IMPLEMENTATION OF INFORMATION TECHNOLOGY BY COMMERCIAL BANKS

This summary intends to provide information for relevant stakeholders. It is not an official translation of the OJK Regulation. All information refers to OJK Regulation (POJK) No. 11/POJK.03/2022.
The information contained in this summary cannot be used for legal purposes. In the event of inconsistencies between this document and the POJK, refer to the POJK as the primary reference.

A. Background

The use of information technology (IT) is required for banks to support the continuity of their business operations and services to the public. Hence, OJK Regulation (POJK) No. 11/POJK.03/2022 regarding the Implementation of Information Technology by Commercial Banks was issued to amend OJK Regulation (POJK) No. 38/POJK.03/2016 and OJK Regulation (POJK) No. 13/POJK.03/2020 in strengthening IT governance to provide added value through the optimization of resources in mitigating risks faced by banks.

B. Key Provisions

General Provisions

1. Commercial banks, hereinafter referred to as Banks, are banks that carry out their businesses conventionally or on the basis of Islamic (Sharia) principles, which include payment transfer services, including branch offices of banks domiciled abroad as well as Sharia business units.
2. Information Technology, hereinafter referred to as IT, is a technique to collect, prepare, store, process, notify, analyze, and/or disseminate information.
3. Electronic System is a set of electronic tools and procedures which function to prepare, collect, process, analyze, store, display, notify, transmit, and/or disseminate electronic information.
4. Data Centre is a facility used for placing an Electronic System and its related components for the purpose of placing, storing, and processing data.
5. Data Recovery Centre is a facility used to restore data or information as well as critical functions of an Electronic System that were disrupted or damaged as a result of natural or man-made disasters.
6. Disaster Recovery Plan is a document that contains plans and measures to replace and/or restore access to the data, hardware, and software required for Banks to carry out their critical business operations after a disruption and/or disaster.

Bank's IT Governance

<u>General</u>

7. Banks are required to apply good IT governance in their IT implementation by weighing the following factors at the very minimum:
   a. strategy and business objectives of the Bank;
   b. the size and complexity of the Bank's business;
   c. the role of IT for the Bank;
   d. IT resources procurement method;

e. IT-related risks and issues;
f. national and international practices or standards; and
g. provisions of the statutory regulations.

8. In applying good IT governance, Banks undertake at least the following:
   a. strategic options evaluation, IT strategic directions implementation, and strategic outcomes monitoring;
   b. the alignment, planning, and organization of all units, strategies, and activities that support the IT implementation;
   c. the definition, acquisition, and implementation of IT solutions and their integration into the Bank's business processes;
   d. the provision of IT operational support services to stakeholders; and
   e. monitoring the performance and suitability of the IT implementation with the internal performance targets, internal control, and the provisions of the statutory regulations.
9. Good IT governance applies to all IT management units and/or functions and IT users at the Bank.
10. In implementing IT governance, Banks are required to synergistically outline, plan, and/or set at least the following aspects:
    a. business process;
    b. organizational structure;
    c. policies, standards, and procedures;
    d. needs and flow of information supporting the business processes;
    e. supporting human resources;
    f. IT culture; and
    g. infrastructure and applications.
11. Banks are required to implement policies, standards, and procedures consistently and continuously as well as to conduct periodical reviews and updates as referred to in Point 10 Letter c.

<u>Implementation of Bank's IT Governance</u>

12. Banks are required to establish clear authorities and responsibilities of the Board of Directors, Board of Commissioners, and officials for each position related to the implementation of IT governance.
13. The authorities and responsibilities of the Board of Directors are to include at least:
    a. establishing an IT strategic plan;
    b. establishing adequate policies, standards, and procedures on the implementation and use of IT as well as communicating them effectively to working units and end-users; and
    c. evaluating the strategic objectives, directing Bank's executive officers, and monitoring all IT implementation activities to ensure:
       i. implementation of IT governance is in line with the Bank's needs and characteristics;
       ii. effectiveness and efficiency of the overall IT implementation to deliver optimal benefits for the Bank;
       iii. effective risk management processes in IT implementation;

iv. availability of adequate resources for IT implementation to effectively and efficiently support the Bank's business; and
v. stakeholders' support and engagement in IT governance implementation.

