Monetary Authority of Singapore

Consultation Paper
P012-2026 – June 2026

Consultation Paper on Proposed Amendments to Notices on Technology Risk Management

Contents

1. Preface

1.1. The Monetary Authority of Singapore ("MAS") proposes to amend MAS Notices on Technology Risk Management (FSM-N03, FSM-N05, FSM-N07, FSM-N09, FSM-N11, FSM-N13, FSM-N17, FSM-N19, FSM-N21, FSM-N23 and FSM-N25) (the "Notice") to strengthen the technology resilience of the financial services sector.

1.2. The proposed amendments to the Notice will require the relevant Financial Institutions (FIs) to implement measures across the following key areas:

(a) IT asset management
(b) IT risk assessment and monitoring
(c) Capacity planning and management
(d) Change management controls
(e) Continuous system and security monitoring
(f) Immutable and offline data backup
(g) Incident management

1.3. MAS invites comments from all interested parties on the proposed requirements.

Please note that all submissions received will be published and attributed to the respective respondent unless they expressly request MAS not to do so. As such, if respondents would like (a) their whole submission or part of it (but not their identity), or (b) their identity along with their whole submission, to be kept confidential, please expressly state so in the submission to MAS. MAS will only publish non-anonymous submissions. In addition, MAS reserves the right not to publish any submission received where MAS considers it not in the public interest to do so, such as where the submission appears to be libelous or offensive.

1.4. Please submit written comments by 31 July 2026 via the *FormSG link*.

1.5 Should you encounter any technical difficulties in your submission, please send your enquiry to *techrisk@mas.gov.sg*.

2. Proposed amendments to the Notice

2.1. The following sets out the key enhancements to the Notice.

IT asset management

2.2. IT asset management entails the planning, tracking, handling and monitoring of an organisation's IT assets to maintain effective control and oversight across their entire lifecycle, from acquisition and deployment, to decommissioning and disposal. This allows FIs to optimise utilisation and cost, as well as support FIs' business objectives and risk management, thereby engendering technology and operational resilience.

2.3. A key requirement under IT asset management is the maintenance of a proper inventory of IT assets. This provides FIs with an accurate view of their IT operating environment and supports other IT processes, including vulnerability and patch management, technology obsolescence management, cryptographic key management and digital certificate management. In addition, the inventory facilitates the identification and management of risks relating to specific third-party components and supply chain issues.

2.4. MAS proposes that FIs maintain a comprehensive and up-to-date inventory of all of their IT assets, which includes hardware, software, cryptographic assets, open-source and third-party components.

Question 1: MAS seeks comments on the proposed scope of the IT asset inventory and the information to be recorded and maintained by FIs.

IT risk assessment and monitoring

2.5. IT risk assessment and monitoring are essential to enable effective risk management in FIs. In conducting the IT risk assessment, FIs must consider the threats and vulnerabilities that their systems may be subject to, including those associated with their IT supply chains and the use of artificial intelligence, and assess the risks that could arise from these threats and vulnerabilities, including the potential likelihood and impact of such risks affecting the FIs' operations or the services provided to its customers (the "identified risks"), in accordance with the FI's established risk assessment criteria.

2.6. MAS proposes that FIs establish and maintain a framework and process to conduct regular IT risk assessments that cover these areas and implement risk mitigation measures that are commensurate with the identified risks (the "risk mitigation measures").

2.7. MAS also proposes that FIs maintain an IT risk register that records (1) the material identified risks, (2) the risk owners who will be accountable for managing the material identified risks, and (3) the measures to mitigate the material identified risks. Additionally, FIs must establish and maintain key

risk indicators (KRIs) to effectively monitor the material identified risks and the effectiveness of the measures to mitigate the material identified risks.

Question 2:	*MAS seeks comments on the proposed scope of the IT risk assessment, the information to be maintained in the IT risk register and whether specific KRIs should be specified in the Notice for the monitoring of material identified risks.*

Capacity planning and management

2.8. Inadequate system capacity planning and management can lead to service degradation or disruption. It is important that FIs proactively plan and manage system capacity to meet their operational and business needs, and to cater for future growth.

2.9. MAS proposes that FIs establish a framework and process to ensure that the capacity of all critical systems, and the systems that the critical systems depend on, are sufficient to meet business needs, including projected business growth and potential surges in customer traffic.

Question 3:	*MAS seeks comments on the proposed capacity planning and management requirements, including whether a specific frequency should be prescribed for capacity planning*.

Change management controls

2.10. MAS has noted that a significant number of IT incidents in FIs were attributed to poor change management. The lapses observed include insufficient risk and impact assessment of changes, poor understanding of system dependencies, inadequate testing of changes, and the absence of effective change recovery plans. In addition, it is essential that FIs implement controls to prevent unauthorised changes, carry out robust testing and validation of system changes to minimise the introduction of system defects and misconfigurations to the production environment, and have in place effective change recovery plans to deal with potential issues during the change implementation.

2.11. MAS proposes that FIs must implement effective controls to prevent unauthorised system changes so as to maintain system integrity and availability.

2.12. FIs are also required to establish and maintain a framework and process to assess the risks arising from proposed changes to their systems prior to implementation. Such assessments must evaluate the potential impact arising from the failure or incorrect implementation of the proposed changes, including the impact on upstream and downstream systems. FIs must implement risk mitigation measures that are commensurate with the risks identified.

2.13. Additionally, FIs must carry out testing for all changes to critical systems before they are implemented in the production environment. FIs must have in place effective change recovery measures to recover any critical system affected by any issue arising during or after change implementation.

Continuous system and security monitoring

2.14. MAS has observed that a number of major IT incidents have also been attributed to lack of monitoring, delayed detection and/or slow response to rectify the causes of the incidents, such as those related to capacity, performance or cybersecurity. The incidents could have been averted if the FIs had promptly discovered and responded to the issues.

2.15. MAS proposes that FIs establish and maintain a framework and process to continuously monitor all critical systems for timely detection and response to issues affecting the system performance or security**.** FIs must ensure that the framework and process include, at a minimum: (a) defined indicators and thresholds that trigger alerts; and (b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issue.

