GUIDELINES TO FINANCIAL INSTITUTIONS

GUIDELINES NO. TRS/G-3/2022/2

GUIDELINES ON INFORMATION TECHNOLOGY THIRD PARTY RISK MANAGEMENT

---

1. INTRODUCTION

1.1 With the increase in the number of IT companies, businesses nowadays have access to the privilege of various products and services offered by third party vendors, suppliers and service providers. Moreover, IT outsourcing and cloud services will enable the FIs to access IT resources and talents for the management of their IT system and operations.

1.2 IT third party arrangements, may include:

i. all forms of IT outsourcing including Head Office, Parent Company and Group;

ii. cloud computing services;

iii. provision of IT and IT-related services;

iv. development or supply of commercial hardware, software and equipment; and

v. counterparties such as government agency, other FIs and financial market infrastructure.

1.3 While IT third party service can bring benefits, it may affect the risk profile of FIs due to, for example, strategic, reputation, compliance and operational risks arising from failure of a service provider in providing the service, breaches in security, or inability to comply with legal and regulatory requirements by the FIs. FIs can also be exposed to country risk where the service provider is located.

1.4 As such, FIs need to understand the degree and level of risk from these third-party arrangements. FIs should put in place adequate and robust due diligence and supervision process as well as ensure adequate control is in place on both FIs and IT third party as FIs are ultimately responsible and accountable for managing third party risks.

1.5 The objectives of these Guidelines are to:

i. Encourage FIs to perform due diligence on third-party and risk assessment on the engagement;

ii. Promote effective governance on the FIs relating to supervision on the third party;

iii. Encourage FIs to deploy IT controls to protect sensitive information; and

iv. Recommend business continuity and exit strategy relating to third-party issue are established.

1.6 These Guidelines are issued pursuant to section 32 of the Brunei Darussalam Central Bank Order, 2010 and are aimed at FIs licensed, registered or regulated under the following:

i. Banking Order, 2006;

ii. Islamic Banking Order, 2008;

iii. Insurance Order, 2006;

iv. Takaful Order, 2008;

v. Finance Companies Act, Cap. 89;

vi. Securities Markets Order, 2013;

vii. Money-Changing and Remittance Businesses Act, Chapter 174;

viii. Moneylenders Act, Chapter 62; and

ix. Pawnbrokers Order, 2002.

1.7 These Guidelines are also applicable to:

i. operators of payment systems that have been approved to operate in Brunei Darussalam under the Notice on Requirements for Payment Systems [Notice No. PSO/N-1/2020/1]; and

ii. Perbadanan Tabung Amanah Islam Brunei established under the Perbadanan Tabung Amanah Islam Brunei Act [Cap. 163].

1.8 These Guidelines should be read with the following:

i. Notice on Application for Approval of Outsourcing Arrangement for Insurance Companies and Takaful Operators [Notice No. TIU/N-1/2019/11];

ii. Notice on Early Detection of Cyber Intrusion and Incident Reporting [Notice No. FTU/N1/2017/1 and TRS/N-1/2020/1];

iii. Notice on Outsourcing for Capital Markets Services Licence Holders [Notice No. CMA/N-1/2020/15];

iv. Notice on Requirements for Payment Systems [Notice No. PSO/N-1/2020/1];

v. Guidelines on Outsourcing Arrangement for Insurance Companies and Takaful Operators [Guidelines No. TIU/G-1/2019/10];

vi. Guidelines on Outsourcing for Banks;

vii. Standard Technology Risk Management Guideline [TRS/G-1/2019/1]; and

viii. Guidelines on Technology Risk Management for Financial Institutions [TRS/G-1/2022/2].

1.9 Implementation of these Guidelines should be risk-based and commensurate with the size of the FIs, nature and types of products and services offered by the FIs, and the complexity of IT operations of the individual FIs.

1.10 These Guidelines shall take effect on 1st July 2022.

2. DEFINITIONS

For the purpose of these Guidelines:

2.1 "Agents" refer to individuals or entities that provide service to the customers on behalf of the FIs or act as intermediaries between the customer and FIs. This includes insurance/takaful agents, brokers, collection services and applicable FinTech companies.