14. The authorities and responsibilities of the Board of Commissioners are to include at least:
    a. evaluating, directing, and monitoring the IT strategic plan and IT governance plan; and
    b. evaluating, directing, and monitoring the implementation of IT governance.
15. Banks are required to have an IT steering committee responsible for giving recommendations to the Board of Directors pertaining to at least:
    a. IT strategic plan in line with the Bank's corporate plans;
    b. IT policies, standards, and procedures;
    c. compatibility between the IT development plan and the IT strategic plan;
    d. compatibility between the actual IT development and the plan;
    e. evaluation of IT's cost-effectiveness in achieving the benefits as planned;
    f. monitoring of IT's performance and measures to improve the IT's performance;
    g. measures to resolve IT-related issues that cannot be addressed by the IT users and IT management working units in an effective, efficient, and timely manner; and
    h. adequacy and allocation of IT-related resources owned by the Bank.
16. The IT steering committee consists of at least:
    a. the director in charge of the IT implementation working unit;
    b. the director in charge of the risk management working unit;
    c. the highest-level official leading the IT implementation in the working units; and
    d. the highest-level official leading the IT user work unit.
17. The IT steering committee is chaired by one of the Bank's directors who also serves as a committee member.
18. Banks are required to have an IT implementation working unit responsible for IT management, at least for the following activities:
    a. planning;
    b. design or development;
    c. operation; and
    d. monitoring

    of IT implementation activities.
19. IT management activities as referred to in Point 18 are carried out in line with the directions set by the Board of Directors to achieve the Bank's business objectives.

Bank's IT Architecture

Preparation of the Bank's IT Architecture

20. IT Architecture is a strategic documentation of the Bank's IT resources that are organized and integrated to achieve and support the Bank's business objectives. IT architecture includes, among others, data, applications, and technology.

21. Banks are required to have an IT architecture that considers at least the following factors:
    a. the bank's vision and mission;
    b. the bank's corporate plan;
    c. the bank's business processes and capabilities;
    d. IT governance;
    e. the bank's principles of data management, applications, and technology;
    f. the size and complexity of the Bank's business;
    g. capacity of bank's capital;
    h. national and international standards application; and
    i. provisions of the statutory regulations.
22. The IT architecture is prepared comprehensively to include the following processes:
    a. planning;
    b. design;
    c. implementation; and
    d. control
23. In the event of any changes in the factors as referred to in Point 21, the Bank is required to update its IT architecture.

Preparation of the Bank's IT Strategic Plan

24. Banks are required to have an IT strategic plan that supports the Bank's corporate plan, and is designed for a long-term IT implementation in accordance with the period of the Bank's corporate plan.
25. Banks are required to submit the IT strategic plan as referred to in Point 24 to the Financial Services Authority (OJK) no later than the end of November in the year before the initial period of the IT strategic plan begins.
26. In the event of any conditions that significantly affect the Bank's IT goals and strategies as outlined in the ongoing IT strategic plan, the Bank may make changes to the IT strategic plan.
27. Banks are to submit the changes to the IT strategic plan as referred to in Point 26 to the OJK at any time within the IT strategic plan period as referred to in Point 24.

The Implementation of Bank's IT Risk Management

General

28. Banks are required to apply integrated effective risk management in the IT implementation at every stage of IT implementation by carrying out at least the following processes:
    a. risk identification;
    b. risk measurement;
    c. risk monitoring; and
    d. risk control
29. Banks are required to ensure the adequacy of their risk management information system in the IT implementation.

Information Security for the Bank's IT Implementation

30. Banks are required to ensure that information security is carried out effectively and efficiently in the aspects of human resources, processes, technology, and physical or environmental for the overall IT implementation.
31. The implementation of information security is carried out based on the risk assessment on the information held by the Bank.
32. Banks are required to ensure that the communication network provided by the Bank meets the principles of confidentiality, integrity and availability.
33. Banks are required to have a Bank Disaster Recovery Plan and ensure that the plan can be implemented, thus the Bank can continue its operations in the event of a disaster and/or disruption to the Bank's IT facilities.
34. Banks are required to conduct a testing of the Disaster Recovery Plan on all the critical applications and infrastructure based on the business impact analysis, at least 1 (one) time in 1 (one) year with the involvement of the IT users.
35. Banks are required to review the Disaster Recovery Plan at least 1 (one) time in 1 (one) year.
36. Conventional commercial banks that have sharia business units are required to have a system that can produce separate reports for the activities of sharia business units.