Question 4:	*MAS seeks comments on the proposed requirements on continuous system and security monitoring, including the scope of monitoring, indicators and thresholds, response and remedial action frameworks, and key implementation considerations.*

Immutable or offline data backup

2.16. System bugs, cyber-attacks (e.g. ransomware), and human errors can lead to loss and corruption of data that is essential to the delivery of FIs' business services. Beyond real-time data replication to achieve high availability, implementing immutable and/or offline data backup forms an important part of a resilient data protection strategy to enable data recovery in the event that the production data is corrupted, tampered with, or made inaccessible. This is important to ensure the timely and reliable resumption of services.

2.17. MAS proposes that FIs must maintain an immutable or offline backup of data that are crucial for supporting the FIs' relevant business services, to enable timely and reliable resumption of those services in the event the production data is corrupted, tampered with, or made inaccessible.

Question 5:	*MAS seeks comments on whether FIs should be required to maintain data backups that are both immutable and offline, or whether maintaining either form of backup would suffice to enable the timely and reliable resumption of the FIs' relevant business services. MAS also welcomes suggestions on alternative approaches or strategies to achieve the same objective.*
Question 6:	*MAS seeks comments on whether there is a need to prescribe the backup frequency for immutable and offline data backup respectively.*

Incident management

2.18. In the event of an incident, FIs need a well-defined process and procedure to recover their systems and the affected services, so as to minimise the impact of the disruption and to maintain business and operational continuity.

2.19. MAS proposes that FIs establish an incident management framework and process, with clearly defined roles and responsibilities for managing and responding to IT incidents, including procedures to collect and preserve evidence for incident investigation, stakeholder and customer communication, and prompt notification to FIs' senior management upon identification of the IT incident to enable informed decision-making.

Question 7:	*MAS seeks comments on the proposed areas that are to be covered in the incident management framework, and whether there are other key areas that should be included in the Notice.*

Monitoring of unscheduled downtime

2.20. The current Notice requires FIs to ensure that the total unscheduled downtime for each critical system does not exceed 4 hours within any 12-month period. Accordingly, FIs are required to monitor and document any such downtime that affects their operations or services to customers. However, MAS has observed that some FIs did not account for partial and intermittent disruptions that affected their operations or services to customers, which undermines the intent of the original requirement.

2.21. In this regard, MAS is proposing to make it clear and explicit in the requirement that any partial or intermittent disruption must be included in the computation of unscheduled downtime for critical systems.

Question 8:	*MAS seeks comments on whether the phrase "partial or intermittent disruption", as set out in the revised Notice, is sufficiently clear to enable consistent classification of disruption scenarios in practice for the purposes of computing unscheduled downtime of critical systems. Respondents are invited to suggest terms and definitions that will enhance the clarity of the requirement.*

Effective Date of the Notice

2.22. MAS proposes that the requirements set out in the revised Notice shall take effect **12 months** after the date that the finalised Notice is published.

Question 9: *MAS seeks comments on whether the implementation timeline for the requirements of the Notice is sufficient.*

2.23. MAS seeks feedback on Questions 1 to 9, as well as other comments on the proposed amendments to the Notice, taking into account emerging risk developments, including AI-enabled threats. Where respondents envisage challenges in observing specific requirements, respondents are encouraged to propose alternatives to the drafting of the requirements and the rationale for doing so.

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N03

Notice to licensed insurers other than captive insurers, ~~and~~ marine mutual insurers and Special Purpose Reinsurance Vehicles
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "**Act**") and **applies to all licensed insurers** under the Insurance Act 1966, other than captive insurers, marine mutual insurers and Special Purpose Reinsurance Vehicles (each an "**insurer**").

Definitions

2 **For the purpose of this Notice—**

"business service" means an external-facing service that is provided to the insurer's customers;
[FSM-N03 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;
[FSM-N03 (Amendment) 2026]

"captive insurer" has the meaning given by section 2 of the Insurance Act 1966;

"critical system", in relation to an insurer, means a system, the failure of which will cause significant disruption to the operations of the insurer or materially impact the insurer's service to its customers, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;

[FSM-N03 (Amendment) 2026]

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N03 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of customer information~~;

[FSM-N03 (Amendment) 2026]

"licensed insurer" has the meaning given by section 2 of the Insurance Act 1966;

"marine mutual insurer" has the meaning given by section 2 of the Insurance Act 1966;

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N03 (Amendment) 2026]

"relevant business service" means a business service of an insurer which, if disrupted, will have a significant impact on the insurer's customers or other financial institutions that depend on the business service;

[FSM-N03 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the insurer's operations or materially impacts the insurer's service to its customers, or compromises the confidentiality of customer information;

[FSM-N03 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N03 (Amendment) 2026]

"Special Purpose Reinsurance Vehicle" has the meaning given by regulation 2 of the Insurance (General Provisions and Exemptions for Special Purpose Reinsurance Vehicles) Regulations 2018;

[FSM-N03 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within an insurer's IT infrastructure;

[FSM-N03 (Amendment) 2026]

~~"system malfunction" means a failure of any of the insurer's critical systems.~~

[FSM-N03 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N03 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 An insurer must put in place a framework and process to identify critical systems.

5 An insurer must make all reasonable effort to maintain high availability for critical systems. The insurer must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the insurer's operations or the insurer's service to its customers. The insurer must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the insurer's operations or service to its customers~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N03 (Amendment) 2026]

6 An insurer must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The insurer must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N03 (Amendment) 2026]

7 An insurer must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N03 (Amendment) 2026]

8 An insurer must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the insurer's operations or the services provided to its customers. The insurer must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the insurer's operations or the services provided to its customers (the "identified risks"), in accordance with the insurer's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N03 (Amendment) 2026]

9 An insurer must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N03 (Amendment) 2026]

10 An insurer must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N03 (Amendment) 2026]

11 An insurer must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in customer traffic.

[FSM-N03 (Amendment) 2026]

12 An insurer must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The insurer must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N03 (Amendment) 2026]

13 An insurer must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N03 (Amendment) 2026]

14 An insurer must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the insurer's operations or the services provided to its customers, prior to implementation. The insurer must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and downstream systems. The insurer must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N03 (Amendment) 2026]

15 An insurer must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The insurer must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N03 (Amendment) 2026]

16 An insurer must ensure the availability of data supporting relevant business services. The insurer must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N03 (Amendment) 2026]

17 An insurer must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the insurer's operations or services to its customers;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the insurer's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the insurer's customers need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N03 (Amendment) 2026]

~~7~~18 An insurer must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 An insurer must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain—

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the insurer's—

i. compliance with laws and regulations applicable to the insurer;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 An insurer must implement effective IT controls to protect customer information from unauthorised access or disclosure.