2.2 "Cloud Computing" refers to service and delivery model for enabling on-demand network access to a shared pool of configurable computing resources (servers, storage and services). Hosting, storing or processing of information are within the service provider's computing infrastructure.

2.3 "Configuration policy" refers to policy and/or guidelines that define baseline for configuration of software and hardware in the FIs.

2.4 "Contractors" refers to vendors, suppliers, service providers, outsourced service providers and/or consultants that have made contract with the FIs to provide specific and consistent products or services to the FIs. Contractors are usually effective during IT project or within time period of the agreed contract.

2.5 "Counterparties" refers to individual or entity that provide services to the FIs mainly through mandate, trust, cooperation or membership. This includes but not limited to government agencies, regulators, partner and financial market infrastructure (e.g. SWIFT and payment settlement system). Unlike IT outsourcing and service provider, counterparties often involved special requirements and arrangements imposed to the FIs.

2.6 "Critical system" refers to any system that supports the provision of FIs services, where failure of the system can significantly impair the FIs' provision of services to its customers or stakeholders, business operations, financial position, reputation or compliance with applicable laws and regulatory requirements.

2.7 "Cyber insurance" refers to takaful or insurance policy that an entity can purchase to help reduce the financial risks associated with cybersecurity incidents. It is also known as cyber liability insurance, cybersecurity insurance or cyber protection insurance.

2.8 "Encryption" refers to the process of encoding messages or information in such a way that only authorized parties can read it.

2.9 "IaaS" or "Infrastructure-as-a-Service" is a cloud model in which the physical data centre and servers are managed by the cloud service provider, while the FIs mainly manage the virtual machine or operating system, application and database.

2.10 "Incident" refers to IT or IT-related issues such as power failure, system downtime and cyber-attack that affect the business operations or service delivery of the FIs.

2.11 "Insurer" refers to a registered takaful operator or insurance company that the FIs engaged with.

2.12 “IT Operations” refers to the people and management processes associated with IT service management to deliver the right set of services at the right quality and at competitive costs for customers.

2.13 “IT Outsourcing” refers to outsourcing of IT function, operation or service to a service provider.

2.14 “Manufacturer” refers to individual or entity that prepare finished products for sale and distribution.

2.15 “Material outsourcing” means an outsourcing arrangement which:

i. in the event of a service failure or security breach, has the potential to either significantly impact the FIs':

a. business operations, reputation or profitability; or

b. ability to manage risk and comply with applicable laws and regulations; or

ii. involves customer personal information or data and, in the event of any unauthorised access or disclosure, loss or theft of the personal information or data, may have a material impact on the customer.

2.16 “Outsourcing” refers to an arrangement whereby FI engages in a third party (i.e. service provider) to provide FI with a service that may already or may conceivably be performed by the FI itself which includes the following characteristics:

i. the FI is dependent on the service on an ongoing basis but excludes services that involve the provision of a finished product;

ii. the service is integral to the provision of a financial service by the FI and/or the service is provided to the market by the service provider in the name of the FI; and

iii. it is prohibitive to change the service provider as substitutes are lacking in the market or may only be replaced at significant cost to the FI.

2.17 “PaaS” or “Platform-as-a-Service” is a cloud model in which IT infrastructure is managed by the cloud service provider, while the FIs mainly manage the application and database.

2.18 “Partners” refers to individual or entity that vendor or third parties work with in order to deliver products or services, usually within partnership or subsidiary.

2.19 “Personal data” refers to data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the FI has or is likely to have access.

2.20 “Project” refers to a temporary endeavour undertaken to create an unique product or service. It has a defined scope and consists of sets of operations to deliver specific goal.

2.21 “SaaS” or “Software-as-a-Service” is cloud model in which all IT infrastructure including database are managed by the cloud service provider, while the FI focuses only on the application.

2.22 “Service provider” refers to an individual or entity that provides a service to the FIs, including a member of the group to which the FIs belongs, e.g. its Head Office, parent insurer, another branch or related company, whether it is located in Brunei Darussalam or elsewhere.