Bank Cyber Security and Resilience

37. Banks are required to maintain cyber-security by carrying out at least the following:
    a. identification of assets, threats, and vulnerabilities;
    b. asset protection;
    c. cyber incident detection; and
    d. cyber incident response and recovery
38. Banks are to ensure that the process for maintaining cyber resilience as referred to in Point 37 is supported by an adequate cyber resilient information system.
39. Banks are required to conduct an annual self-assessment of their cyber security maturity level as per the end of December position.
40. Banks may update their self-assessment of the cyber security maturity level at any time when necessary.
41. Banks are required to submit the results of their self-assessment of the cyber security maturity level as referred to in Point 39 to the OJK as part of their report on the current condition of the Bank's IT implementation.
42. Banks are required to conduct cyber-security testing based on using scenario-based and vulnerability analyses.
43. Cyber-security testing based on vulnerability analysis must be carried out periodically and reported to the OJK as part of the report on the current condition of the Bank's IT implementation.
44. Cyber-security testing based on scenarios must be carried out at least 1 (one) time in 1 (one) year.
45. The scenario-based cyber-security testing includes at least:
    a. setting the test objectives, scope, and scenarios;
    b. execution of the test;

c. evaluation of the test results; and
d. assessment of the effectiveness of the Bank's mitigation, response, and recovery actions against cyber attacks.

46. Banks are required to submit a report on the results of scenario-based cyber security testing to the OJK no later than 10 (ten) working days after the cyber security testing is completed, to include at least:
    a. summary of the test implementation;
    b. lessons learned or observations from the test results; and
    c. plans or improvements that have been made.
47. Banks are required to establish a unit or function in charge of handling the Bank's cyber-security and resilience which is independent of the IT management function.

The Use of IT Service Providers in the Bank's IT Implementation

48. Banks may use IT service providers in their IT implementation.
49. Banks that use IT service providers as referred to in Point 48 must have the capacity to supervise the implementation of the Bank's activities delivered by the IT service providers.
50. Banks are required to have policies and procedures for the use of IT service providers as referred to in Point 48 to include at least:
    a. the process of identifying the needs for using an IT service provider;
    b. the process of selecting the IT service provider;
    c. the procedures for establishing cooperation with the IT service provider;
    d. the risk management process in using the IT service provider; and
    e. the procedures for evaluating the performance and compliance of the IT service provider.
51. Banks in identifying the need to use IT service providers as referred to in Point 50 Letter a, must perform at least the following:
    a. examine the capacity of the prospective IT service provider; and
    b. develop the criteria for the required IT service provider.
52. Banks, in selecting the IT service providers as referred to in Point 50 Letter b, are to asses at least:
    a. the qualifications and competencies of the IT service provider, including their human resources;
    b. performing the cost-benefit analysis by engaging the Bank's IT implementation working unit;
    c. prudential principles and risk management; and
    d. the principle of arm's length transaction if the IT service provider is a related party of the Bank.
53. Banks, in entering into cooperation with the IT service provider as referred to in Point 50 Letter c, are required to have a cooperation agreement with the IT service provider, considering at least:
    a. the qualifications and competencies of human resources of the IT service provider;
    b. the commitment of the IT service provider in maintaining data confidentiality and/or information of the Bank and of the Bank's customers;

c. the commitment of the IT service provider to submit the results of periodic IT audits conducted by an independent auditor on the provision of IT services to the Bank;
d. the transferring of some activities, or subcontracting, by the IT service provider is carried out upon the approval of the Bank as evidenced by a written document;
e. the mechanism for reporting critical incidents by the IT service provider to the Bank;
f. the mechanism for terminating cooperation agreement if a termination is made before the term of the agreement ends;
g. compliance with the provisions of the statutory regulations on the provision of IT services by the IT service provider;
h. the willingness of the IT service provider to meet the obligations and/or requirements specified in the cooperation agreement; and
i. the willingness of the IT service provider to provide access for the OJK and/or other authorized parties to conduct inspections of the provision of IT services in accordance with the provisions of the statutory regulations.