[FSM-N03 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments**:

1. FSM-N03 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

An insurer must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N03 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N05

Notice to banks in Singapore
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all banks in Singapore (each a "Bank").

Definitions

2 For the purpose of this Notice —

"banking business" has the meaning given by section 2(1) of the Banking Act 1970;

"bank in Singapore" has the meaning given by section 2(1) of the Banking Act 1970;

"business service" means an external-facing service that is provided to a Bank's customers;

[FSM-N05 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;

[FSM-N05 (Amendment) 2026]

"critical system", in relation to a Bank, means a system, the failure of which will cause significant disruption to the operations of the Bank or materially impact the Bank's service to its customers, such as a system which —

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;

[FSM-N05 (Amendment) 2026]

"customer", in relation to a Bank, includes the Monetary Authority of Singapore or any monetary authority or central bank of any other country or territory, and any company which carries on a banking business, a merchant banking business or an investment banking business;

"customer information", in relation to a Bank, means —

(a) any information relating to, or any particulars of, an account of a customer of the Bank, whether the account is in respect of a loan, investment or any other type of transaction, but does not include any information that is not referable to any named customer or group of named customers; or

(b) deposit information;

"deposit information", in relation to a Bank, means any information relating to —

(a) any deposit of a customer of the Bank;

(b) funds of a customer under management by the Bank; or

(c) any safe deposit box maintained by, or any safe custody arrangements made by, a customer with the Bank,

but does not include any information that is not referable to any named person or group of named persons;

"funds of a customer under management" means any funds or assets of a customer (whether of the Bank or any financial institution) placed with that Bank for the purpose of management or investment;

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N05 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of customer information~~;

[FSM-N05 (Amendment) 2026]

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N05 (Amendment) 2026]

~~"permitted business" has the meaning given by section 55Q of the Banking Act 1970~~

[FSM-N05 (Amendment) 2026]

"relevant business service" means a business service of a Bank which, if disrupted, will have a significant impact on the Bank's customers or other financial institutions that depend on the business service;

[FSM-N05 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the ~~b~~Bank's operations, ~~or~~ materially impacts the Bank's service to its customers, or compromises the confidentiality of customer information;

[FSM-N05 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N05 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a Bank's IT infrastructure;

[FSM-N05 (Amendment) 2026]

~~"system malfunction" means a failure of any of the Bank's critical systems.~~

[FSM-N05 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N05 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A Bank must put in place a framework and process to identify critical systems.

5 A Bank must make all reasonable effort to maintain high availability for critical systems. The Bank must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the Bank's operations or the Bank's service to its customers. The Bank must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the Bank's operations or service to its customers~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N05 (Amendment) 2026]

6 A Bank must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be~~

~~restored.~~ The Bank must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N05 (Amendment) 2026]

7 A Bank must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N05 (Amendment) 2026]

8 A Bank must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the Bank's operations or the services provided to its customers. The Bank must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the Bank's operations or the services provided to its customers (the "identified risks"), in accordance with the Bank's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N05 (Amendment) 2026]

9 A Bank must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N05 (Amendment) 2026]

10 A Bank must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N05 (Amendment) 2026]

11 A Bank must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in customer traffic.

[FSM-N05 (Amendment) 2026]

12 A Bank must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The Bank must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N05 (Amendment) 2026]

13 A Bank must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N05 (Amendment) 2026]

14 A Bank must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the Bank's operations or the services provided to its customers, prior to implementation. The Bank must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and downstream systems. The Bank must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N05 (Amendment) 2026]

15 A Bank must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The Bank must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N05 (Amendment) 2026]

16 A Bank must ensure the availability of data supporting relevant business services. The Bank must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N05 (Amendment) 2026]

17 A Bank must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the Bank's operations or services to its customers;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the Bank's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the Bank's customers need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N05 (Amendment) 2026]

~~7~~18 A Bank must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 A Bank must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the Bank's –

i. compliance with laws and regulations applicable to the Bank;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A Bank must implement effective IT controls to protect customer information from unauthorised access or disclosure.

[FSM-N05 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments:**

1. FSM-N05 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A Bank must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N05 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N07

Notice to credit card or charge card licensees in Singapore
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all credit card or charge card licensees in Singapore.

Definitions

2 For the purpose of this Notice —

"business service" means an external-facing service that is provided to a credit card or charge card licensee's customers;

[FSM-N07 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;

[FSM-N07 (Amendment) 2026]

"credit card or charge card licensee" means a person who is licensed to carry on the business of issuing credit cards or charge cards, or both, in Singapore under section 57B of the Banking Act 1970;

"critical system", in relation to a credit card or charge card licensee, means a system, the failure of which will cause significant disruption to the operations of the credit card or charge card licensee or materially impact the credit card or charge card licensee's service to its customers, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;

[FSM-N07 (Amendment) 2026]

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N07 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of customer information~~;

[FSM-N07 (Amendment) 2026]

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N07 (Amendment) 2026]

"relevant business service" means a business service of a credit card or charge card licensee which, if disrupted, will have a significant impact on the credit card or charge card licensee's customers or other financial institutions that depend on the business service;

[FSM-N07 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the credit card or charge card licensee's operations, ~~or~~ materially impacts the credit card or charge card licensee's service to its customers, or compromises the confidentiality of customer information;

[FSM-N07 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N07 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a credit card or charge card licensee's IT infrastructure;

[FSM-N07 (Amendment) 2026]

~~"system malfunction" means a failure of any of the credit card or charge card licensee's critical systems.~~

[FSM-N07 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N07 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A credit card or charge card licensee must put in place a framework and process to identify critical systems.

