

OJK Regulation No. 11/POJK.03/2022 on the Implementation of Information Technology by Commercial Banks <sup>P1</sup>

## OJK Regulation No. 11/POJK.03/2022 on the Implementation of Information Technology by Commercial Banks

In response to the advancement and innovative use of IT in the banking industry to provide financial services, Otoritas Jasa Keuangan (OJK) released regulation No. 11/POJK.03/2022 regarding the Implementation of IT by Commercial Banks (*Penyelenggaraan Teknologi Informasi Oleh Bank Umum*, referred to herein as the “POJK PTI”) on 7 July 2022. The POJK PTI will come into effect on 7 October 2022 and will replace OJK regulation No. 38/POJK.03/2016 regarding the Application of Risk Management in the Use of IT by Commercial Banks.

The POJK PTI aims to provide guidelines on the IT aspects that need to be fulfilled by banks, and aims to increase the maturity level of digital banking by enforcing good IT governance that supports the banks’ business objectives.

### What’s new in the POJK PTI

#### **Cyber Security and Resilience**

Banks must ensure cyber security resilience. At the minimum, banks must perform the following:

- a. Asset, threat, and vulnerability identification;
- b. Asset protection;
- c. Cyber incident detection; and
- d. Cyber incident response and recovery.

To achieve the above, banks need to establish **independent cyber security and resilience functions** that are independent from the IT management functions.

Furthermore, regular assessments will be required to be conducted, which are:

- a. Performing a **cyber security maturity level** assessment on an annual basis. This assessment can be performed in the form of a self-assessment and must cover the end-of-year period in December. The result must be submitted to OJK as part of the regular report regarding banks’ IT operation.
- b. Performing **cyber security testing** through:
  - 1) **Vulnerability Assessment and Penetration Testing (VAPT)**
    - Must be performed on a regular basis.
    - The testing result is reported as part of the report of the current condition of the bank’s IT operation.

- 2) **Scenario-based testing** (e.g., cyber incident response, table-top exercise, and red teaming)
  - Must be performed at least once a year;
  - The assessment result is reported to OJK no more than ten working days after the assessment has been completed; and
  - The scope of work should include, at minimum: objective, scope, and scenarios; testing execution; test evaluation; and assessment of the effectiveness of cyber incidents' mitigation, response, and recovery processes.

Each bank's cyber security maturity level assessment must include a comprehensive analysis, including analysis of the cyber testing results.  
(Ref: Article 21-27)

### **Data Governance**

Banks must ensure effective data governance is in place, which considers at the minimum: data ownership and governance, data quality, data management systems, and supporting data governance resources.  
(Ref: Article 43)

### **Personal Data Protection**

Banks shall uphold personal data protection principles in personal data processing activities. Should any condition potentially raise the risk towards a data subject, banks are required to perform a Data Protection Impact Assessment (DPIA).

In implementing personal data protection on data transfer, banks must determine at the minimum:

- a. Personal data identification and classification;
- b. Rights and obligations of the parties involved in personal data transfer;
- c. Agreements of personal data transfer;
- d. Method of personal data transfer; and
- e. Personal data security.

Data transfer must be performed according to customers'/potential customers' consent, as regulated by law.  
(Ref: Article 44-45)

### **IT Architecture**

In building IT architecture, banks must at least consider several factors, e.g., data, application, and technology management principles, as well as related laws, such as the law of information and electronic transactions.  
(Ref: Article 11)

### **IT Strategic Plan**

Banks are required to have an IT strategic plan which should be prepared for long-term IT implementation and which supports the banks' corporate plans. The IT strategic plan is to be submitted to OJK no later than the end of November of the year before the initial period in which the IT strategic plan begins. Changes made to the IT strategic plan can be submitted at any time during the period.

Banks may make amendments to the IT strategic plan in the event where the conditions significantly affect the banks' IT goals and strategies in regard to the ongoing IT strategic plan.  
(Ref: Article 12-13)

### **Use of IT Services**

Banks may use external IT service providers to support their IT operations: e.g., the use of cloud computing services as Data Centres (DC) and/or as Disaster Recovery Centres (DRC). Furthermore, banks are required to prepare working agreements which, at the minimum, address the following clauses:

- a. Commitment of the IT service provider to protect the bank and customer data and information privacy;

- b. Commitment of the IT service provider to submit the results of periodic IT audits conducted by independent auditors on IT services provided to the banks;
- c. A reporting mechanism of critical incidents by IT service providers to the banks;
- d. Willingness of the IT service provider to provide access to OJK and/or other authorised parties, to conduct inspections of the IT service activities provided in accordance with the laws and regulations.

