Policy Statement of the Bank of Thailand

Re: Data Governance

September 27, 2021

BANK OF THAILAND

Issued jointly by:

Regulatory Policy Department 2

Financial Institutions Policy Group

Technology Risk Supervision Department

Payment Systems Policy and Financial Technology Group

Bank of Thailand

Tel: 0-2283-5806, 0-2283-6559

e-mail: FIOP-RPD2@bot.or.th, ITSupervision@bot.or.th

Table of contents

Unofficial Translation

This translation is for the convenience of those unfamiliar with the Thai language

Please refer to the Thai text for the official version

Policy Statement of the Bank of Thailand

Re: Data Governance

---

1. Rationale

Data is an important asset of any financial institution. Therefore, applying the technology to enhance the benefit from employing the data at hand, ranging from general information to financial information of customers that are growing in numbers, has become an important driver in providing financial services in the present time. Financial institutions have employed this data not only for product development and financial services that cater more towards customers' needs but also for executing efficient risk management. All of the stated data usage should be based on strong data protection and having customers' best interests in mind. If financial institutions fail to put in place sufficient data governance and data management, they then post a major risk that could potentially lead to the loss in confidence in the financial system. Therefore, financial institutions should establish the process for data quality assurance and data securities while safeguarding the personal data of customers. This process should be customized to fit the size, business model, complexity and data risk of the financial institutions as well as complying with the relevant regulations and legislations on data governance.

The Bank of Thailand (BOT) encourages financial institutions to use the data in the most efficient way so that financial institutions can improve financial services in a way that would better fit customer needs. At the same time, financial institutions should ensure that suitable data risk management is well-established. With this principle in mind, BOT hence issued this policy statement on data governance as a reference for financial institutions to consult in order to establish their data governance guideline that would be in line with the international standard and to manage data appropriately. Also, BOT hoped that all financial institutions under the

Financial Institutions Business Act would employ this policy statement in conducting data governance in their organizations that would be very beneficial for their business operations. In addition, other businesses that are not financial institutions might also benefit from using this policy statement to set the standard on data governance within their organizations as well.

2. Content

2.1 Definitions

Data[1] is defined as an element that could convey facts not only through the anatomy of the data itself but also through various methods or forms such as messages, statistics or others and can be in the electronic or non-electronic form; for example, customer data, personnel data and business-related data.

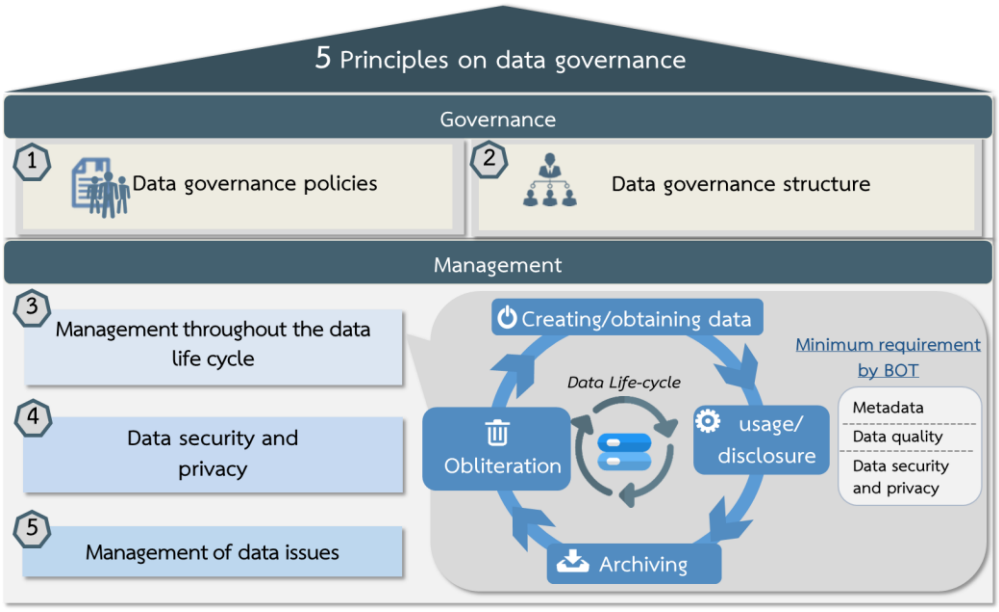
Data risk is defined as the potential risk arising from the data itself or from the usage of data that could affect business operations of financial institutions such as data leakage that could lead to legal prosecution and reputation risk, failure to provide the data that would suit the needs of data users as well as distorted or bad quality data. These risks could lead to distorted or erroneous decisions being made and in turn could result in inefficiency in business operations.