5 A credit card or charge card licensee must make all reasonable effort to maintain high availability for critical systems. The credit card or charge card licensee must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the credit card or charge card licensee's operations or the credit card or charge card licensee's service to its customers. The credit card or charge card licensee must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the credit card or charge card licensee's operations or service to its customers~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N07 (Amendment) 2026]

6 A credit card or charge card licensee must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The credit card or charge card licensee must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N07 (Amendment) 2026]

7 A credit card or charge card licensee must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N07 (Amendment) 2026]

8 A credit card or charge card licensee must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the credit card or charge card licensee's operations or the services provided to its customers. The credit card or charge card licensee must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the credit card or charge card licensee's operations or the services provided to its customers (the "identified risks"), in accordance with the credit card or charge card licensee's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N07 (Amendment) 2026]

9 A credit card or charge card licensee must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N07 (Amendment) 2026]

10 A credit card or charge card licensee must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N07 (Amendment) 2026]

11 A credit card or charge card licensee must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in customer traffic.

[FSM-N07 (Amendment) 2026]

12 A credit card or charge card licensee must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The credit card or charge card licensee must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N07 (Amendment) 2026]

13 A credit card or charge card licensee must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N07 (Amendment) 2026]

14 A credit card or charge card licensee must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the credit card or charge card licensee's operations or the services provided to its customers, prior to implementation. The credit card or charge card licensee must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and

downstream systems. The credit card or charge card licensee must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N07 (Amendment) 2026]

15 A credit card or charge card licensee must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The credit card or charge card licensee must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N07 (Amendment) 2026]

16 A credit card or charge card licensee must ensure the availability of data supporting relevant business services. The credit card or charge card licensee must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N07 (Amendment) 2026]

17 A credit card or charge card licensee must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the credit card or charge card licensee's operations or services to its customers;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the credit card or charge card licensee's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the credit card or charge card licensee's customers need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N07 (Amendment) 2026]

~~7~~18 A credit card or charge card licensee must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 A credit card or charge card licensee must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the credit card or charge card licensee's –

i. compliance with laws and regulations applicable to the credit card or charge card licensee;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A credit card or charge card licensee must implement effective IT controls to protect customer information from unauthorised access or disclosure.

[FSM-N07 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments**:

1. FSM-N07 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A credit card or charge card licensee must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N07 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N09

Notice to finance companies
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all finance companies.

Definitions

2 For the purpose of this Notice —

"business service" means an external-facing service that is provided to a finance company's customers;
[FSM-N09 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;
[FSM-N09 (Amendment) 2026]

"critical system", in relation to a finance company, means a system, the failure of which will cause significant disruption to the operations of the finance company or materially impact the finance company's service to its customers, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;
[FSM-N09 (Amendment) 2026]

"finance company" has the meaning given by section 2 of the Finance Companies Act 1967;

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N09 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of customer information~~;

[FSM-N09 (Amendment) 2026]

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N09 (Amendment) 2026]

"relevant business service" means a business service of a finance company which, if disrupted, will have a significant impact on the finance company's customers or other financial institutions that depend on the business service;

[FSM-N09 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the finance company's operations, ~~or~~ materially impacts the finance company's service to its customers, or compromises the confidentiality of customer information;

[FSM-N09 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N09 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a finance company's IT infrastructure;

[FSM-N09 (Amendment) 2026]

~~"system malfunction" means a failure of any of the finance company's critical systems.~~

[FSM-N09 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N09 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A finance company must put in place a framework and process to identify critical systems.

5 A finance company must make all reasonable effort to maintain high availability for critical systems. The finance company must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the finance company's operations or the finance company's service to its customers. The finance company must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the finance company's operations or service to its customers~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N09 (Amendment) 2026]

6 A finance company must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The finance company must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N09 (Amendment) 2026]

7 A finance company must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N09 (Amendment) 2026]

8 A finance company must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the finance company's operations or the services provided to its customers. The finance company must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the finance company's operations or the services provided to its customers (the "identified risks"), in accordance with the finance company's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N09 (Amendment) 2026]

9 A finance company must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N09 (Amendment) 2026]

10 A finance company must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N09 (Amendment) 2026]

11 A finance company must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in customer traffic.

[FSM-N09 (Amendment) 2026]

12 A finance company must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The finance company must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N09 (Amendment) 2026]

13 A finance company must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N09 (Amendment) 2026]

14 A finance company must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the finance company's operations or the services provided to its customers, prior to implementation. The finance company must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the

proposed change, including the impact on upstream and downstream systems. The finance company must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N09 (Amendment) 2026]

15 A finance company must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The finance company must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N09 (Amendment) 2026]

16 A finance company must ensure the availability of data supporting relevant business services. The finance company must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N09 (Amendment) 2026]

17 A finance company must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the finance company's operations or services to its customers;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the finance company's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the finance company's customers need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N09 (Amendment) 2026]

~~7~~18 A finance company must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 A finance company must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the finance company's –

i. compliance with laws and regulations applicable to the finance company;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A finance company must implement effective IT controls to protect customer information from unauthorised access or disclosure.

[FSM-N09 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments**:

1. FSM-N09 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A finance company must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N09 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N11

Notice to merchant banks in Singapore
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all merchant banks in Singapore (each a "Merchant Bank~~s~~").

