Effective date: 30 June 2023

NOTICE FOR BANKS AND FINANCIAL INSTITUTIONS
NOTICE NO. TRS/N-1/2023/2

NOTICE ON TECHNOLOGY RISK MANAGEMENT

1. INTRODUCTION

1.1. This Notice is issued pursuant to section 54 of the Brunei Darussalam Central Bank Order, 2010 requiring banks and financial institutions (FIs) to implement the following:

1.1.1. Incorporation of IT risks in the Three Line of Defence functions;

1.1.2. Identification and review of critical systems;

1.1.3. Notification of system acquisition, development and integration;

1.1.4. Testing of new critical systems and system using artificial intelligence;

1.1.5. Maintain list of IT third party arrangement on critical systems; and

1.1.6. Perform self-assessment on IT risk management.

1.2. This Notice is applicable to banks and FIs licensed, registered or regulated under the following:

1.2.1. Banking Order, 2006;

1.2.2. Islamic Banking Order, 2008;

1.2.3. Insurance Order, 2006;

1.2.4. Takaful Order, 2008;

1.2.5. Finance Companies Act, Cap. 89; and

1.2.6. Securities Markets Order, 2013.

1.3. This Notice is also applicable to:

1.3.1 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

1.3.2 Perbadanan Tabung Amanah Islam Brunei established under the Perbadanan Tabung Amanah Islam Brunei Act (Cap. 163).

1.4 This Notice shall be read with Guidelines No. TRS/G-2/2022/1 on "Technology Risk Management" (hereinafter referred to as "Guidelines No. TRS/G-2/2022/1") and Guidelines No. TRS/G-3/2022/2 on "IT Third Party Risk Management" (hereinafter referred to as "Guidelines No. TRS/G-3/2022/2").

1.5 This Notice shall also be read in conjunction with the following:

1.5.1 Notice on Application for Approval of Outsourcing Arrangement for Insurance Companies and Takaful Operators (Notice No. TIU/N-1/2019/11);

1.5.2 Notice on Early Detection of Cyber Intrusion and Incident Reporting (Notice No. FTU/N-1/2017/1);

1.5.3 Notice on Measures for Non-Face-To-Face Customer Onboarding and Ongoing Customer Due Diligence (Notice No. FIU/N-1/2022/1);

1.5.4 Notice on Outsourcing for Capital Markets Services Licence Holders (Notice No. CMA/N-1/2020/15);

1.5.5 Notice on Providing Market Access to a Foreign Market (Notice No. CMA/N-2/2019/14);

1.5.6 Notice on Requirements for Payment Systems (Notice No. PSO/N-1/2020/1);

1.5.7 Notice for the Establishment of a Complaints Handling Function within Financial Institutions (Notice No. FCI/N1/2021/1);

1.5.8 FinTech Regulatory Sandbox Guidelines (Guideline No. FTU/G-1/2017/1);

1.5.9 Guidelines on Measures for Non-Face-To-Face Customer Onboarding and Ongoing Customer Due Diligence (Guidelines No. FIU/G-1/2022/1);

1.5.10 Guidelines on Online Distribution for Insurance Companies and Takaful Operators (Guideline No. TIU/G-1/2020/11);

1.5.11 Guidelines on Outsourcing Arrangement for Insurance Companies and Takaful Operators (Guideline No. TIU/G-1/2019/10);

1.5.12 Guidelines on Outsourcing for Banks; and

1.5.13 Guideline on Providing Market Access to a Foreign Market (Guideline No. CMU/G-2/2019/7).

1.6 This Notice shall take effect starting from 30 June 2023.

2. DEFINITIONS

2.1 For the purposes of this Notice, the following terms shall have the following meanings except where the context otherwise requires -

2.1.1 "application Programming Interface" or "API" refers to a software intermediary or set of programming codes that enables data transmission or add-on functionality between one software to another software;

2.1.2 "artificial intelligence" or "AI" refers to a software that provides automation capability for computer or machine to perform tasks that are normally performed by humans;

2.1.3 "Audit Committee" refers to a board-level committee which is responsible for oversight of the banks' and FIs' internal control and reporting process, including reviewing and approving audit plans and external auditors;

