NOTICE FOR BANKS
NOTICE NO. TRS/N-2/2025/1

NOTICE ON COMPLIANCE AND SECURITY BY DESIGN

1. INTRODUCTION

1.1. This Notice is issued pursuant to section 66 of the Banking Act, Chapter 95 and section 66 of the Islamic Banking Act, Chapter 168 and applies to all banks and Islamic banks (banks) in Brunei Darussalam.

1.2. The Brunei Darussalam Central Bank (BDCB) may, at its discretion, take supervisory action against any banks if it fails to comply with any provisions under this Notice.

1.3. This Notice requires banks to incorporate and practice compliance and security by design approaches throughout the project and critical system development lifecycle. This is to ensure security and compliance risks are assessed and addressed from the planning phase to the end of a critical system's lifecycle. The following provisions of this Notice shall apply to all identified critical systems.

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

1.4.1 Notice on Technology Risk Management (Notice No. TRS/N-1/2023/2);

1.4.2 Notice on Early Detection of Cyber Intrusion and Incident Reporting (Notice No. TRS/N-1/2020/1);

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

1.4.4 Guidelines on Technology Risk Management (Guidelines No. TRS/G-2/2022/1);

1.4.5 Guidelines on Information Technology Third Party Risk Management (Guidelines No. TRS/G-3/2022/2); and

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

1.5 This Notice shall take immediate effect.

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 "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;

2.1.2 "critical system" refers to any system that supports the provision of banks' services, where failure of the system can significantly impair the banks' provision of services to its customers or stakeholders, business operations, financial

position, reputation or compliance with applicable laws and regulatory requirements;

2.1.3 "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;

2.1.4 "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;

2.1.5 "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;

2.1.6 "independent internal function" refers to a business or control functions that are not directly involved in the day-to-day IT operations;;

2.1.7 "security features" refers to system features or configurations that are made available to users as security measures, such as transaction limit, and SMS alert feature;

2.1.8 "security controls" refers to coding or configurations set by the banks as security measures such as audit trail and software token, or back-end feature provided for banks for security purpose, such as fraud transaction alert and user access control;

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

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

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

2.1.12 "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;

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

2.1.14 "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 Banking Act, Chapter 95 or Islamic Banking Act, Chapter 168.

3. PLANNING AND DESIGN

3.1 Banks shall determine whether a proposed system is a critical system during the initiation or planning phase. A critical system is subject to the necessary notifications and measures in accordance with Notice No. TRS/N-1/2020/1 and Notice No. TRS/N-1/2023/2.

3.2 Banks shall conduct risk assessments and implement appropriate measures to address identified risks throughout a critical system's entire project and system lifecycle.

3.3 Risk management measures shall be applied continuously across all phases of a critical system's lifecycle. These measures shall remain relevant and incorporate new risks that may emerge throughout the lifecycle.

3.4 Banks shall identify and assess all applicable laws and regulations, including those relevant to the users of a critical system. Business units shall also be consulted to ensure compliance with laws and regulations specific to their operations.

3.5 Banks shall establish a security baseline based on international standards and/or industry best practices. This baseline shall serve as a reference for the implementation of security controls and features within their critical system.

3.6 The security features of critical systems shall be configured as securely as possible, such as by setting minimal access, and minimum thresholds for alerts or restrictions as default. Where applicable, the banks shall provide options for users to adjust the configurations and/or thresholds according to their risk appetite.

3.7 An independent internal function within the banks shall:

3.7.1 review all critical systems plans and designs for compliance and security;

3.7.2 review any subsequent changes and/or updates to the plans and designs; and

3.7.3 monitor, review, and assess the implementation of compliance and security measures throughout every phase of a critical systems lifecycle, including maintenance and end of life.

4. TESTING AND DEPLOYMENT

4.1 In addition to UAT, banks shall establish testing scripts or scenarios to test and validate security controls and features of its critical systems, ensuring that they support compliance with relevant laws and regulations. This includes, but is not limited to, the following:

4.1.1 Vulnerability Assessment and Penetration Testing;

4.1.2 Source code security review (for in-house developed systems);

4.1.3 In-app security feature testing (e.g. digital token, device binding);

4.1.4 Security feature configuration testing (e.g. alert thresholds, transaction limits);

4.1.5 Validation of system processes and workflows for alignment with business operations and legal compliance; and

4.1.6 Other specialised testing relevant to the nature of the system (e.g. Biometric verification and Artificial Intelligence functionality).

4.2 These tests may be conducted independently of the UAT. All identified issues shall be resolved based on the associated risk level. Critical and high-risk issues shall be resolved before a critical system's go-live, while remaining issues shall be resolved based on an appropriate timeline.

4.3 An independent internal function shall track and monitor the resolution progress of issues identified during testing.

4.4 Banks shall provide awareness to all users, including customers (for customer-facing systems only) to ensure that they are informed about the security features and controls available on the critical system. This may be accomplished through official announcements, training, disclosure during onboarding, and/or sufficient user manuals.

5. MAINTENANCE AND CHANGES

5.1 Banks shall be required to treat security updates, including bug fixes and security patches as changes. The security updates shall be recorded, assessed, tested and authorised based on the banks' change management policies and procedures.

5.2 Banks shall ensure that the software updates and/or changes do not degrade the security of the critical system, and/or affect compliance to relevant laws and regulations. Therefore, change management processes shall include appropriate testing and validation of security and compliance of the critical system, where required.

5.3 All changes to security features including the introduction of new security features shall be communicated to affected users in accordance with Paragraph 4.4 above.

6. END OF LIFE

6.1 Banks shall identify all applicable laws and regulations relevant to a critical system's end of life phase. This includes obligations such as data retention under personal data protection and business record-keeping laws.

6.2 Banks shall inform all affected users in advance prior to system decommissioning. Sufficient time shall also be provided for all affected users to take any necessary actions before the closure of the critical system, such as data migration or clearing of balances.

6.3 Banks shall ensure security measures are implemented during the critical system's end of life for safe termination and disposal.

MANAGING DIRECTOR
BRUNEI DARUSSALAM CENTRAL BANK

Issue Date: 11 Safar 1447H / 5 August 2025M