Definitions

2 For the purpose of this Notice —

"banking business" has the meaning given by section 2(1) of the Banking Act 1970;

"business service" means an external-facing service that is provided to a Merchant Bank's customers;
[FSM-N11 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;
[FSM-N11 (Amendment) 2026]

"critical system", in relation to a Merchant Bank, means a system, the failure of which will cause significant disruption to the operations of the Merchant Bank or materially impact the Merchant Bank's service to its customers, such as a system which —

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;
[FSM-N11 (Amendment) 2026]

"customer", in relation to a Merchant Bank, includes the Monetary Authority of Singapore or any monetary authority or central bank of any other country or territory, and any company which carries on a banking business, a merchant banking business or an investment banking business;

"customer information", in relation to a Merchant Bank, means—

(a) any information relating to, or any particulars of, an account of a customer of the Merchant Bank, whether the account is in respect of a loan, investment or any other type of transaction, but does not include any information that is not referable to any named customer or group of named customers; or

(b) deposit information;

"deposit information", in relation to a Merchant Bank, means any information relating to —

(a) any deposit of a customer of the Merchant Bank;

(b) funds of a customer under management by the Merchant Bank; or

(c) any safe deposit box maintained by, or any safe custody arrangements made by, a customer with the Merchant Bank, but does not include any information that is not referable to any named person or group of named persons;

"funds of a customer under management" means any funds or assets of a customer (whether of the Merchant Bank or any financial institution) placed with that Merchant Bank for the purpose of management or investment;

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N11 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of customer information~~;

[FSM-N11 (Amendment) 2026]

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N11 (Amendment) 2026]

"merchant bank in Singapore" has the meaning given by section 2(1) of the Banking Act 1970;

~~"permitted business" has the meaning given by section 55Q of the Banking Act 1970;~~

[FSM-N11 (Amendment) 2026]

"relevant business service" means a business service of a Merchant Bank which, if disrupted, will have a significant impact on the Merchant Bank's customers or other financial institutions that depend on the business service;

[FSM-N11 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the Merchant Bank's operations, ~~or~~ materially impacts the Merchant Bank's service to its customers, or compromises the confidentiality of customer information;

[FSM-N11 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N11 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a Merchant Bank's IT infrastructure;

[FSM-N11 (Amendment) 2026]

~~"system malfunction" means a failure of any of the Merchant Bank's critical systems.~~

[FSM-N11 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N11 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A Merchant Bank must put in place a framework and process to identify critical systems.

5 A Merchant Bank must make all reasonable effort to maintain high availability for critical systems. The Merchant Bank must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the Merchant Bank's operations or the Merchant Bank's service to its customers. The Merchant Bank must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the Merchant Bank's operations or service to its customers~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N11 (Amendment) 2026]

6 A Merchant Bank must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The Merchant Bank must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N11 (Amendment) 2026]

7 A Merchant Bank must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N11 (Amendment) 2026]

8 A Merchant Bank must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the Merchant Bank's operations or the services provided to its customers. The Merchant Bank must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the Merchant Bank's operations or the services provided to its customers (the "identified risks"), in accordance with the Merchant Bank's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N11 (Amendment) 2026]

9 A Merchant Bank must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N11 (Amendment) 2026]

10 A Merchant Bank must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N11 (Amendment) 2026]

11 A Merchant Bank must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in customer traffic.

[FSM-N11 (Amendment) 2026]

12 A Merchant Bank must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The Merchant Bank must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N11 (Amendment) 2026]

13 A Merchant Bank must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N11 (Amendment) 2026]

14 A Merchant Bank must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the Merchant Bank's operations or the services provided to its customers, prior to implementation. The Merchant Bank must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and downstream systems. The Merchant Bank must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N11 (Amendment) 2026]

15 A Merchant Bank must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The Merchant Bank must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N11 (Amendment) 2026]

16 A Merchant Bank must ensure the availability of data supporting relevant business services. The Merchant Bank must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N11 (Amendment) 2026]

17 A Merchant Bank must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the Merchant Bank's operations or services to its customers;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the Merchant Bank's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the Merchant Bank's customers need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N11 (Amendment) 2026]

~~7~~18 A Merchant Bank must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 A Merchant Bank must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the Merchant Bank's –

i. compliance with laws and regulations applicable to the Merchant Bank;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A Merchant Bank must implement effective IT controls to protect customer information from unauthorised access or disclosure.

[FSM-N11 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments**:

1. FSM-N11 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A Merchant Bank must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N11 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N13

Notice to operators and settlement institutions of designated payment systems and holders of payment services licence (digital payment token service)
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all the following entities regulated under the Payment Services Act 2019:

(a) operators and settlement institutions of designated payment systems;

(b) holders of a payment services licence that carry on a business of providing digital payment token service ("digital payment token service providers"), (each a "relevant entity").

Definitions

2 For the purpose of this Notice —

"business service" means an external-facing service that is provided to a relevant entity's customers;

[FSM-N13 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;

[FSM-N13 (Amendment) 2026]

"critical system", in relation to a relevant entity, means a system, the failure of which will cause significant disruption to the operations of the relevant entity or materially impact the relevant entity's service to its customers, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;

[FSM-N13 (Amendment) 2026]

"designated payment system" has the meaning given by section 2(1) of the Payment Services Act 2019;

"digital payment token service" has the meaning given by section 2(1) of the Payment Services Act 2019;

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N13 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of customer information~~;

[FSM-N13 (Amendment) 2026]

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N13 (Amendment) 2026]

"operator" has the meaning given by section 2(1) of the Payment Services Act 2019;

"payment service" has the meaning given by section 2(1) of the Payment Services Act 2019;

"relevant business service" means a business service of a relevant entity which, if disrupted, will have a significant impact on the relevant entity's customers or other financial institutions that depend on the business service;

[FSM-N13 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the relevant entity's operations, ~~or~~ materially impacts the relevant entity's service to its customers, or compromises the confidentiality of customer information;

[FSM-N13 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N13 (Amendment) 2026]

"settlement institution" has the meaning given by section 2(1) of the Payment Services Act 2019;

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a relevant entity's IT infrastructure;

[FSM-N13 (Amendment) 2026]

~~"system malfunction" means a failure of any of the relevant entity's critical systems.~~

[FSM-N13 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N13 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A relevant entity must put in place a framework and process to identify critical systems.