2.2 Principles

BOT hereby set the principles regarding data governance and management of financial institutions to ensure that financial institutions would have at hand the data with high levels of quality, security, privacy and benefits to business operations of financial institutions while upholding the data protection and customers' best interests. The policy statement set by BOT was quite principle-based and financial institutions might exert some discretion in applying these principles so that they would fit with the size, business models, complexity and data risk of financial institutions while providing some flexibility in conducting businesses under such principles.

[1] Based on the definition of "data" according to the Notification of the Committee on Digital Government Development regarding Data Governance for Government.

The policy statement issued by BOT had in total five principles regarding data governance, notably (1) data governance policies, (2) data governance structure based on the three lines of defense principle, (3) management throughout the data life cycle, (4) data security and privacy and (5) management of data issues. Financial institutions should employ these principles as guidelines for data governance in their organizations. For financial institutions who successfully complied with the principles stated in this policy statement, they might consider having additional data governance as well such as providing the report and progress assessment in order to continuously improve upon the existing data governance. In addition, they could also employ technology in order to enhance data governance operations so that they would be in line with the financial institutions' development phases.



2.3 Data governance of financial institutions

Financial institutions should adhere to the following five principles for data governance.

Principle 1 Data governance policies

Financial institutions should prescribe data governance policies that are in line with the size, business models, complexities, and data risk of the financial institutions and communicate the aforementioned policies to employees in the organization to raise awareness and to have them abide by such policies. This could be carried out using the following guidelines.

(1) Data governance policies should be written and documented to cover data governance for all types of data under financial institutions' possession, including the services provided by third parties or related business partners. [2] The policies may be specifically drafted or be an add-on to the existing policies employed already by the financial institutions, but they should at least cover the following issues:

(1.1) Data governance structure, roles and responsibilities of relevant parties should follow the three lines of defense principle along with having a clear segregation of duty and resource management that are suitable and sufficient according to Principle 2.

(1.2) Management throughout the data life cycle ranges from creating and obtaining data, data usage and disclosure, data archiving and data obliteration to being mindful of the potential risks that could have risen during each phase of the life cycle, as detailed in Principle 3.

(1.3) Data security and privacy throughout the data life cycle should be corresponding to the level of data risk and the relevant regulations and legislations, as detailed in Principle 4.

(1.4) Management of data issues is crucial in mitigating the impact from the damage, as detailed in Principle 5.

(2) Data governance policies must be approved by the designated committee and must be reviewed with an appropriate frequency, including when there are significant changes or development.

(3) Data governance policies must be explicated and communicated to all relevant parties and should be formally implemented in the organization for all people to adhere to such policies.

[2] Based on the definition of "third party" from the Notification of Bank of Thailand No. FPG. 21/2562 Re: Regulations on information technology risk supervision of financial institutions (with revised version) and using the definition of "business partners" from the Notification of Bank of Thailand No. FPG. 16/2563 Re: Regulations on the use of services from business partners of financial institutions (with revised version)

<u>Principle 2</u> Data governance structure based on the three lines of defense principle

Data governance structure should be based on the three lines of defense principle to ensure proper control, regulation and auditing and must have a clear segregation of duty as well as resource management that are suitable and sufficient. This could be done through

(1) Designating the personnel and relevant divisions with direct roles and responsibilities for data governance which consists of the following:

Roles and responsibilities for data governance	
1. Oversight committee on data governance	Oversight committee
2. Data administrators 2.1 Senior management level 2.2 Division or team level 3. Officers authorizing data-related operations 4. Data users	1st Line
5. Risk management division 6. Compliance unit	2nd Line
7. Division responsible for data-related operations and data risk management audit	3rd Line

Financial institutions should clearly specify and document the roles and responsibilities of the committee, divisions or personnel responsible for data governance. This is to ensure that the relevant parties are mindful of their own roles and responsibilities (details in Appendix 1). However, financial institutions may consider implementing the data governance structure that is tailor-made to the size, business model, complexity and data risk of financial institutions, providing that there are sufficient personnel and operating divisions to adhere to the duties stated previously and are not in conflict with the auditing principles or the check and balance system put in place. For example, financial institutions may assign the data governance duty to the Technology Committee without having to set up a separate committee specifically for data governance.