54. The risk management process for using IT service providers as referred to in Point 50 Letter d includes:
    a. the responsibility of the Bank in implementing risk management for using an IT service provider;
    b. the availability of a properly-tested and adequate Disaster Recovery Plan; and
    c. the establishment of data and/or information security requirements in the internal policies and procedures as well as in cooperation agreements.
55. Banks, in assessing the performance and compliance of the IT service providers as referred to in Point 50 letter e, are to consider at least:
    a. the regular monitoring and evaluation of the reliability of the IT service provider regarding performance, the reputation of the IT service provider, and continuity of service provision;
    b. an adequate implementation of IT controls by the IT service provider, as evidenced by the results of audits and/or assessments conducted by the independent parties; and
    c. the level of service provided in accordance with the service level agreement between the Bank and the IT service provider.
56. In the event of any significant changes to the organization of the IT service provider, the Bank is required to reassess the materiality of the IT service provider.
57. In the event of any of the following conditions:
    a. the results of the materiality reassessment referred to in Point 56 indicate that the IT service provider could potentially deliver an ineffective performance;
    b. a decline in the IT implementation performance by the IT service provider that could potentially cause and/or result in a significant impact on the Bank's business activities and/or operations;
    c. the IT service provider becomes insolvent, goes into liquidation, or is declared bankrupt by the court;
    d. the IT service provider violates the provisions of the statutory regulations on Banking secrecy and/or customer personal data;

e. conditions that make the Bank unable to provide the data required for OJK supervision; and/or
f. other conditions that disrupt or halt the provision of IT services from the IT service provider to the Bank,

Banks are required to take certain measures.

58. Certain measures as referred to in Point 57 include at least:
    a. reporting to the OJK in no later than 3 (three) working days after any condition as referred to in Point 57 is known by the Bank;
    b. deciding the follow-up actions to be taken to address the problem, including terminating the use of the IT service provider, if necessary; and
    c. reporting to the OJK in no later than 3 (three) working days after the Bank terminates the use of the IT service provider before the term of the agreement ends, in the event that the Bank decides to stop using the IT service provider.
59. In the event that the use of an IT service provider or planning of the use of an IT service provider causes or is indicated to cause difficulties in the supervision conducted by the OJK, the OJK may:
    a. instruct the Bank to terminate the use of the IT service provider before the term of the agreement ends; or
    b. refuse the plan to use the IT service provider for the Bank.
60. In the event that the Bank will terminate the use of its IT service provider, the Bank must:
    a. prepare a plan to terminate the use of the IT service provider;
    b. assess the service continuity and data related to the activities assigned to the IT service provider as well as the testing or simulation of the Bank's continuity on the business activities and/or operations; and
    c. ensure that the termination of the use of the IT service provider does not cause a disruption to the Bank's business activities and/or operations.

Placement of the Electronic Systems and IT-Based Transaction Processing

<u>The Placement of Electronic Systems</u>

61. Banks are required to place their Electronic Systems in Data Centers and Disaster Recovery Centers in Indonesia.
62. Banks may place their Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia upon obtaining authorization from the OJK.
63. The criteria for Electronic Systems that can be placed in Data Centers and/or Disaster Recovery Centers outside Indonesia as referred to in Point 62 include:
    a. The Electronic System is used to support an integrated analysis in order to comply with the regulations issued by the authority of the Bank's country of origin, which have a global nature, including cross-border;
    b. The Electronic System is used for integrated risk management with the Bank's head office or main office or main entity office outside Indonesia;
    c. The Electronic system is used to implement an integrated implementation of anti-money laundering and counter-financing of terrorism (AML/CFT) with the Bank's head office or main office of the Bank outside Indonesia;

d. The Electronic System is used to deliver services to global customers, which require an integration with the Electronic Systems owned by the Bank's group outside Indonesia;
e. The Electronic system is used for communication management between the Bank's head office and branch offices, or between subsidiary companies and parent company; and/or
f. The Electronic system is used for the Bank's internal management.