5 A relevant entity must make all reasonable effort to maintain high availability for critical systems. The relevant entity must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the relevant entity's operations or the relevant entity's service to its customers. The relevant entity must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the relevant entity's operations or service to its customers~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N13 (Amendment) 2026]

6 A relevant entity must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The relevant entity must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N13 (Amendment) 2026]

7 A relevant entity must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N13 (Amendment) 2026]

8 A relevant entity must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the relevant entity's operations or the services provided to its customers. The relevant entity must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the relevant entity's operations or the services provided to its customers (the "identified risks"), in accordance with the relevant entity's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N13 (Amendment) 2026]

9 A relevant entity must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N13 (Amendment) 2026]

10 A relevant entity must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N13 (Amendment) 2026]

11 A relevant entity must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in customer traffic.

[FSM-N13 (Amendment) 2026]

12 A relevant entity must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The relevant entity must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N13 (Amendment) 2026]

13 A relevant entity must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N13 (Amendment) 2026]

14 A relevant entity must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the relevant entity's operations or the services provided to its customers, prior to implementation. The relevant entity must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and downstream systems. The relevant entity must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N13 (Amendment) 2026]

15 A relevant entity must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The relevant entity must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N13 (Amendment) 2026]

16 A relevant entity must ensure the availability of data supporting relevant business services. The relevant entity must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N13 (Amendment) 2026]

17 A relevant entity must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the relevant entity's operations or services to its customers;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the relevant entity's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the relevant entity's customers need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N13 (Amendment) 2026]

~~7~~18 A relevant entity must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 A relevant entity must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the relevant entity's –

i. compliance with laws and regulations applicable to the relevant entity;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A relevant entity must implement effective IT controls to protect customer information from unauthorised access or disclosure.

[FSM-N13 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on the following dates:

(a) where a relevant entity is an operator or settlement institution of a designated payment system, on 10 May 2024; and

(b) where a relevant entity is a digital payment token service provider, on 06 November 2024.

***Notes on History of Amendments**:

1. FSM-N13 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A relevant entity must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N13 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N17

Notice to licensed credit bureaus
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all licensed credit bureaus.

Definitions

2 For the purpose of this Notice —

"business service" means an external-facing service that is provided to a licensed credit bureau's relevant persons;

[FSM-N17 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;

[FSM-N17 (Amendment) 2026]

"credit facility" has the meaning given by section 2 of the Credit Bureau Act 2016;

"critical system", in relation to a licensed credit bureau, means a system, the failure of which will cause significant disruption to the operations of the licensed credit bureau or materially impact the licensed credit bureau's service to a relevant person, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to relevant persons;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;

[FSM-N17 (Amendment) 2026]

"customer" has the meaning given by section 2 of the Credit Bureau Act 2016;

"data subject" has the meaning given by section 2 of the Credit Bureau Act 2016;

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N17 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of relevant person information~~;

[FSM-N17 (Amendment) 2026]

"licensed credit bureau" has the meaning given by section 2 of the Credit Bureau Act 2016;

"member" has the meaning given by section 2 of the Credit Bureau Act 2016;

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N17 (Amendment) 2026]

"relevant business service" means a business service of a licensed credit bureau which, if disrupted, will have a significant impact on the licensed credit bureau's relevant persons or other financial institutions that depend on the business service;

[FSM-N17 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the licensed credit bureau's operations, ~~or~~ materially impacts the licensed credit bureau's service to its relevant persons, or compromises the confidentiality of relevant person information;

[FSM-N17 (Amendment) 2026]

"relevant person" means a customer, data subject, or member;

"relevant person information" means any information relating to, or any particulars of, any relevant person, where a named relevant person or group of named relevant persons can be identified, or is capable of being identified, from such information;

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N17 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a licensed credit bureau's IT infrastructure; ~~and~~

[FSM-N17 (Amendment) 2026]

~~"system malfunction" means a failure of any of the licensed credit bureau's critical systems.~~

[FSM-N17 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N17 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A licensed credit bureau must put in place a framework and process to identify critical systems.

5 A licensed credit bureau must make all reasonable effort to maintain high availability for critical systems. The licensed credit bureau must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the licensed credit bureau's operations or the licensed credit bureau's service to its relevant persons. The licensed credit bureau must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the licensed credit bureau's operations or service to its relevant persons~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N17 (Amendment) 2026]

6 A licensed credit bureau must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The licensed credit bureau must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N17 (Amendment) 2026]

7 A licensed credit bureau must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N17 (Amendment) 2026]

8 A licensed credit bureau must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the licensed credit bureau's operations or the services provided to its relevant persons. The licensed credit bureau must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the licensed credit bureau's operations or the services provided to its relevant persons (the "identified risks"), in accordance with the licensed credit bureau's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N17 (Amendment) 2026]

9 A licensed credit bureau must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N17 (Amendment) 2026]

10 A licensed credit bureau must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N17 (Amendment) 2026]

11 A licensed credit bureau must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in relevant persons traffic.

[FSM-N17 (Amendment) 2026]

12 A licensed credit bureau must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The licensed credit bureau must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N17 (Amendment) 2026]

13 A licensed credit bureau must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N17 (Amendment) 2026]

14 A licensed credit bureau must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the licensed credit bureau's operations or the services provided to its relevant persons, prior to implementation. The licensed credit bureau must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and downstream systems. The licensed credit bureau must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N17 (Amendment) 2026]

15 A licensed credit bureau must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The licensed credit bureau must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N17 (Amendment) 2026]

16 A licensed credit bureau must ensure the availability of data supporting relevant business services. The licensed credit bureau must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N17 (Amendment) 2026]

17 A licensed credit bureau must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the licensed credit bureau's operations or services to its relevant persons;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the licensed credit bureau's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the licensed credit bureau's relevant persons need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N17 (Amendment) 2026]

~~7~~18 A licensed credit bureau must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 A licensed credit bureau must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the licensed credit bureau's –

i. compliance with laws and regulations applicable to the licensed credit bureau;

ii. operations; and

iii. service to its relevant persons; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A licensed credit bureau must implement effective IT controls to protect relevant person information from unauthorised access or disclosure.

[FSM-N17 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments**:

1. FSM-N17 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A licensed credit bureau must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N17 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N19

Notice to registered insurance brokers
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all registered insurance brokers.

