ASSEGAF HAMZAH
& PARTNERS

RAJAH & TANN ASIA
LAWYERS
WHO
KNOW
ASIA

Client Update: Indonesia
6 April 2023

OJK Sets New Cyber Security Best Practices for the Banking Industry

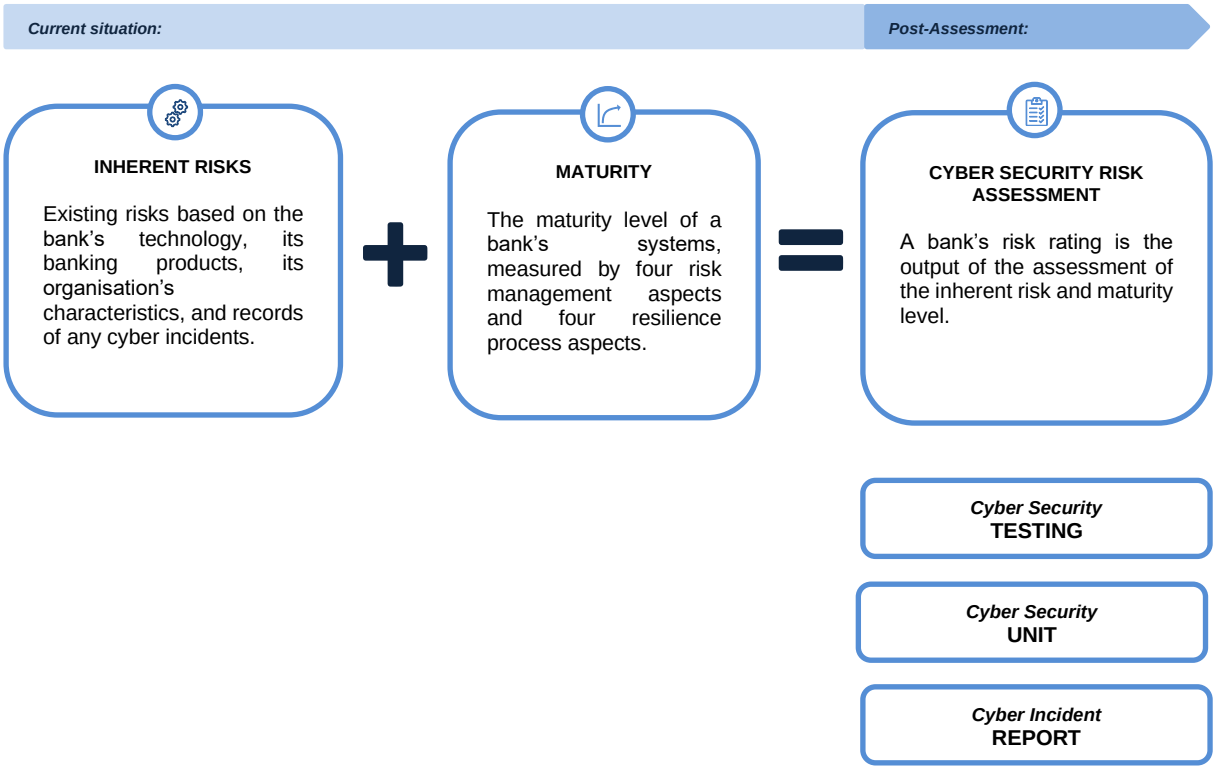
Last year, the Financial Services Authority ("**OJK**") issued OJK Regulation No. 11/POJK.03/2022 on the Implementation of Information Technology by Commercial Banks. This regulation was part of the revolution by OJK of regulations on data, technology, risk management, collaboration, and institutional setting, all of which is designed to boost the acceleration of Indonesia's digital banking transformation. To follow up the regulation, OJK issued OJK Circular Letter No. 29/SEOJK.03/2022 on Cyber Security and Resilience for Commercial Banks ("**Circular**") as one of the implementing regulations to safeguard this digital banking transformation.

In the Circular, the OJK puts the onus on commercial banks (which include conventional and shariah banks) ("**banks**") to identify their cyber security risk by going through a series of assessments and processes on an annual basis. Once banks completed the self-assessment, they must report their self-assessed rating to OJK. In addition, banks must also report any cyber incident to OJK and set up a new cyber security structure.

The cyber security assessment is proceeded by assessment of the inherent risk (existing factors) and cyber security maturity (controls that are already in place) as outlined below:

Client Update: Indonesia

6 April 2023



We take a closer look at the above aspects below.

Assessment of Cyber Security Risk Level

A bank must keep track of its cyber security position. To do so, it must assess its cyber security risk level annually. The risk level is divided into five: 1 (low), 2 (low to moderate), 3 (moderate), 4 (moderate to high), and 5 (high).