2.23 “Supplier” refers to an external individual or entity that provides and distributes finished IT products including hardware and software to the FIs.

2.24 “Supply chain” refers to an individual or entity beyond a direct supplier. This includes a manufacturer, developer, authorised distributer, reseller and importer, as well as a manufacturer and supplier of parts or components of the finished IT products.

2.25 “System” refers to information system used by the FIs for performing their business operation, which is made up of hardware, software, network, and other IT components.

2.26 “Technology risk” refers to any risks that is caused by IT and IT-related failure or vulnerability, which can impact FIs’ systems, data and business processes.

2.27 “User access policy” is a policy that outlines expectations on user access management and access control configuration.

2.28 “Vendor” refers to an external individual or entity that offers solutions to FIs directly or through suppliers and service providers. Vendors usually liaise on the business relationship with the FIs and engage with suppliers and service providers to deliver products or services.

3. THIRD-PARTY GOVERNANCE

3.1 While the FIs may transfer full or partial service delivery and operational responsibilities to outsourced service provider or counterparties, FIs are still responsible and accountable to their customers and BDCB in respect of the operations and performance of the outsourced service provider or counterparties. The board of directors or senior management of the FIs should hold responsibility and accountability for the oversight and any decisions relating to the outsourced service provider and counterparties.

3.2 The board of directors of an FI should ensure the senior management has established a framework in the selection and oversight of IT third-parties.

3.3 The FIs and IT third-parties should identify, assess and be aware of their respective roles and responsibilities in the third-party arrangement and ensure these are outlined in the agreement between the FIs and the third-parties.

3.4 The FIs should assess the capability of the IT third-parties in overseeing their partners, sub-contractors, suppliers and supply chains.

3.5 FIs should ensure and verify that the IT third parties have performed background check and security screening in the selection of their personnel, especially on personnel that are designated to perform work activities on the FIs. This include but not limited to the following:

i. Financial or credit status;
ii. Criminal record;
iii. Previous work history; and
iv. Competency assessment.

3.6 FIs' policies, standards, guidelines and procedures should be clearly communicated to vendors, service providers or other third parties depending on the applicability and scopes of the document.

3.7 Vendors, service providers or other third parties who are authorised to access the FIs' critical systems, sensitive information and customer personal data should be required to protect sensitive and confidential information. The related personnel of the third parties should sign a non-disclosure agreement to ensure information security.

4. IT OUTSOURCING

4.1 IT outsourcing involves outsourcing of IT functions to a third-party service provider located in Brunei Darussalam or abroad. FIs should oversee and keep track of all IT outsourcing arrangements within the FIs, and adhere to any relevant law or regulation in Brunei Darussalam including BDCB's notices and guidelines relating to outsourcing.

4.2 For IT outsourcing relating to FIs' critical system or customer's personal information, the FIs should have strong justification for the decision on the IT outsourcing such as when the outsourcing arrangement would provide higher quality, more efficient and more secure services than the FIs might be able to provide internally.

4.3 Risks relating to the outsourced services might be different to those risks the FIs might be exposed to if these functions were performed internally by the FIs. Hence, FIs should identify and assess risks relating to IT outsourcing and manage them accordingly. FIs should ensure that these outsourcing activities do not hinder their daily operations and business processes.

4.4 Before an outsourced service provider is appointed, due diligence should be carried out to determine the outsourced service provider's viability, reliability, track record and reputation, as well as financial position, and compliance with applicable Brunei Darussalam's laws and regulations.

4.5 Where the outsourced service provider is located outside Brunei Darussalam, the FIs should ensure personal data protection has been established in the country and the outsourced service provider has established their own privacy policy. The FIs should also review the jurisdiction and policy to ensure FIs' data and customer data are protected and will not be disclosed without authorisation.

4.6 As part of the due diligence, FIs should also ensure the outsourced service provider will be able to provide sufficient level of support to the FIs at all times, by ensuring adequate expertise are available when required.

4.7 FIs should ensure that relevant personnel of the outsourced service providers including contractors, have the requisite level of competence and skills to perform the outsourced functions and manage technology risks related to the outsourced functions.