64. In the event of conditions that significantly disrupt the Bank's operations, OJK may determine regarding the placement of the Bank's Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia using criteria other than those referred to in Point 63 on a temporary basis.
65. Examples of conditions that significantly disrupt the Bank's operations include the cessation of work or services from the IT service provider and there are no other IT service providers in Indonesia that can provide similar work or services.
66. Before the placement period for Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia expires, the Bank conducts an evaluation to determine the availability and reliability of the Electronic System providers in Indonesia.
67. Banks may apply for an authorization as referred to in Point 62, provided that they:
    a. meet the regulatory provisions on the use of IT service providers in IT implementation;
    b. submit the results of the country risk analysis;
    c. ensure that the placement of the Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia does not diminish the effectiveness of OJK's supervision as demonstrated by a statement letter;
    d. ensure that information regarding the Bank's confidentiality is only disclosed on the condition that such disclosure complies with the provisions of the statutory regulations in Indonesia, as evidenced by the cooperation agreement between the Bank and the IT service provider;
    e. ensure that the written agreement with the IT service provider contains a choice of law clause;
    f. submit a no-objection letter from the supervisory authority of the IT service provider outside Indonesia that OJK can conduct inspections on ~~of~~ the IT service provider;
    g. submit a statement letter that the Bank shall periodically submit the results of assessments conducted by the bank office(s) outside Indonesia on the application of risk management on the IT service provider;
    h. ensure that the placement plan of the Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia delivers more benefits than the costs for the Bank;
    i. submit the Bank's plan to improve the Bank's human resources capacity, both in IT implementation and in business transactions or products offered; and
    j. submit an action plan for placing the Electronic Systems in Data Centers and/or Disaster Recovery Centers in Indonesia for Banks that will place their

Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia as referred to in Point 64.

68. OJK grants or rejects the applications for an authorization to place the Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia as referred to in Point 62 no later than 3 (three) months after all the requirements are met by the Bank and completed application documents have been received by OJK;
69. Banks are required to ensure that the data used in the Electronic Systems placed in Data Centers and/or Disaster Recovery Centers outside Indonesia are not used for purposes other than those referred to in Point 63 and Point 64;
70. In the event that OJK's assessment indicates that the placement of Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia:
    a. is not in line with the application for an authorization submitted to the OJK to place the Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia;
    b. could potentially diminish the effectiveness of OJK's supervision;
    c. could potentially have a negative impact on the Bank's performance; and/or
    d. is not in accordance with the provisions of the statutory regulations,

    OJK may require Banks to place their Electronic Systems in Data Centers and/or Disaster Recovery Centers in Indonesia.
71. Banks are required to ensure that the Data Centers and Disaster Recovery Centers as referred to in Point 61 to 64 ensure the continuity of the Bank's business.

IT-Based Transaction Processing

72. Banks are required to process IT-based transactions within the Indonesian territory.
73. The processing of IT-based transaction can be performed by the IT service providers in Indonesia.
74. The processing of IT-based transactions by the IT service providers as referred to in Point 73 can be carried out provided that they:
    a. comply with the prudential principle;
    b. comply with the regulatory provisions on the IT service providers in IT implementation; and
    c. take heed of consumer protection.
75. The processing of IT-based transactions by the IT service providers outside Indonesia can be carried out provided that the Bank has obtained authorization from OJK.
76. Banks may apply for an authorization as referred to in Point 75 on the condition that:
    a. Banks meet the requirements as referred to in Point 74;
    b. the supporting documents for financial administration for transactions conducted at the Bank offices in Indonesia are administered at the Bank offices in Indonesia; and
    c. The Bank's business plan demonstrates efforts to increase the Bank's role in developing Indonesia's economy.

77. OJK grants or rejects the applications for an authorization on the processing of IT-based transactions by the IT service providers outside Indonesia as referred to in Point 75 no later than 3 (three) months after all the requirements are met by the Bank and completed application documents have been received by OJK.

Procedures to Apply for an Authorization and the Deadline for Implementation After the Authorization is Obtained

78. The applications for an authorization on the placement of Electronic Systems in Data Centers and/or Disaster Recovery Centers and the Process of IT-based transaction by the IT service providers outside Indonesia are submitted online to OJK through OJK's integrated licensing and registration system;
79. Banks must:
    a. place the Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia; and/or
    b. implement the IT-based transaction processing by IT service providers outside Indonesia.

    no later than 6 (six) months after obtaining authorization from OJK.
80. If Banks do not implement the provisions as referred to in Point 79 within 6 (six) months from the time when the authorization is obtained from the OJK, such authorization will become invalid.