As mentioned above, the responsibility to assess the cyber security risk level lies with the banks. In doing so, the Circular sets out the assessments that must be carried out:

1. ***Inherent risk assessment***

   First, a bank must determine its inherent risk level based on the following indicators:

   a. technology, e.g., how connected and accessible its IT system is and the engagement of IT service providers;

   b. banking products, e.g., its ATM mechanisms and whether it has any digital banking services;

   c. its organisation's characteristics, e.g., turnover rate, privilege access management; and

   d. its cyber incidents track record, e.g., frequency and impact of the cyber incidents.

The bank's response to the above indicators (from a level of 1 to 5 as detailed above) will determine its inherent risk level. The Circular also provides banks with a template that they can use when they are conducting this assessment, and banks can also include any other parameters or indicators that are relevant to their business.

2. ***Maturity level assessment***

The second assessment is the maturity level assessment to determine the current level of the bank's cyber security, i.e., controls that are already in place. There are four risk management aspects and four resilience process aspects to evaluate, as detailed below:

a. Risk management aspects, which comprised of:

(i) cyber security risk governance;

(ii) cyber security risk framework;

(iii) cyber security risk processes resources and information systems; and

(iv) cyber security risk control systems.

b. Resilience processes, which comprised of:

(i) asset, threat, and vulnerability identification;

(ii) asset protection;

(iii) cyber incident detection; and

(iv) cyber incidents response and recovery.

Like the first assessment on inherent risk, the bank must assign a level of 1 to 5 to each of the risk management and resilience process parameters or indicators.

3. ***Cyber security risk assessment***

The last step is the cyber security risk assessment, which is derived from the results of the inherent risk assessment and the maturity level assessment. Again, this assessment will result in a level of 1 to 5.

The result of each of the above assessments must be submitted to the OJK as part of the "Report on the Current Condition of the Bank's IT System Implementation", and submitted within 15 business days from the end of the report year. Considering that the Circular was only issued in late 2022, the deadline for the first report following the Circular's issuance (i.e., the report for 2022) has been extended to the end of June 2023.

Upon submission of the report, OJK will review the reported self-assessed risk level. If they find any discrepancies between the bank's actual condition and the stated risk level, OJK can make the necessary adjustments. The resulting risk level will affect the bank's overall soundness level. If a bank's soundness level is low, the OJK will require the bank to prepare and conduct specific action plans to address any relevant issues.

Cyber Security Testing

The second requirement under the Circular is for banks to conduct cyber security testing on a regular basis. The Circular does not specify the number of tests that must be performed.

Cyber security testing consists of:

1. ***Vulnerability analysis***

   The bank must conduct a vulnerability analysis to identify the weak points in its IT system, by way of:

   a. identifying the system's vulnerabilities; and

   b. conducting penetration tests.

2. ***Scenario-based testing***

   A scenario-based testing is conducted to validate the countermeasures and any prescribed corrective action for a potential cyber incident. It includes:

   a. a table-top exercise;

   b. a cyber range exercise;

   c. a social engineering exercise; and

   d. an adversarial attack simulation exercise.

3. ***Other proactive measures***

   The bank can also implement proactive measures to compose a realistic testing scenario (e.g., by way of a thorough threat hunting).

The result of the cyber security testing must be included in the "Report on the Current Condition of the Bank's IT System Implementation" and submitted to OJK.

Cyber Security Unit

The third requirement in the Circular is for banks to have an independent cyber security unit or function to manage their cyber security and resilience, in particular to:

1. implement the cyber resilience processes;
2. conduct the cyber risk assessment, inherent risk assessment, and maturity level assessment;
3. conduct the cyber security testing; and
4. coordinate the cyber incident response team.

The cyber security unit/function must be independent from the bank's IT management unit/function.

Cyber Incident Report

The fourth and last requirement in the Circular is for banks to report any cyber incident to OJK. A cyber incident is a cyber threat in the form of an attempt, activity, and/or action that results in the failure of an electronic system. The Circular lists malware, web defacement, denial of services (DOS), and distributed denial of services (DDOS) as examples of cyber incidents.

There are two types of report that a bank must carry out if a cyber incident occurs. First, the bank must submit an initial notification report setting out the basic information of the incident to OJK within 24 hours of the bank being aware of the incident. Then, within five days of the incident, the bank must submit a cyber incident report to OJK, which details the incident. Both reports must be submitted electronically and by following the format set out in the Circular.

The Circular further provides that if any other government authority requires a cyber incident report to be submitted earlier than the deadline under the Circular, a bank must comply with this requirement and submit the report to OJK at the same time as the submission of the report to the authority, i.e., earlier than the deadline under the Circular. However, if the deadline sets by the other authority is later than the Circular's, the bank must follow the deadline under the Circular.

Key Takeaways

As cyber-attacks and events of data breach continues to increase in line with technological advancement in many sectors including banking, companies must prioritise and manage their cyber security efforts now more than ever. With the issuance of this Circular, banks are certainly leading the market and the Circular could be the model to follow for other sectors or industries in improving their cyber security efforts.