(2) Having adequate resources in terms of personnel and tools to support the data governance-related operations, including personnel who are knowledgeable, experienced and specialized in the field. In addition, financial institutions should provide the training and knowledge building exercise on data governance to relevant personnel with means to assess the effectiveness of the training and exercise as well.

(3) Having a plan to continuously raise awareness on data governance for all levels of personnel as well as relevant third parties. The plan should be clear and implemented on a regular basis with means to assess its effectiveness. In addition, the content of the training should be reviewed and revised to ensure that it is still suitable for addressing the current development.

Principle 3 Management throughout the data life cycle

Financial institutions should manage the data throughout its life cycle, from creating and obtaining data, data usage and disclosure, data archiving and data obliteration while being mindful of the potential risks that could have arisen during each phase of the life cycle. Financial institutions should make certain that there is appropriate control in place to ensure that the data within each phase of the life cycle possesses sufficient quality, security and privacy. More specifically, financial institutions should

(1) Create a diagram or documents that would provide the information on how all of the data within the organization is related, ranging from creating and obtaining data, data transfers between operating systems, data usage and disclosure, and data archiving in operating systems or other types of storage media. This is to ensure that financial institutions would be able to manage the data throughout its life cycle and manage in a way that would be in line with the risk and complexity of the data in the organization.

(2) Manage the metadata so that financial institutions can employ the data for the analysis on the relationship and interconnectedness between relevant systems in a complete and accurate fashion (details in Appendix 2).

(3) Put in place the data quality management to ensure that the data is of quality, reliability and applicability to be accurately and appropriately used in the analysis and business decision making while building confidence for data users (details in Appendix 3).

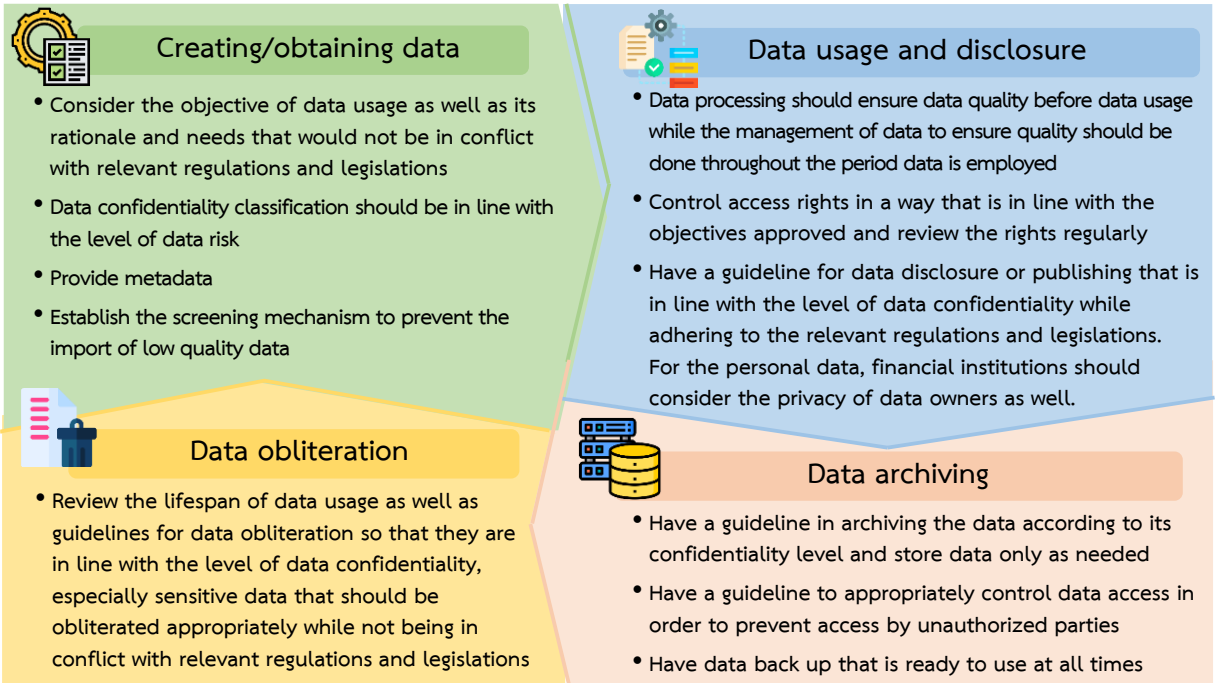
Examples of low quality data and its impact on financial institutions