Data Management and Protection of Personal Data in Bank IT Implementation

Data Management by Banks

81. Banks are required to effectively manage their data in the Bank's data processing to support the achievement of the Bank's business objectives, by considering at least:
    a. data ownership and stewardship;
    b. data quality;
    c. data management system; and
    d. supporting resources for data management

Personal Data Protection by Banks

82. Banks are required to implement the principles of personal data protection in processing personal data.
83. In the event of certain conditions that could potentially increase the risks for the personal data owner, Banks are required to carry out an impact assessment on the implementation of the personal data protection principles.
84. In implementing personal data protection in data sharing activities, Banks are required to specify at least:
    a. the classification of data which constitutes personal data;
    b. the rights and obligations of the parties involved in sharing the personal data;
    c. personal data sharing agreement;
    d. medium of personal data sharing; and
    e. personal data security.

85. The personal data sharing as referred to in Point 84 is carried out by obtaining the approval of customers and/or potential customers in compliance with the provisions of the statutory regulations.

Provision of IT Services by Banks

86. Banks can only provide IT services to other financial institutions which are:
    a. supervised by OJK; and/or
    b. outside Indonesia where supervision is carried out by the local supervisory and regulatory institution of financial institutions.
87. Banks that will provide IT services as referred to in Point 86, must:
    a. meet the requirement that the provision of IT services does not become one of the Bank's main activities;
    b. comply with the prudential principle;
    c. weigh the cost-benefit analysis;
    d. comply with the arm's length principle of transactions; and
    e. comply with the provisions of the statutory regulations.
88. Banks are required to obtain authorization from OJK for any plans to provide IT services as referred to in Point 86.
89. IT services provided to financial institutions other than banks in the form of applications can be delivered on the condition that:
    a. the financial institutions that use the IT services are in the same group or conglomeration with the Bank; and
    b. the use of the application is intended to support general operational activities.
90. The application for authorization as referred to in Point 88 is submitted online to the OJK through OJK's integrated licensing and registration system.
91. Banks must implement the plan to provide IT services as referred to in Point 88 in no later than 6 (six) months after obtaining authorization from OJK.
92. If the Bank does not implement the plan to provide IT services as referred to in Point 88 within 6 (six) months from the time when the authorization is obtained from the OJK, the authorization will become invalid.

The Internal Control and Internal Audit in the Bank's IT Implementation

Bank's Internal Control in IT Implementation

93. Banks are required to implement an effective internal control system in IT implementation, which includes at least:
    a. oversight by the management and implementation of a culture of control;
    b. risk identification and assessment;
    c. control of activities and segregation of functions;
    d. information system, accounting system, and communication system support; and
    e. monitoring activities and corrective actions for any divergence, carried out by the operational working unit, internal audit work unit, and other parties.
94. The information system, accounting system, and communication system as referred to in Point 93 Letter d must be supported by adequate technology, human resources and organizational structure of the Bank.

95. Activities to monitor and correct divergence as referred to in Point 93 Letter e are to include at least:
    a. ongoing monitoring activities;
    b. implementation of an effective and holistic internal audit function; and
    c. correction of the identified divergence.

Internal Audit in the Implementation of IT

96. Banks must carry out an effective and holistic IT internal audits in accordance with OJK Regulations on the implementation of internal audit function for commercial banks.
97. Ensuring the effective and holistic implementation of IT internal audits, Banks are required to ensure the availability of audit trails of all IT implementation activities for the purposes of supervision, law enforcement, dispute resolution, verification, testing and other inspections.
98. In the event that a Bank uses the services of an external party to perform IT internal audits, the use of such external services is carried out in accordance with OJK Regulations on the implementation of internal audit function for commercial banks.
99. Banks are required to carry out internal audits of IT implementation in accordance with the needs, priorities, and risk analysis of IT implementation, at least 1 (one) time in 1 (one) year.
100. Banks are required to have guidelines for internal audits on IT implementation.
101. Banks are required to review the internal audit function of IT implementation at least 1 (one) time in 3 (three) years using the services of an independent external party.
102. Banks are required to submit to the OJK:
    a. the results of the review as referred to in Point 101 as part of the report on the results of the review by an independent external party; and
    b. IT internal audit results as part of the implementation report and the main outcomes from the internal audits

    in accordance with OJK Regulation (POJK) regarding the implementation of internal audit function for commercial banks.