*(Ref: Article 29-30)*

### **Electronic System and IT-based Transaction Processing Placement**

Banks are required to place their electronic systems at DC and DRC in the territory of Indonesia. Banks that wish to place their systems offshore (outside of Indonesia) will need to obtain permission from OJK, as well as meeting the following systems criteria:

- a. Supporting integrated analysis;
- b. Integrated risk management;
- c. Integrated implementation of anti-money laundering and prevention of terrorism financing;
- d. Customer service integration to provide services to customers globally;
- e. Communication management between the banks' head office and branch offices; and
- f. Internal management of the banks.

*(Ref: Article 35)*

### **Other Provisions**

There are several other provisions which are worth mentioning, such as:

- a. The **IT Internal audit function** is to be reviewed by an independent external party once every three years, at the very least. Documentation required to be submitted to OJK includes:
  - 1) Results of the review as part of the independent external party review report; and
  - 2) Complete IT internal audit results as part of the implementation and internal audit results report, in accordance with OJK regulation regarding the implementation of the internal audit function for commercial banks. *(Ref: Article 55)*
- b. **Implementation of IT risk management**, in which banks are required to have a disaster recovery plan (DRP) and to perform testing of the DRP on all critical applications and infrastructure, in accordance with the business impact analysis, at least once a year, involving IT users. *(Ref: Article 18)*
- c. **Self-assessment to determine the bank's digital bank maturity level**, to be conducted by reviewing all IT management aspects regulated in the POJK PTI, at least once a year. The result is to be submitted, as part of the report on the current condition of the Bank's IT operations, to OJK. *(Ref: Article 66)*
- d. **Adjusted policies, standards, and procedures, as well as risk management guidelines** for IT implementation, at most six months after the validity of the OJK regulation. *(Ref: Article 67)*

### **Sanctions**

Incompliance with the requirements of this regulation may result in administrative sanctions, which include written warnings, fines, temporary suspension of activities, and a decreased score of governance factors in the assessment of soundness level.

## Key Takeaways

Many banks will be faced with revisiting how they manage compliance with the POJK PTI, not only to increase its effectiveness and reduce cost but redefine what is possible for compliance while doing more with less. This will result in unprecedented change and opportunities where fit-for-future, technology-enabled and efficient compliance functions will no longer be optional, but a requirement to remain not only competitive but operational and positioned for future success.

- a. There are major changes according to which banks are required to adjust their internal policies and procedures by April 2023:
  - 1) Establishing an independent cyber security function and regular cyber security testing.
  - 2) Establishing a data governance and data privacy mechanism. This can be approached by:
    - Identifying sensitive data/information;
    - Governing the steps to manage the data lifecycle – from the creation/acquiring of data to the disposal of data; and
    - Defining the processes and technologies for appropriate data protection.
  - 3) Developing a comprehensive IT architecture.
  - 4) Conducting a digital maturity assessment annually.
- b. Banks are allowed to host their system in the cloud, as long as they can ensure the data centre facilities are in Indonesia.
- c. Banks need to develop or update their IT strategic plan to align with the POJK PTI by November 2022.

## Your PwC Indonesia Contacts:

**Subianto**  
Broader Assurance Services Leader  
subianto.subianto@pwc.com

**Andrew Tirtadjaja**  
Risk Assurance Director  
andrew.tirtadjaja@pwc.com

**Melissa Gunarto**  
Risk Assurance Director  
melissa.g.gunarto@pwc.com


**Hengky Antony**  
Risk Assurance Director  
hengky.antony@pwc.com


**Beatrix Ariane**  
Risk Assurance Senior Manager  
beatrix.b.ariane@pwc.com

**Mila Ichwanto**  
Risk Assurance Manager  
mila.ichwanto@pwc.com

**Ledwin Ewaldo**  
Risk Assurance Manager  
ledwin.ewaldo@pwc.com

[www.pwc.com/id](http://www.pwc.com/id)

 PwC Indonesia

 @PwC\_Indonesia

If you would like to be removed from this mailing list, please reply and write UNSUBSCRIBE in the subject line, or send an email to [id\\_contactus@pwc.com](mailto:id_contactus@pwc.com).

**DISCLAIMER:** This content is for general information purposes only and should not be used as a substitute for consultation with professional advisors.

PwC Indonesia is comprised of KAP Tanudiredja, Wibisana, Rintis & Rekan, PT PricewaterhouseCoopers Indonesia Advisory, PT Prima Wahana Caraka, PT PricewaterhouseCoopers Consulting Indonesia, and Melli Darsa & Co., Advocates & Legal Consultants, each of which is a separate legal entity and all of which together constitute the Indonesia member firm of the PwC global network, which is collectively referred to as PwC Indonesia.

© 2022 PwC. All rights reserved. PwC refers to the Indonesia member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details..