- ❖ Data is not up-to-date, resulting in the inaccurate analysis
- ❖ Data is not ready to be used, resulting in the interruption of business operations

(4) Monitor and manage data risk throughout its life cycle properly, adhering to the risk management guidelines of the financial institutions. This is to avoid having the potential development of risks that could affect the business operations of the financial institutions.

In addition, in order to ensure efficient data management throughout its life cycle, financial institutions should clearly specify the management process for each phase of the data life cycle so that all relevant parties could and would adhere to. Examples of key points to be considered in specifying the management process during each phase of the data life cycle are as follows.

Key points to be considered for each phase of the data life cycle



<u>Principle 4</u> Data security and privacy

Financial institutions should ensure that the data is well protected and secured while having data privacy throughout the life cycle that is in line with the level of data confidentiality and is in compliance with relevant regulations and legislations, notably

(1) Ensuring that data protection and security are in place and in line with the level of data confidentiality. This implementation should cover data transfers via the communication network, data collection or data usage on the operating system and storage media, data archiving and data obliteration. In addition, it is also relevant under the case where financial institutions employ connection services or data access from external parties. Financial institutions may use the Notification of the Bank of Thailand Re: Regulations on information technology risk supervision of financial institutions[3] or other relevant guiding principles as references regarding data security.

(2) Ensuring data privacy that is in line with relevant regulations and legislations, notably Personal Data Protection Act B.E. 2562. Financial institutions must perform data collection, data usage or personal data disclosure only if necessary and operate within the specified objectives while being mindful of the rights of data owners.

(3) Ensuring that the handling of data complies with the minimum requirement issued by the Bank of Thailand in the Notification of the Bank of Thailand Re: Management for market conduct.[4]

<u>Principle 5</u> Management of data issues

Financial institutions should be prepared for the management of data issues in order to prevent damaging events from occurring or to mitigate the impact if the damage already happened. This includes the following.

(1) Establish a process for monitoring and managing data issues, including detection, identification, containment, root cause determination and analysis, evidence or document collection, problem solving and management to resume normal business operations as well as a process revision to minimize the chance of having the same problem occurring repeatedly in the future. For the case where the

[3] Notification of the Bank of Thailand No. FPG. 21/2562 Re: Regulations on information technology risk supervision of financial institutions (with revision)

[4] Notification of the Bank of Thailand No. SVG2. 4/2563 Re: Management for market conduct (with revision)

problem already affected the continuity of business operations, financial institutions should activate and take action according to their own business continuity plans.

(2) Make preparation for the case of data breach incidents such as data leakage, especially regarding personal data. Financial institutions must report the data breach incident according to the Personal Data Protection Act B.E. 2562. This includes the data breach incident which carries a risk of having a severe impact on individual right and liberty. Under this case, financial institutions must report the data breach incident to the owner of the personal data along with the remedy plan without any delay.

Appendix 1

Roles and responsibilities on data governance following the three lines of defense principle

1. The committee responsible for data governance[5] carries the task of

- Setting data governance target to be in line with the strategic plan of the financial institution
- Ensuring that the data governance implementation, review and policy revision are in place
- Supervising and monitoring data-related operations as well as giving advice and making important data-related decisions
- Providing continuous and comprehensive support as well as reinforcement for data governance
- Overseeing and advocating the communication on data governance for all personnel in the organization in order to raise awareness regarding the importance of data and safe data usage that would lead to good data governance within the organization

