
Updated Policy Document on Risk Management in Technology (RMiT): Additional Requirements Relating to Management of Cloud Technology Risks

Introduction

On 1 June 2023, the Central Bank of Malaysia ("**BNM**", or *Bank Negara Malaysia*) issued an updated version of its [Policy Document on Risk Management in Technology](#) ("**Updated RMiT PD**"), which sets out additional requirements in respect of a financial institution's ("**FI**") management of cloud technology risks.¹ In conjunction with the issuance of the Updated RMiT PD, BNM also revised its [FAQs for the Updated RMiT PD](#) to provide further guidance and clarifications regarding such additional requirements.

This Update seeks to provide a summary of the key requirements being introduced under the Updated RMiT PD that FIs should take note of.

Key Updates in the Updated RMiT PD

The new requirements introduced by the Updated RMiT PD are mainly focused on the technology risk management issues regarding the adoption of cloud services by FIs, which include the following:

(a) New Requirements for Adoption of Public Cloud² for Critical Systems³

Under the existing Policy Document on Risk Management in Technology issued on 19 June 2020 ("**Existing RMiT PD**"), an FI is required to conduct a comprehensive risk assessment prior to cloud adoption and:

- (i) consult BNM prior to using public cloud for critical systems;⁴ and
- (ii) notify BNM of its intention to use cloud services for non-critical systems.⁵

¹ Particularly, the additional requirements relating to cloud are set out in paragraph 10.50, paragraph 15 and Appendix 10 of the Updated RMiT PD.

² "**Public cloud**" is defined under the Updated RMiT PD to refer to a fully virtualised environment in which a service provider makes resources such as platforms, applications or storage available to the public over the Internet via a logically separated multi-tenant architecture.

³ "**Critical systems**" is defined under the Updated RMiT PD to refer to any application system that supports the provision of critical banking, insurance or payment services, where failure of the system has the potential to significantly impair the financial institution's provision of financial services to customers or counterparties, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements.

⁴ Paragraph 10.51 of the Existing RMiT PD.

⁵ Paragraph 10.50 of the Existing RMiT PD.

To this end, the Updated RMIT PD clarifies that:⁶

- (i) an FI is only required to **consult** BNM prior to the first-time adoption of public cloud for critical systems;
- (ii) an FI is only required to **notify** BNM for any subsequent adoption of public cloud for critical system;
- (iii) an FI is no longer required to notify BNM of its intention to use cloud services for non-critical systems; and
- (iv) an FI must ensure that the roadmap for adoption of cloud services (for critical and non-critical systems) is included in the annual outsourcing plan submitted to BNM.

The new requirements above demonstrate BNM's shift to a risk-based approach in relation to cloud adoption by FIs.

Furthermore, under the Updated RMIT PD⁷, FIs are encouraged to carry out an assessment of common key risks and put in place control measures as specified in the newly incorporated Appendix 10 when adopting public cloud for critical systems. It is worth highlighting that the guidance set out in Appendix 10 of the Updated RMIT PD is largely adopted from the Cloud Technology Risk Assessment Guideline (CTRAG) Exposure Draft that was released by BNM in 2022 for public feedback.

Some of the key requirements introduced in Appendix 10 of the Updated RMIT PD are as follows:

- (i) the development of internal policies and procedures by FIs to regulate internal adoption of cloud services;
- (ii) due diligence on prospective cloud service providers;
- (iii) the inclusion in FIs' agreements with their cloud service providers of minimum contractual clauses that set clear parameters on the information security and operational standards expected of the cloud service providers; and
- (iv) the identification of operational considerations that must be taken into account when adopting cloud services for critical systems.

(b) Multi-factor authentication ("MFA") Security Controls as a Standard Requirement

Under the Existing RMIT PD, BNM merely recommends FIs to deploy MFA technology and channels that are more secure than unencrypted short messaging service ("**SMS**").

⁶ Paragraph 15 of the Updated RMIT PD.

⁷ Paragraph 10.50 of the Updated RMIT PD.

The Updated RMIT PD now makes it a mandatory requirement for FIs to deploy MFA technology and channels that are more secure than unencrypted SMS, and ensure that the MFA solution is resistant to interception or manipulation by any third party throughout the authentication process.

Effective Date of the Updated RMIT PD

The Updated RMIT PD came into effect on 1 June 2023. However, the new amendments specifically related to cloud technology risk management take effect as follows:

- 1 June 2023 - for licensed digital banks and Islamic digital banks; and
- 1 June 2024 - for FIs other than licensed digital banks and Islamic digital banks.

Concluding Remarks

In view of BNM's shift to a risk-based approach in relation to FIs' adoption of public cloud for their critical systems and the revised requirements for such adoption of public cloud for critical systems, FIs will need to review their internal policies and procedures regarding the adoption and rollout of cloud services, as well as their contractual terms with their respective cloud service providers in order to ensure compliance with the new requirements under the Updated RMIT PD.

We trust that the above provides you with a quick update on the revised requirements introduced by BNM in the Updated RMIT PD. Should you require any assistance or clarification regarding the above, or about any matter pertaining to the same, please feel free to reach out to our team at your convenience.