2.1.4 "Board" means the Board of Directors of a bank and FI;

2.1.5 "cloud services" refers to service and delivery model for enabling on-demand network access to a shared pool of configurable computing resources (servers, storage and services);

2.1.6 "contractors" refers to vendors, suppliers, service providers, outsourcing service providers and/or consultants that have formed contract with the banks and FIs to provide specific and relevant products or services to the bank and FIs. Contractors are usually effective during IT project or within time periods of the agreed contract(s);

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

2.1.8 "IT audit" refers to formal inspection and verification to assess whether IT standards, policies and guidelines are being complied with by the banks' and FIs' personnel. This includes implementing IT controls and ensuring target efficiency and effectiveness of IT systems and operations have been met;

2.1.9 "Open API" refers to publicly available API that provides a developer with programmatic access to a certain feature of the banks' and FIs' application or service;

2.1.10 "outsourcing service provider" refers to an individual or entity that provides outsourcing services to the banks and FIs. This includes a member of the group to which the institution belongs e.g. its Head Office, parent institution, another branch or related company, or an unrelated party, whether located in Brunei Darussalam or elsewhere;

2.1.11 "outsourcing" refers to an arrangement whereby a bank and FI engages in a third party (i.e. service provider) to provide the bank and FI with a service that may already or may conceivably be performed by the bank and FI itself which includes the following characteristics:

(a) the bank and FI is dependent on the service on an ongoing basis but excludes services that involve the provision of a finished product;

(b) the service is integral to the provision of a financial service by the bank and FI and/or the service is provided to the market by the service provider in the name of the bank and FI; and

(c) 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 bank and FI.

2.1.12 "penetration testing" refers to a type of testing by means of carrying out an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to its functions and data;

2.1.13 "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 organisation has or is likely to have access to;

2.1.14 "project" refers to a temporary endeavour undertaken to create a unique product or service. It has a defined scope and consists of sets of operations to deliver specific goals;

2.1.15 "Private API" refers to API that is limited for banks' and FIs' internal system or for third party system in which the banks and FIs and the third party have made a prior formal agreement on;

2.1.16 "second-line of defence function" refers to a business or control function designated to undertake second level roles (i.e. risk and compliance) in the three lines of defence governance model;

2.1.17 "Senior Management" refers to upper management or executive management of the banks and FIs, which is the highest level of management that are responsible to carry out direction from the board of directors and lead the organisation.

2.1.18 "service provider" refers to an individual or entity that provides a service to the banks and FIs, including a member of the group to which the banks and FIs belong to, e.g. its Head Office, parent insurer, another branch or related company, whether it is located in Brunei Darussalam or elsewhere;

2.1.19 "system" refers to information system used by the banks and FIs for performing their business operation, made up of hardware, software, network, and other IT component that deliver the functions;

2.1.20 "system acquisition" refers to the process of acquiring IT systems for the banks and FIs, through purchase or development;

2.1.21 "system development" refers to the process of developing software or application from scratch or based on minimal templates in order to better suit the banks' and FIs' requirements. This should be performed by the banks' and FIs' IT team (in-house) or third party (outsourced);

2.1.22 "system integration" refers to linking a system with another internal or external system or component directly or through an intermediary;

2.1.23 "three lines of defence" refers to a governance model that provides an effective way to enhance communications of risk management and control in the banks and FIs by clarifying essential roles and duties into three lines: operational management, risk and compliance, and assurance or internal audit;

2.1.24 "technology risk" or "IT risk" refers to risks caused by IT and IT-related failures or vulnerabilities, which can impact the banks' and FIs' systems, data and business processes;

2.1.25 "users" refers to individual, personnel or stakeholders that uses banks' and FIs' IT system and/or IT assets for their business operations and activities;

2.1.26 "user acceptance testing" or "UAT" refers to final stage of system testing that involves users or clients of the systems in validating their expectations to the functionality of the system;

2.1.27 "vendor" refers to an individual or entity that offers products or services. The vendor usually deals with business relationships between clients, suppliers and service providers;

2.1.28 "vulnerability" refers to a weakness in IT asset and system that can be exploited by threat; and

2.1.29 "vulnerability assessment" or "VA" refers to the process of identifying, quantifying, and prioritising (or ranking the vulnerabilities) in a system.