2. Data administrators including the senior management and division or team level

2.1 Senior management should play a role in

- Overseeing that data management is executed according to the policy, the standard as well as to the set orders and procedures relating to data governance
- Advocating knowledge building and raising awareness for all personel within the organization

2.2 Division or team level should play a role in

- Implementing data governance as well as reviewing and revising data governance policies, standard and procedures so that they are up-to-date
- Communicating, building knowledge and providing advice regarding the policies, standard and procedures relating to data governance while raising

[5] The committee responsible for data governance may consist of related management positions such as Chief Information Officer, Chief Data Officer, Chief Information Security Officer, Chief Risk Officer or other executives from relevant divisions.

awareness on the importance of data and safe data usage that would lead to good data governance within the organization

- Monitoring the status on data management as well as reporting the outcome, problem or risk found to the committee responsible for data governance oversight on a regular basis

3. Personnel responsible for approving the data-related operations should play a role in

- Approving data-related operations such as data access permission, data usage and data disclosure
- Supervising to ensure that data management is executed according to the policy, the standard as well as to the set orders and procedures relating to data governance such as overseeing the data registratry and review so that it is up-to-date as well as overseeing data confidentiality classification and setting data quality standard

4. Data users should play a role in

- Complying to the policies, standard as well as orders and procedures relating to data governance
- Ensuring that the data governance implementation is in line with the need for data employment and reporting the problem found during the usage of data to the division or team responsible for data management

5. Risk management division should play a role in

- Setting up the risk management framework and process for the financial institution so that they cover all types of data risk as well as encouraging various divisions to perform data risk assessment
- Providing advice, monitoring and reviewing data risk so that it resides within the risk appetite level and compiling and assessing interconnectedness between data risk and other types of risks as well as reporting risk management outcomes to relevant committees

6. Compliance division should play a role in

- Monitoring, providing advice and supervising data-related operations in order to prevent data breach or failure to comply with the data-related regulations and legislations of the regulator

7. Audit division should play a role in

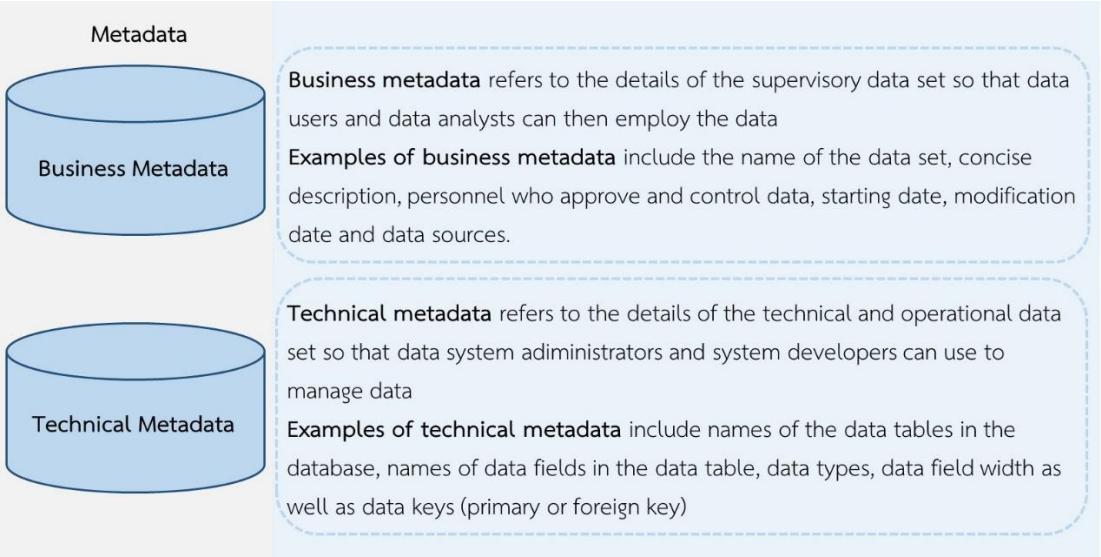
- Auditing the data-related operations and risk management in order to verify with confidence that they are executed according to the policies, standard as well as to the orders and procedures relating to data governance