Not surprisingly, there was a mixed reaction in the market when the Circular was announced. Most market players see the requirements under the Circular as reasonable in the context of risk management measures (which may include IT management issues). However, other requirements under the Circular

may prove to be more difficult to implement, for example the requirements pertaining to the human resources for the cyber security unit.

In addition to the efforts by the banks themselves, it is crucial that the customers know of the risks and are taking part to prevent possible cyber security threats. As seen above, the Circular does not address these matters and is, instead, more focused on the measures that are under control of the banks. Other aspects that may impact the success of OJK's initiative with the Circular is whether non-bank financial services and other industries will apply similar standards.

Contacts

Zacky Zainal Husein
Partner

D +62 21 2555 9956
F +62 21 2555 7899
zacky.husein@ahp.id

Muhammad Iqsan Sirie
Partner

D +62 21 2555 7805
F +62 21 2555 7899
iqsan.sirie@ahp.id

Regina Damaris also contributed to this alert.

ASSEGAF HAMZAH & PARTNERS

Client Update: Indonesia

6 April 2023

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

Regional Contacts

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

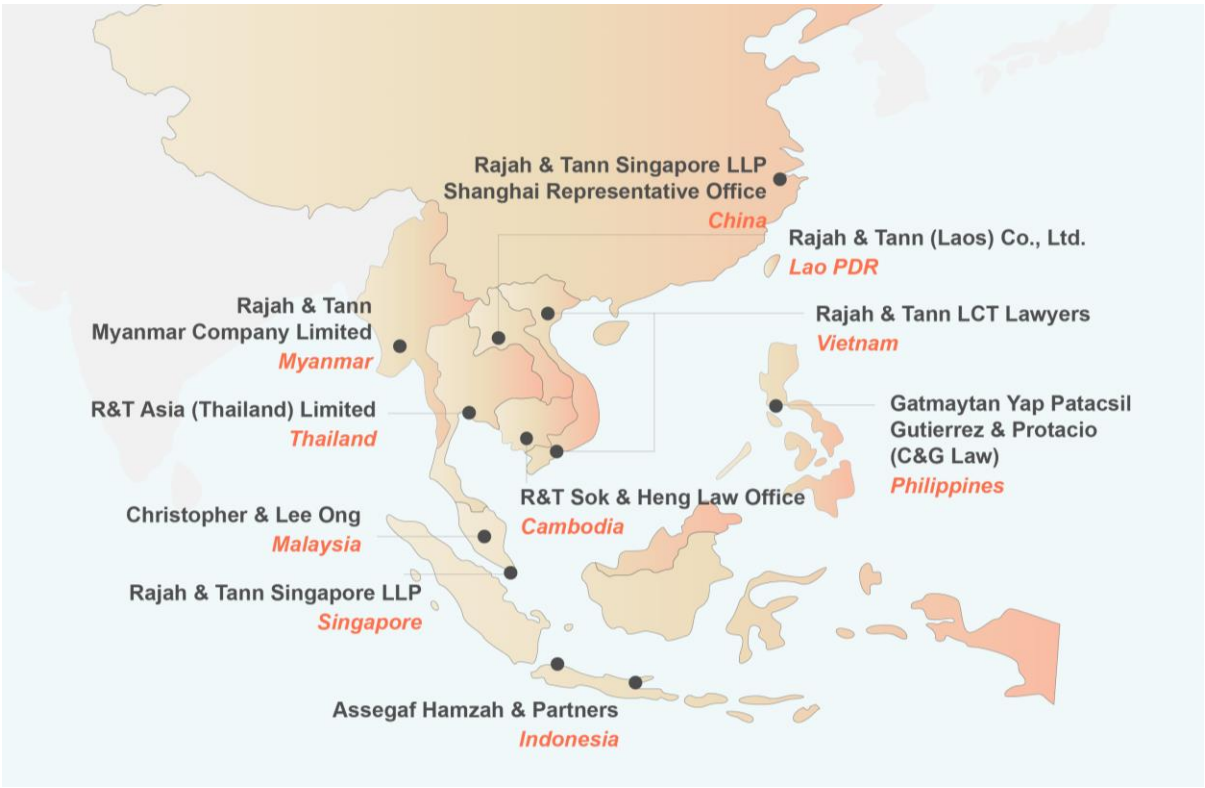
Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Client Update: Indonesia

31 March 2023

Our Regional Presence



Based in Indonesia, and consistently gaining recognition from independent observers, Assegaf Hamzah & Partners has established itself as a major force locally and regionally and is ranked as a top-tier firm in many practice areas. Founded in 2001, it has a reputation for providing advice of the highest quality to a wide variety of blue-chip corporate clients, high net worth individuals, and government institutions.

Assegaf Hamzah & Partners is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.