may include establishing routine data cleansing<sup>5</sup> and data validation<sup>6</sup> activities.

4.18 Any systematic deterioration observed in data quality should be fully investigated by senior management. The observations, findings and remedial actions proposed and taken to restore data quality should be reported to the board. The report to the board should provide an assessment of the nature and extent of risks posed to the institution from such a deterioration, how these risks are being managed, and the prospects and time needed to restore data quality to the desired level. The board should promptly inform the Bank of any developments that may have a material bearing on the institution's operations, risk profile or financial condition.

<sup>4</sup> E.g. borrower financial details

<sup>5</sup> Data cleansing refers to the process of detecting, removing and/or correcting data that is incorrect, out-of-date, redundant, incomplete or formatted incorrectly from the database.

<sup>6</sup> Data validation refers to the process of ensuring that a program uses data that is accurate, complete or meets the specified criteria.

BNM/RH/GL_018_1	Prudential Financial Policy Department	Guidelines on Data Management and MIS Framework	Page 10 / 13
-----------------	----------------------------------------	-------------------------------------------------	--------------

**Principle 5: Financial institutions should maintain effective controls over data security and privacy to preserve a high level of systems and data integrity.**

- 4.19 Systems and data integrity refers to the reliability of information processed, stored or transmitted both within the institution, and between the institution and its customers or other third parties.
- 4.20 Financial institutions must establish adequate preventive and detective controls to ensure that logical and physical access to systems and data is secure and only available to authorised personnel for specific purposes.
- 4.21 The controls should be commensurate with the criticality and sensitivity of the relevant systems and data handled. In this connection, policies and procedures should be established for the classification of data, having regard to the potential impact that unauthorised access to, or tampering of, data could have on the institution's ability to accurately assess its risk exposures and financial condition, plan and manage its financial resources, preserve individual (including customers') rights to privacy, maintain the institution's competitive position, and fulfill its regulatory reporting obligations.
- 4.22 Similarly, financial institutions should identify critical data systems, generally defined as those systems that, if disrupted or tampered with, would materially impact the institution's business operations, reputation or financial condition. More rigorous controls should be in place for access to data and systems classified as highly sensitive or critical.
- 4.23 Access rights to systems and data should be clearly defined, documented and where appropriate, segregated to prevent critical data or systems from being compromised. Given the sensitivity of the bulk of data handled by financial institutions, access should generally be given on a "need to know" basis.
- 4.24 Employees should not have concurrent access to data files residing in and computer facilities supporting both the production systems and backup systems. Persons given access to backup files or system recovery resources

<b>BNM/RH/GL_018_1</b>	<b>Prudential Financial Policy Department</b>	<b>Guidelines on Data Management and MIS Framework</b>	<b>Page 11 / 13</b>
------------------------	-----------------------------------------------	--------------------------------------------------------	---------------------

should be limited and duly authorised to have access for specific purposes and a specified period only. Any access should be documented and logged for audit purposes.

- 4.25 Access to critical data or systems by external parties (e.g system vendors and service providers) must be properly authorised. Financial institutions must ensure that such access by external parties is closely supervised, monitored and appropriately restricted in line with the purpose of the access given. Legal agreements for services contracted should clearly prohibit the unauthorized disclosure of confidential data by the external party and provide for adequate remedies to the financial institution.
- 4.26 Financial institutions are generally expected to limit manual data manipulations or changes in the institution's day-to-day operations to a minimum level. Where manual intervention is required (e.g. for the purpose of data patching<sup>7</sup>), the interventions should be properly authorized and a historical log maintained for audit purposes.
- 4.27 Appropriate safeguards should be put in place to ensure that personal data is not misused or disclosed in a wrongful manner. Personal information (of customers, employees or any other parties that the financial institution may conduct business with) should be handled properly to ensure confidentiality of the information and compliance with relevant legislation.
- 4.28 To ensure that safeguards and security measures implemented over data and IT systems are effective, financial institutions are encouraged to obtain the MS ISO/IEC 27001:2007 Information Security Management Systems (ISMS) certification for critical systems, particularly the payment and settlement systems.

---

<sup>7</sup> Data patching refers to the process of updating software by comparing the different versions of a software and extracting the differences (e.g. security or features update) between the files. Patching can be done manually on each computer or through an automated system.

BNM/RH/GL_018_1	Prudential Financial Policy Department	Guidelines on Data Management and MIS Framework	Page 12 / 13
-----------------	----------------------------------------	-------------------------------------------------	--------------

**Principle 6: The operation of MIS functions should be effective and robust to enable timely access to critical data for decision-making, analysis and control purposes.**

4.29 The MIS functions and processes must be capable of providing and disseminating up-to-date information to a wide range of users identified as requiring access to data for decision making, analysis or to support the institution's various control, including risk management functions.

4.30 The MIS should be capable of efficiently and effectively transforming data that is tailored to the needs of various users of information within the organisation. Information produced by MIS systems should fulfil the institution's data quality standards, and effectively address specified information needs in terms of its relevance, timeliness and granularity to specific user groups. To achieve this, user requirements should be clearly defined at the outset of the system development stage, and regularly reviewed thereafter to inform subsequent system enhancements.

<b>BNM/RH/GL_018_1</b>	<b>Prudential Financial Policy Department</b>	<b>Guidelines on Data Management and MIS Framework</b>	<b>Page 13 / 13</b>
------------------------	---------------------------------------------------	----------------------------------------------------------------	-------------------------

## **PART C      IMPLEMENTATION**

### **5.      Implementation Requirements**

- 5.1      The board is responsible to ensure that the principles in these Guidelines are observed on an on-going basis in line with the level of sophistication and the needs of the institution, and any deficiencies in the institution's data management and MIS practices are addressed within a reasonable period to be determined by the board.