2.2 Any expression used in this Notice shall, except where expressly defined in this Notice or where the context requires otherwise, have the same meaning as in the BDCB Order, 2010.

3. IT RISK, IT COMPLIANCE AND IT AUDIT

3.1 Banks and FIs shall establish a technology risk management framework, or incorporate oversight and execution of technology risk management activities into their overall risk management framework. This shall include the implementation of appropriate controls for the management of IT risk including the conduct of risk assessment.

3.2 Banks and FIs shall include IT audits in their annual audit plan, which shall be approved by the Audit Committee or equivalent.

3.3 Banks and FIs shall assess that IT-related policies, standards, guidelines and procedures are being understood and adhered to by the banks' and FIs' personnel, through a designated second-line of defence function. This includes performing compliance reviews, regular reporting of compliance breaches, and conducting awareness exercises on compliance to rules and regulations.

4. CRITICAL SYSTEMS

4.1 Banks and FIs shall identify and maintain a list of critical systems from all of their new and existing IT systems. The list shall be approved by Senior Management, and submitted to BDCB with at least the following details:

4.1.1 Name of the IT systems;

4.1.2 Type of systems (e.g. web, smartphone, background services);

4.1.3 Function or purpose of the IT systems;

4.1.4 Initial date when the system was implemented and operational;

4.1.5 Name and version of the software or applications used for the systems;

4.1.6 Name of the manufacturer, developer and/or vendor that provides the system;

4.1.7 Ownership of the systems (i.e. business units accountable for the system);

4.1.8 Type of users of the systems (e.g. internal, customer, agent); and

4.1.9 Location of the systems (e.g. office premise, local data centre, cloud services).

4.2 Banks and FIs shall review the criticality of their IT systems annually. In addition to the aforementioned annual reviews, banks and FIs shall also review the criticality of their IT systems when there is major change to their IT systems such as system upgrade with additional features, and migration to cloud. The list of critical systems shall be updated, and be submitted to BDCB no later than **three (3) months** after the end of every financial year.

5. SYSTEM ACQUISITION, DEVELOPMENT AND INTEGRATION

5.1 Banks and FIs shall notify BDCB prior to acquiring or developing new critical systems or application, introduction of new features within the critical system or application that may potentially affect the customer's experience and personal data. Banks and FIs shall furnish the following information to BDCB before engaging the vendor or third-party selection, and start of the software development project:

5.1.1 Rationale of the proposal (to include if the proposal is aligned to the banks' and FIs' IT strategy);

5.1.2 Details on improvements or changes to banks' and FIs' services and business processes following the implementation of the new system or application;

5.1.3 Preliminary risk assessment and analysis of the new system and application, mitigating strategies to address concerns identified after the risk assessment and analysis;

5.1.4 Proposed critical end-to-end process flow on the front-end and back-end side;

5.1.5 Proposed architecture diagram and/or data-flow diagram that will help to explain the interrelationship between banks and FIs applications/modules/components;

5.1.6 Name of all IT third parties involved, and its relationship in the system acquisition or development;

5.1.7 Preliminary exit strategy that outlines action in the event that the project fails, vendor termination and other unforeseen circumstances; and

5.1.8 Proposed details on migration of data including data sanity check and data cleansing (if applicable).

5.2 Banks and FIs shall also notify BDCB prior to integrating a third-party system or service with any of their critical systems, including using third party API, that may have potential material impact to the customer. Banks and FIs shall furnish the following information to BDCB before finalising their engagement with any third party:

5.2.1 Rationale on the integration including expectation from the third-party system;

5.2.2 Details on expected change in banks' and FIs' service delivery and/or business process following the system integration;

5.2.3 Preliminary risk assessment and analysis on the system integration and action plan to address concerns identified from the risk assessment and analysis;

5.2.4 Proposed critical end-to-end process flow between the third-party system and banks and FIs system;

5.2.5 Details on technology and methodology used for the integration;

5.2.6 Due diligence and assessment on the third party and their vendors or suppliers;

5.2.7 Preliminary exit strategy that outlines action in the event that the integration fails and other unforeseen circumstances; and

5.2.8 Proposed details on migration of data including data sanity check and data cleansing (if applicable).

5.3 If banks and FIs allow a third party to integrate banks' and FIs' service into the third party's system using API, the banks and FIs shall maintain a list of all integration done and to submit the list to BDCB annually, no later than **three (3) months** after the end of every financial year, or as when required by BDCB.