Contacts



Deepak Pillai
Head
Technology, Media &
Telecommunications; Data
Protection

T +60 3 2275 2675
F +60 3 2273 8310
deepak.pillai@christopherleeong.com



Intan Haryati Binti Mohd Zulkifli
Partner
Technology, Media &
Telecommunications; Data
Protection

T +60 3 2675 2674
F +60 3 2273 8310
intan.haryati@christopherleeong.com



Anissa Maria Anis
Partner
Technology, Media &
Telecommunications; Media &
Entertainment

T +60 3 2267 2750
F +60 3 2273 8310
anissa.anis@christopherleeong.com



Yong Shih Han
Partner
Technology, Media &
Telecommunications; Data
Protection

T +60 3 2273 1919
F +60 3 2273 8310
shih.han.yong@christopherleeong.com

Contribution Note

This Client Update is contributed by the Contact Partners listed above, with the assistance of **Ng Hong Syuen** (Associate, Christopher & Lee Ong) and **Yeap Yee Lin** (Associate, Christopher & Lee Ong).

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.co.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

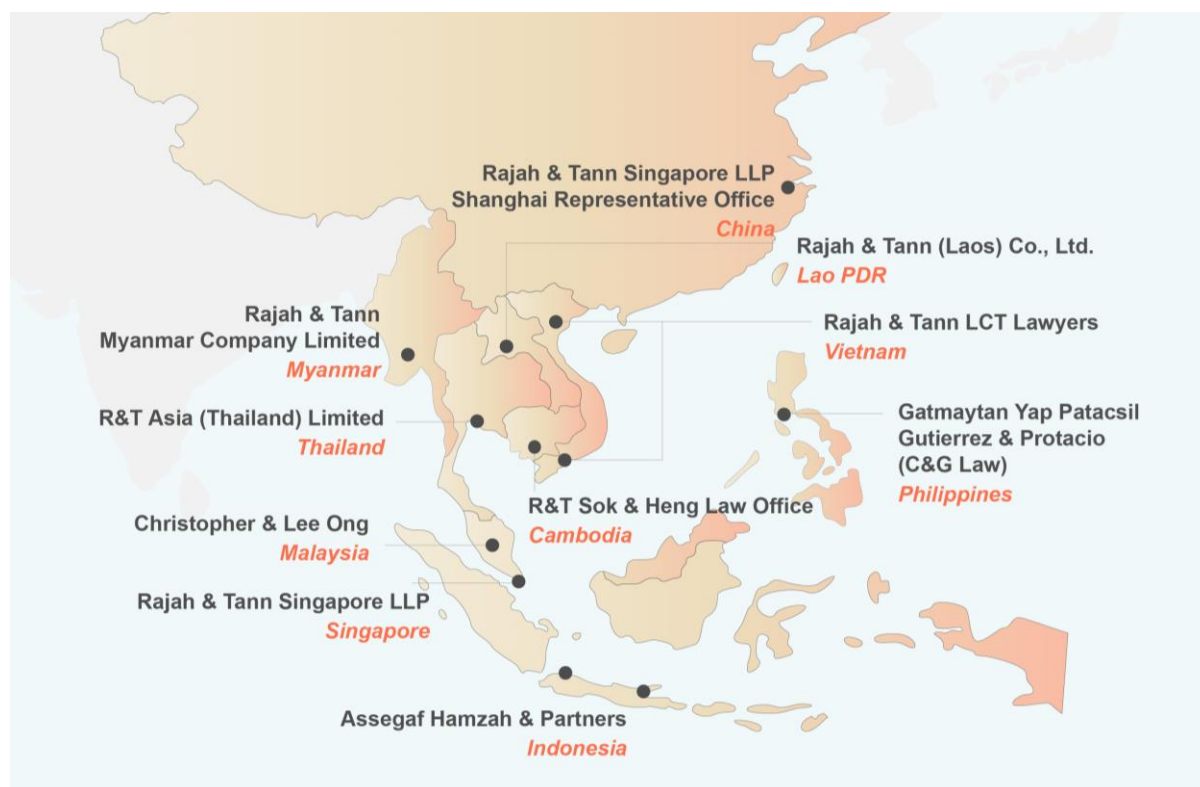
www.rajahtannlct.com

Rajah & Tann Asia is a network of legal practices based in Asia.

Member firms are independently constituted and regulated in accordance with relevant local legal requirements. Services provided by a member firm are governed by the terms of engagement between the member firm and the client.

This update is solely intended to provide general information and does not provide any advice or create any relationship, whether legally binding or otherwise. Rajah & Tann Asia and its member firms do not accept, and fully disclaim, responsibility for any loss or damage which may result from accessing or relying on this update.

Our Regional Presence



Christopher & Lee Ong is a full service Malaysian law firm with offices in Kuala Lumpur. It is strategically positioned to service clients in a range of contentious and non-contentious practice areas. The partners of Christopher & Lee Ong, who are Malaysian-qualified, have accumulated considerable experience over the years in the Malaysian market. They have a profound understanding of the local business culture and the legal system and are able to provide clients with an insightful and dynamic brand of legal advice.

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

The contents of this Update are owned by Christopher & Lee Ong and subject to copyright protection under the laws of Malaysia and, through international treaties, other countries. No part of this Update may be reproduced, licensed, sold, published, transmitted, modified, adapted, publicly displayed, broadcast (including storage in any medium by electronic means whether or not transiently for any purpose save as permitted herein) without the prior written permission of Christopher & Lee Ong.

Please note also that whilst the information in this Update is correct to the best of our knowledge and belief at the time of writing, it is only intended to provide a general guide to the subject matter and should not be treated as a substitute for specific professional advice for any particular course of action as such information may not suit your specific business or operational requirements. It is to your advantage to seek legal advice for your specific situation. In this regard, you may call the lawyer you normally deal with in Christopher & Lee Ong.