Appendix 2

Metadata Management

1. Set the standard, orders and procedures on metadata management to address the roles and responsibilities of the relevant parties, the process of creating metadata, supervision and verification of metadata
2. Designate the division or the personnel to be responsible for creating, amending and verifying metadata as well as for revising the metadata registration so that it is up to date
3. Create both the business metadata and the technical metadata covering all of the important data while setting it as a part of the process for information technology system development

Metadata should consist of the following



4. Specify the process for controlling data access, access right and metadata modification to prevent the operational risk or errors from occuring
5. Modify the metadata registration so that it is up to date

Appendix 3

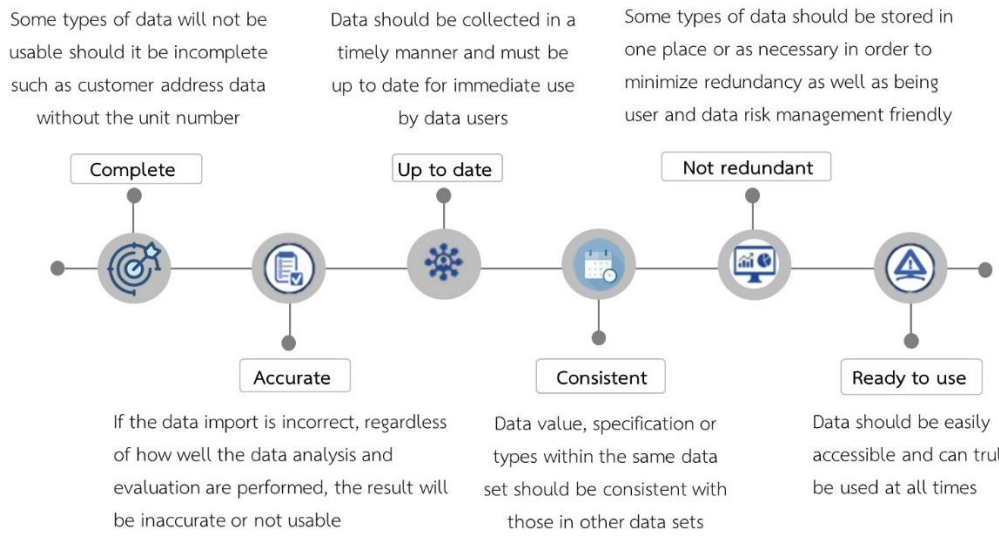
Data quality management

Financial institutions should have data quality management by setting the standard, orders and procedures regarding data management as well as setting up the divisions or personnel responsible for data quality management. In addition, there should be a clear specification on the characteristics of good quality data and the data management process as follows.

1. Specifying the guidelines for data quality

- Specify the critical data elements that must be of quality for each data set
- Specify the data quality level for each data set to be used for data set quality assessment
- Specify the process for controlling the change in the guidelines for data quality as well as the characteristics of good quality data to prevent the operational risk or errors from occuring

Examples of good quality data



Examples of the description from the Notification of Committee on Digital Government Development regarding Data Governance for Government

2. Data quality assessment

- Assess the quality of the data according to the data quality guidelines such as data profiling examination and analysis on critical data element that should be

of quality for each data set and benchmark it with the data quality standard specified by the financial institution

- Prepare data quality assessment results to be used for continuous data quality monitoring
- Have means to identify the data set that fails to meet the data quality standard and to inform the personnel responsible for the data approval and data control in order to formulate the guidelines for corrective actions to improve data quality

3. Data quality improvement

- Have in place a process to improve the data set that fails to meet the quality assessment criteria
- Perform a root cause analysis to prevent the formation of low quality data set in the future
- Specify the vigilant control process for the data quality improvement such as the process regarding the management of changes, approval process by the personnel responsible for granting approval and data supervision and the collection of evidence before and after data modification to prevent the unauthorized data modification

4. Data quality control and monitoring

- Monitor and update the data quality assessment results regularly as a part of a timely monitoring of data quality
- Set up a process or make available an instrument for monitoring data quality level should the data set fail to meet the specified data quality standard
- Perform data quality verification according to the specified guidelines regularly
- Write a report on data quality monitoring including the summary of the progress made on refining the data set which fails to meet the quality assessment criteria. In addition, the emerging risk and issues as well as the overview of the problem and its root causes that make the data set fail to be of quality should be reported to the designated committee or senior management on a regular basis

Example of the data quality management process