Definitions

2 For the purpose of this Notice —

"business service" means an external-facing service that is provided to a registered insurance broker's customers;

[FSM-N19 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;

[FSM-N19 (Amendment) 2026]

"critical system", in relation to a registered insurance broker, means a system, the failure of which will cause significant disruption to the operations of the registered insurance broker or materially impact the registered insurance broker's service to its customers, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;

[FSM-N19 (Amendment) 2026]

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N19 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of customer information~~;

[FSM-N19 (Amendment) 2026]

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N19 (Amendment) 2026]

"registered insurance broker" has the meaning given by section 2 of the Insurance Act 1966;

"relevant business service" means a business service of a registered insurance broker which, if disrupted, will have a significant impact on the registered insurance broker's customers or other financial institutions that depend on the business service;

[FSM-N19 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the registered insurance broker's operations, ~~or~~ materially impacts the registered insurance broker's service to its customers, or compromises the confidentiality of customer information;

[FSM-N19 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N19 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a registered insurance broker's IT infrastructure;

[FSM-N19 (Amendment) 2026]

~~"system malfunction" means a failure of any of the registered insurance broker's critical systems.~~

[FSM-N19 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N19 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A registered insurance broker must put in place a framework and process to identify critical systems.

5 A registered insurance broker must make all reasonable effort to maintain high availability for critical systems. The registered insurance broker must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the registered insurance broker's operations or the registered insurance broker's service to its customers. The registered insurance broker must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the registered insurance broker's operations or service to its customers~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N19 (Amendment) 2026]

6 A registered insurance broker must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The registered insurance broker must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N19 (Amendment) 2026]

7 A registered insurance broker must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N19 (Amendment) 2026]

8 A registered insurance broker must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the registered insurance broker's operations or the services provided to its customers. The registered insurance broker must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the registered insurance broker's operations or the services provided to its customers (the "identified risks"), in accordance with the registered insurance broker's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N19 (Amendment) 2026]

9 A registered insurance broker must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N19 (Amendment) 2026]

10 A registered insurance broker must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N19 (Amendment) 2026]

11 A registered insurance broker must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in customer traffic.

[FSM-N19 (Amendment) 2026]

12 A registered insurance broker must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The registered insurance broker must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N19 (Amendment) 2026]

13 A registered insurance broker must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N19 (Amendment) 2026]

14 A registered insurance broker must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the registered insurance broker's operations or the services provided to its customers, prior to implementation. The registered insurance

broker must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and downstream systems. The registered insurance broker must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N19 (Amendment) 2026]

15 A registered insurance broker must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The registered insurance broker must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N19 (Amendment) 2026]

16 A registered insurance broker must ensure the availability of data supporting relevant business services. The registered insurance broker must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N19 (Amendment) 2026]

17 A registered insurance broker must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the registered insurance broker's operations or services to its customers;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the registered insurance broker's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the registered insurance broker's customers need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N19 (Amendment) 2026]

~~7~~18 A registered insurance broker must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 A registered insurance broker must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the registered insurance broker's –

i. compliance with laws and regulations applicable to the registered insurance broker;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A registered insurance broker must implement effective IT controls to protect customer information from unauthorised access or disclosure.

[FSM-N19 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments**:

1. FSM-N19 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A registered insurance broker must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N19 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N21

Notice to capital markets financial institutions
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all the following financial institutions:

(a) approved exchanges under the Securities and Futures Act 2001 ("SFA");

(b) licensed trade repositories under the SFA;

(c) approved clearing houses under the SFA;

(d) recognised clearing houses under the SFA which are incorporated in Singapore;

(e) holders of a capital markets services licence under the SFA;

(f) recognised market operators under the SFA which are incorporated in Singapore;

(g) trustees for a collective investment scheme authorised under section 286 of the SFA, that are approved under the SFA;

(h) authorised benchmark administrators under the SFA;

(i) authorised benchmark submitters under the SFA;

(j) designated benchmark submitters under the SFA;

(k) the Depository as defined in section 81SF of the SFA,
(each a "specified financial institution").

Definitions

2 For the purpose of this Notice —

"business service" means an external-facing service that is provided to a specified financial institution's customers;

[FSM-N21 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;

[FSM-N21 (Amendment) 2026]

"critical system", in relation to a specified financial institution, means a system, the failure of which will cause significant disruption to the operations of the specified financial institution or materially impact the specified financial institution's service to its customers, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"customer" –

(a) in relation to a holder of a capital markets services licence, has the meaning given by paragraph (a)(i) of the definition of "customer" in section 2(1) of the SFA; and

(b) in relation to an approved clearing house or a recognised clearing house, has the meaning given by paragraph (b) of the definition of "customer" in section 2(1) of the SFA;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;

[FSM-N21 (Amendment) 2026]

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N21 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of customer information~~;

[FSM-N21 (Amendment) 2026]

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N21 (Amendment) 2026]

"relevant business service" means a business service of a specified financial institution which, if disrupted, will have a significant impact on the specified financial institution's customers or other financial institutions that depend on the business service;

[FSM-N21 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the specified financial institution's operations, ~~or~~ materially impacts the specified financial institution's service to its customers, or compromises the confidentiality of customer information;

[FSM-N21 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N21 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a specified financial institution's IT infrastructure;

[FSM-N21 (Amendment) 2026]

~~"system malfunction" means a failure of any of the specified financial institution's critical systems.~~

[FSM-N21 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N21 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A specified financial institution must put in place a framework and process to identify critical systems.