4.8 A written agreement should be present in all IT outsourcing arrangements. The terms of the contract and conditions that define the roles and responsibilities, relationships, termination, liabilities, service levels, sub-contracting and obligations of all contracting parties should be clearly stated and understood by the FIs and service providers alike.

4.9 IT outsourcing should not result in any weakening or degradation of the FIs' internal controls. There should be assurance of proper security measures and controls in place by the outsourced service provider. FIs should ensure that these measures and controls are at least as stringent as it would expect for its own operations.

4.10 FIs should ensure the outsourced service provider is subjected to periodic independent audits relating to the FIs outsourced operations. The audits can be performed by an independent external auditor hired by the FIs or the outsourced service provider.

4.11 FIs should also come up with appropriate contingency plans for any IT outsourcing activities in the case there is a degradation in the delivery of services or decline in quality of the products and services by the service provider due to various internal and external factors.

4.12 FIs should ensure that the outsourced service provider signs a non-disclosure agreement to protect sensitive data and information belonging to the FIs or as required by applicable laws or regulations. Where necessary, personnel of the outsourced service provider that are assigned to perform sensitive tasks on the FIs' premise should also sign the non-disclosure agreement.

4.13 When the outsourced service provider requires access to the FIs' IT system or IT resources, the FIs should ensure access is only given in order to perform the scope of work as agreed in the contract or agreement. The FIs should also monitor if the access and tasks performed by the outsourced provider are in accordance to the contract or agreement.

4.14 The use of certain IT or IT related services from IT third-parties by FIs may not constitute outsourcing such as telecommunication service and media forensic service. However, as many of these services may affect FIs' business operation and customer personal information, the FIs should assess these services' exposure to various technology risks associated with the loss of data confidentiality, integrity and service availability, and manage these associated risks. Therefore, similar measures should be considered for service provider as IT outsourcing.

4.15 In the event of contract termination with the outsourcing service provider, either on expiry or ended prematurely, the FIs should have the contractual power and means to ensure that the service provider return, remove and destroy information shared by the FIs including data stored at the service provider's systems, computing resources and backups at all location.

5. VENDOR MANAGEMENT

5.1 FIs should establish a risk-based vendor management framework for the procurement of IT or IT-related products and services from third parties, which should include the following:

i. selection criteria and evaluation;

ii. risk assessment and vendor classification;

iii. due diligence and security assessment;

iv. vendor performance and/or competency review;

v. purchasing or payment processes; and

vi. contract and agreement management where applicable.

5.2 The framework should also map or clarify the link between vendor management with IT project, system acquisition, system development, IT operation and IT services management.

5.3 FIs are recommended to create a list of authorised vendors for the procurement, supply, implementation and maintenance of IT system and IT asset. The list should be updated to reflect any addition, change or termination of vendors.

5.4 FIs should verify any personnel from the vendors and their selected suppliers or service providers before entering their premise and IT system. Their activity should be monitored and recorded to ensure that the activities performed are within their scope of the contract or service level agreement.

5.5 When the vendors and their selected suppliers or service providers require privilege access to FIs' IT system or IT resources, the FIs should ensure the access is only given temporarily and only to perform necessary tasks in development or pre-production environment. For live production environment, the access should be performed only by personnel from the FIs. The FIs should monitor if the tasks performed by vendors are in accordance to the scope of work and contract.

5.6 For vendors, suppliers or service providers that require standard access to the IT system or IT resources, the access should be given on minimal basis with restrictions in accordance to their scope of work and contract. Vendor access to the FIs' systems should be tightly controlled and periodically reviewed.

5.7 The activities of the vendors and their selected suppliers or service providers should be monitored and reviewed to ensure the products and services delivered are within acceptable quality and as agreed in the quotation, contract or service level agreement. This include performing verification check and testing after delivery or implementation.

5.8 FIs should ensure all credentials and settings of the IT systems, hardware or software provided by the vendors or their selected suppliers or service providers are changed in accordance to the FIs' user access policy and configuration policy.