5.4 In the case of Open API, the banks and FIs shall notify BDCB prior to publishing their Open API on a website or portal. Subsequent to this, the banks and FIs shall maintain list of all download or subscription of the Open API, and the list must be submitted to BDCB whenever requested.

5.5 For new critical systems development or acquisition, banks and FIs shall perform UAT that involves all intended user roles and covers activities that are expected to be performed by each user roles on the system. The UAT scripts and results shall be reviewed by quality control, assurance or personnel that is independent from the project implementation team.

5.6 Banks and FIs shall also perform vulnerability assessment and penetration testing on newly developed or acquired critical systems prior to going live.

5.7 In the event there are open items from the UAT, vulnerability assessment and/or penetration testing such as failed UAT scenarios or detected vulnerabilities, the banks and FIs shall ensure these open items are rectified before going live, especially items that pose critical and high risks. Low and medium risks open items shall be rectified based on the banks' and FIs' internal policy.

6. IT SYSTEM WITH ARTIFICIAL INTELLIGENCE

6.1 Prior to implementing or adding artificial intelligence into their critical system, banks and FIs shall identify the maturity level of their artificial intelligence system according to paragraph 4.13 of the Guidelines No. TRS/G-2/2022/1. Banks and FIs shall notify BDCB prior to implementing or adding artificial intelligence at Levels 3, 4 and 5.

6.2 Banks and FIs shall test the artificial intelligence system based on the period and parameters set in Paragraph 4.13.11 and 4.13.13 of the Guidelines No. TRS/G-2/2022/1. Banks and FIs shall provide BDCB the test result with supporting data every month until the aforementioned condition has been fulfilled.

6.3 During the testing period, banks and FIs shall supervise or review any automated processes to allow intervention and corrective actions if necessary. Details of these interventions shall be included in the test results.

7. IT THIRD PARTY ARRANGEMENT

7.1 Banks and FIs shall notify BDCB prior to signing a contract with an IT outsourcing service provider, counterpart and/or cloud service that involves critical systems. Banks and FIs shall furnish the following information to BDCB:

7.1.1 Details of third parties involved in the arrangement;

7.1.2 Details of the third-party arrangement including the purpose, type of service and service period;

7.1.3 Checklist of responsibilities of the third parties and the banks and FIs in the arrangement;

7.1.4 Information on due diligence assessment on the third parties involved in the arrangement;

7.1.5 Preliminary risk assessment and analysis for the third-party arrangement and mitigation strategies; and

7.1.6 Preliminary exit strategy that outlines actions in the event that the third-party arrangement fails.

7.2 Banks and FIs shall submit an updated list of all IT third party arrangements as defined in Guidelines No. TRS/G-3/2022/2 to BDCB no later than **three (3) months** after the end of every financial year.

8. SELF-ASSESSMENT ON IT RISK MANAGEMENT

8.1 Banks and FIs shall perform an annual self-assessment to evaluate their inherent risks and IT management maturity level based on BDCB's Technology Risk Assessment Framework (T-RAF). The annual self-assessment shall be submitted to BDCB no later than 30 June of every year, or when BDCB requires.

8.2 Banks and FIs shall review, and perform a gap analysis and risk assessments against the guidelines contained in BDCB's Guidelines No. TRS/G-2/2022/1 and Guidelines No. TRS/G-3/2022/2. Based on the gaps and risk assessments, banks and FIs shall establish action plans in addressing identified gaps and risks.

8.3 Banks and FIs shall observe new and existing laws and regulations related to IT, information security and personal data protection, and shall assess compliance with the applicable laws and regulations.

MANAGING DIRECTOR
BRUNEI DARUSSALAM CENTRAL BANK

Issue Date: 23 Rejab 1444H / 14 February 2023M