Reporting

IT Implementation Report

103. Banks are required to report their IT development plan that will be implemented in the next 1 (one) year no later than the end of November before the year the IT development plan is implemented.
104. Banks may make changes to the IT development plan that has been submitted as referred to in Point 103 a maximum of 1 (one) time, no later than the end of June of the prevailing year.
105. Banks may submit changes to the IT development plan outside the period referred to in Point 104 provided that certain considerations are met and approval from OJK has been obtained.

106. OJK may require Banks to make the changes in the IT development plan as referred to in Point 104.
107. Banks are required to report the current condition of the IT implementation in no later than 15 (fifteen) working days after the end of the reporting year.

Incident Report

108. In the event of an IT incident (in the form of cyber incidents and non-cyber incidents) that could potentially lead to and/or has resulted in significant losses and/or has disrupted the Bank's operation, Banks are required to submit:
    a. an early notification in no later than 24 (twenty-four) hours after the IT incident is known; and
    b. IT incident report in no later than 5 (five) working days after the IT incident is known.
109. The early notification as referred to in Point 108 Letter a is submitted in writing via electronic platform to the OJK based on the initial information available.
110. The IT incident report as referred to in Point 108 Letter b is part of a report on conditions that could potentially cause significant losses to the Bank's financial condition in accordance with:
    a. OJK Regulation (POJK) regarding the implementation of risk management for commercial banks; or
    b. OJK Regulation (POJK) regarding the implementation of risk management for sharia commercial banks and sharia business units.
111. In the event of another regulatory authority requiring the submission of early notification and/or IT incident report within a period that is shorter than the timeframe as referred to in Point 108, Banks are required to submit early notification and/or IT incident report to the OJK at the same time as when required by the provisions of the statutory regulations governing the other authority concerned.
112. Banks that have submitted early notification and/or IT incident report as referred to in Point 111 are considered to have complied with the provisions referred to in Point 108 Letter a and/or Letter b.

Realization Report of Bank's IT Implementation

113. Banks are required to submit reports on the realization of:
    a. placement of the Electronic Systems in Data Centers and/or Disaster Recovery Centers outside Indonesia;
    b. the process of IT-based transaction processing outside Indonesia; and/or
    c. the activities as an IT service provider.
114. The realization report as referred to in Point 113 is submitted no later than 3 (three) months after implementation.

Procedures of Report Submission

115. Banks are required to submit reports of:
    a. scenario-based cyber security test results;

b. IT development plan
c. current condition of IT implementation
d. IT incidents; and/or
e. realization

online through the OJK reporting system.

116. The procedures for submitting reports online are in conformity with the bank's reporting through the OJK's reporting system.

Assessment of Bank's Digital Maturity

117. Banks are required to conduct a self-assessment of the Bank's digital maturity level on a regular basis, at least 1 (one) time in 1 (one) year.
118. The Bank's digital maturity level considers all aspects of IT implementation.
119. Banks are required to submit a report on the results of self-assessment of the Bank's digital maturity level as part of the report on the current condition of the Bank's IT implementation.

Closing Provisions

120. Banks are required to implement the provisions on:
    a. self-assessment of cyber security maturity level;
    b. cyber security testing based on vulnerability analysis;
    c. scenario-based cyber security testing; and
    d. self-assessment of the Bank's digital maturity level;

    for the first time after being stipulated by OJK.

121. When this OJK Regulation (POJK) comes into force, the implementing provisions of POJK No. 38/POJK.03/2016 regarding the Implementation of Risk Management in the Use of Information Technology by Commercial Banks as amended by POJK No. 13/POJK.03/2020 on the Amendments to POJK No. 38/POJK.03/2016 regarding the Implementation of Risk Management in the Use of Information Technology by Commercial Banks shall remain valid provided that they are not contrary to the provisions in this POJK.
122. When this OJK Regulation (POJK) comes into force, POJK No. 38/POJK.03/2016 regarding the Implementation of Risk Management in the Use of Information Technology by Commercial Banks as amended by POJK No. 13/POJK.03/2020 on the Amendment to POJK No. 38/POJK.03/2016 regarding the Implementation of Risk Management in the Use of Information Technology by Commercial Banks shall be revoked and declared null and void.

***