6. SUPPLIER AND SUPPLY CHAIN MANAGEMENT

6.1 Service providers and vendors would usually engage with partners, suppliers, distributers and manufacturers in order to deliver their products and services to the FIs. FIs should be aware that these partners, suppliers, distributers and manufacturers may pose indirect risk to the FIs. Therefore, FIs should ensure their service providers and vendor have identified all suppliers and supply chains associated with their service with the FIs and to maintain list of these suppliers and supply chains.

6.2 In an IT project, the FIs should ensure the vendors list their partners, suppliers and service providers that are involved in the project as subcontractors, while the manufacturers would be included in the hardware and software list.

6.3 FIs should ensure that its vendor or supplier has assessed their partners, service providers and manufacturers related to IT assets, or at least has put in place processes in the assessment and selection of their partners, service providers and manufacturers. The assessment should include the following:

i. selection criteria and evaluation;

ii. due diligence and security assessment; and

iii. performance and competency review.

6.4 FIs should also verify if their vendor or supplier has assessed the credibility of products supplied to the FIs. For example, the FIs may request the following information from the vendor or supplier:

i. condition and quality of products;

ii. compliance and/or certification to standard;

iii. country where the products are manufactured/assembled or where the services are performed;

iv. warranty and maintenance;

v. customer service and support;

vi. vulnerability disclosure report or common vulnerability and exploit (CVE) patches; and

vii. reference or previous customer review.

6.5 On top of the paragraphs above, the FIs should also observe Paragraph 5.4, 5.5, 5.6, 5.7 and 5.8 of this Guidelines.

7. CLOUD COMPUTING

7.1 Depending on the scope of the service, cloud computing should be considered as a form of IT outsourcing with offshore service provider, and Paragraph 4 of this Guidelines is applicable.

7.2 Data hosted in cloud computing services may be subjected to law and regulation of the country where the data is located. FIs should ensure that the country where the cloud service provider operates and the country where the FIs' data being hosted have personal data protection legislation or regulation in place.

7.3 FIs should be mindful of any applicable law and regulation in Brunei Darussalam relating to information or data protection, storage, processing, hosting and transmission, and should be able to address potential issues relating to the law and regulation if any.

7.4 FIs that have subscribed to cloud computing service providers should be aware of the locations (i.e. country) of the servers, applications and data within the cloud service provider's computing infrastructure.

7.5 Considering the inherent risks associated with cloud computing, FIs are advised to perform due diligence checks and sufficient background research of the cloud service provider.

7.6 FIs should also assess the risk and suitability of their cloud model and deployment model for their system. FIs should identify and manage the difference in controls ownership when using Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

7.7 Management and security of cloud service are based on shared responsibility model. Both FIs and the cloud service provider should be clear on their respective roles under the shared responsibility model including the responsibility to implement applicable controls recommended in these Guidelines.

7.8 FIs should identify and assess all tools and controls available to the FIs in the cloud services (e.g. virtual firewalls, encryption, two-factor authentication). As these controls may be disabled by default (e.g. optional security feature), the FIs will have to enable or implement the tools and controls that the FIs see as beneficial.

7.9 As cloud computing service providers may adopt multi-tenancy and data commingling architectures in order to process data for multiple customers, FIs should pay attention to the cloud service providers' abilities to segregate FIs data from other tenants.

7.10 FIs should also pay attention to the cloud service provider's abilities to segregate the multi-tenancy environments such that any change made to one of the tenant's environment will not affect other tenants.

7.11 The FIs should ensure data is protected on transmission between the FIs and the cloud service provider, and at rest on the cloud service provider. The FIs may consider encrypting their sensitive data using their own encryption tools independent from the cloud service provider, or at least ensure the cloud service provider do not keep the FIs' encryption key.

7.12 Any activities that require administrator or privilege account access over IaaS and PaaS should go through privilege account access management and remote access management process. Meanwhile for SaaS, activities that require administrator access on the back-end portal should subject to privilege account access management.

7.13 In the case of the cloud service provider encountering issues that lead to the FIs' services going offline, the expected Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of the cloud service provider should be treated similar to the duration that the FIs would have set if the services are implemented within their own infrastructure.

7.14 In the event of contract termination with the cloud service provider, either on expiry or ended prematurely, the FIs should have the contractual power and means to ensure that the cloud service provider promptly remove and/or destroy data stored at the cloud service provider's systems and backups at all location.

7.15 FIs should establish a cloud exit strategy in case of contract termination with the cloud service provider. This strategy should aim to minimise impact to the FIs' business operations caused by the termination, such as by identifying an alternate cloud service provider and requiring the existing cloud service provider to provide a sufficient transition period before full termination.

8. COUNTERPARTIES

8.1 Counterparties should be regarded as a third parties so the FIs should assess and determine the special requirements and arrangements in engaging with the counterparties instead of other third-parties.

8.2 As the nature of counterparty arrangement is similar to both IT Outsourcing and service provider arrangement, the FIs should take similar measures as outline in Paragraph 4 of this Guidelines. If the measures conflicts with the identified special requirements or arrangements in Paragraph 8.1 above, the FIs should document any possible limitations and to assess the risks. Any decision on risk acceptance should be supported with compensating measures, verified by the Risk Management function and endorsed by the Senior Management of the FIs.

8.3 The counterparty arrangement may be subjected to laws or regulations of the country where the counterparties operated. Therefore, the FIs should assess any potential conflicts between the requirements set by the counterparties and their regulators with the relevant laws in Brunei Darussalam including BDCB's notices and guidelines.

8.4 FIs participating on a financial market infrastructure platform or service, such as SWIFT and card service provider, might be required to comply with certain standards or policy requirements, such as PCI DSS and SWIFT CSP. The FIs should be able to demonstrate to BDCB their compliance to these requirements.

8.5 The FIs should also be mindful of any new compliance requirements from the financial market infrastructure from time to time. The FIs should be able to demonstrate their commitment to comply to the new requirements based on the FIs' risk assessment and deadline given by the financial market infrastructure platform.

9. AGENT MANAGEMENT

9.1 Some FIs may engage agents to represent the FIs to deliver their service to customers. If the agents are not considered as FIs' own personnel and have access to FIs' system, data or IT resources, the agents should be treated as third parties. In this case, Paragraph 3.6 and 3.7 of this Guidelines are applicable.

9.2 FIs that provides system access to their agents should ensure the user access given to the agents are restricted subject to risks and the FIs' user access management policy.

9.3 The FIs should provide segregated system or user interface dedicated for the agents and should not have access to back-end system.

9.4 Agents should ensure devices that are used to access or store FIs' and customer's personal data are authorised by the FIs and are configured securely. If the FIs do not provide IT assets to its agent, the FIs should require the agent to declare their devices and maintain list of the devices.

9.5 The FIs should establish policy or guidelines for the agents on safeguarding FIs' data and ensure the protection of customer personal data.

10. CYBER INSURANCE

10.1 For FIs that are considering to take cyber insurance, the FIs should assess their cyber risk posture and determine IT assets that are worth to be protected. These will help the FIs determine the right cyber insurance and coverage scope.

10.2 Cyber insurance can cover legal cost and recovery cost arising from cyber incident, but accountability still resides with the FIs. The FIs should manage reputational risk and other uncovered risk caused by cyber incident.

10.3 FIs that have taken cyber insurance may be required to provide information regarding their IT system and IT environment during underwriting, investigation, claim or audit process by their cyber insurer. The FIs should ensure there are non-disclosure agreement with the cyber insurer and their appointed auditor. Information should only be given as per required to perform the process above.

10.4 During any cyber incident, the FIs may be required to immediately inform their cyber insurer to be eligible for a claim. FIs should inform BDCB prior or concurrent to engaging their cyber insurer as part of their incident notification to BDCB pursuant to the Notice on Early Detection of Cyber Intrusion and Incident Reporting.

10.5 Depending on the scope of the cyber insurance, the insurer may hire experts to assist in the cyber incident investigation and resolution process. FIs should inform BDCB prior to agreeing to the arrangement as part of their incident progress update pursuant to the Notice on Early Detection of Cyber Intrusion and Incident Reporting.

MANAGING DIRECTOR
BRUNEI DARUSSALAM CENTRAL BANK

Issue Date: 16 Jamadilakhir 1443H / 20 January 2022M