5 A specified financial institution must make all reasonable effort to maintain high availability for critical systems. The specified financial institution must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the specified financial institution's operations or the specified financial institution's service to its customers. The specified financial institution must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the specified financial institution's operations or service to its customers~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N21 (Amendment) 2026]

6 A specified financial institution must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The specified financial institution must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated~~

~~during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N21 (Amendment) 2026]

7 A specified financial institution must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N21 (Amendment) 2026]

8 A specified financial institution must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the specified financial institution's operations or the services provided to its customers. The specified financial institution must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the specified financial institution's operations or the services provided to its customers (the "identified risks"), in accordance with the specified financial institution's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N21 (Amendment) 2026]

9 A specified financial institution must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N21 (Amendment) 2026]

10 A specified financial institution must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N21 (Amendment) 2026]

11 A specified financial institution must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in customer traffic.

[FSM-N21 (Amendment) 2026]

12 A specified financial institution must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The specified financial institution must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N21 (Amendment) 2026]

13 A specified financial institution must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N21 (Amendment) 2026]

14 A specified financial institution must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the specified financial institution's operations or the services provided to its customers, prior to implementation. The specified financial institution must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and downstream systems. The specified financial institution must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N21 (Amendment) 2026]

15 A specified financial institution must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The specified financial institution must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N21 (Amendment) 2026]

16 A specified financial institution must ensure the availability of data supporting relevant business services. The specified financial institution must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N21 (Amendment) 2026]

17 A specified financial institution must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the specified financial institution's operations or services to its customers;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the specified financial institution's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the specified financial institution's customers need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N21 (Amendment) 2026]

~~7~~18 A specified financial institution must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident, other than a relevant incident arising from the circumstances set out in regulations 8(2)(a) and (b), and 21(d) of the Securities and Futures (Organised Markets) Regulations 2018 ("Markets Regulations"), regulation 9(1) of the Securities and Futures (Trade Repositories) Regulations 2013, regulation 11(1) of the Securities and Futures (Clearing Facilities) Regulations 2013, and regulations 11(1)(e) and 19(2)(b) of the Securities and Futures (Financial Benchmarks)Regulations 2018 ("Financial Benchmarks Regulations").

~~8~~19 A specified financial institution must, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident as described in paragraph ~~7~~ 18 or a relevant incident arising from the circumstances set out in regulation 21(d) of the Markets Regulations, as the case may be, submit a root cause and impact analysis report to the Authority. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the specified financial institution's –

i. compliance with laws and regulations applicable to the specified financial institution;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A specified financial institution must implement effective IT controls to protect customer information from unauthorised access or disclosure.

[FSM-N21 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments**:

1. FSM-N21 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A specified financial institution must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N21 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N23

Notice to licensed financial advisers
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all financial advisers licensed under the Financial Advisers Act 2001 ("licensee").

Definitions

2 For the purpose of this Notice —

"business service" means an external-facing service that is provided to a licensee's customers;

[FSM-N23 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;

[FSM-N23 (Amendment) 2026]

"critical system", in relation to a licensee, means a system, the failure of which will cause significant disruption to the operations of the licensee or materially impact the licensee's service to its customers, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to customers;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;

[FSM-N23 (Amendment) 2026]

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N23 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of customer information~~;

[FSM-N23 (Amendment) 2026]

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N23 (Amendment) 2026]

"relevant business service" means a business service of a licensee which, if disrupted, will have a significant impact on the licensee's customers or other financial institutions that depend on the business service;

[FSM-N23 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the licensee's operations, ~~or~~ materially impacts the licensee's service to its customers, or compromises the confidentiality of customer information;

[FSM-N23 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N23 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a licensee's IT infrastructure;

[FSM-N23 (Amendment) 2026]

~~"system malfunction" means a failure of any of the licensee's critical systems.~~

[FSM-N23 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N23 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A licensee must put in place a framework and process to identify critical systems.

5 A licensee must make all reasonable effort to maintain high availability for critical systems. The licensee must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the licensee's operations or the licensee's service to its customers. The licensee must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the licensee's operations or service to its customers~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N23 (Amendment) 2026]

6 A licensee must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The licensee must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N23 (Amendment) 2026]

7 A licensee must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N23 (Amendment) 2026]

8 A licensee must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the licensee's operations or the services provided to its customers. The licensee must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the licensee's operations or the services provided to its customers (the "identified risks"), in accordance with the licensee's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N23 (Amendment) 2026]

9 A licensee must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N23 (Amendment) 2026]

10 A licensee must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N23 (Amendment) 2026]

11 A licensee must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in customer traffic.

[FSM-N23 (Amendment) 2026]

12 A licensee must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The licensee must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N23 (Amendment) 2026]

13 A licensee must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N23 (Amendment) 2026]

14 A licensee must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the licensee's operations or the services provided to its customers, prior to implementation. The licensee must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and downstream systems. The licensee must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N23 (Amendment) 2026]

15 A licensee must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The licensee must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N23 (Amendment) 2026]

16 A licensee must ensure the availability of data supporting relevant business services. The licensee must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N23 (Amendment) 2026]

17 A licensee must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the licensee's operations or services to its customers;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the licensee's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the licensee's customers need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N23 (Amendment) 2026]

~~7~~18 A licensee must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 A licensee must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the licensee's –

i. compliance with laws and regulations applicable to the licensee;

ii. operations; and

iii. service to its customers; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A licensee must implement effective IT controls to protect customer information from unauthorised access or disclosure.

[FSM-N23 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments**:

1. FSM-N23 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A licensee must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N23 (Amendment) 2026]

Draft of Amended Notice on Technology Risk Management

MAS Notice No.: FSM-N25

Notice to licensed trust companies
Financial Services and Markets Act 2022

Issue Date: 09 May 2024 [Last revised on xx 2026]

NOTICE ON TECHNOLOGY RISK MANAGEMENT

Introduction

1 This Notice is issued pursuant to section 29(1) of the Financial Services and Markets Act 2022 (the "Act") and applies to all licensed trust companies under the Trust Companies Act 2005 ("trust companies").

Definitions

2 For the purpose of this Notice —

"business service" means an external-facing service that is provided to a trust company's protected parties;

[FSM-N25 (Amendment) 2026]

"capacity", in relation to a system, means the ability of the system to handle workloads, including processing, storage and transmission, without performance degradation;

[FSM-N25 (Amendment) 2026]

"critical system", in relation to a trust company, means a system, the failure of which will cause significant disruption to the operations of the trust company or materially impact the trust company's service to its protected parties, such as a system which—

(a) processes transactions that are time critical; or

(b) provides essential services to protected parties;

"cryptographic asset" means any cryptographic component used to secure data, communications or transactions, including cryptographic keys, digital certificates, hardware security modules, encryption software, cryptographic algorithms and key management systems;

[FSM-N25 (Amendment) 2026]

"~~system~~ IT asset" means any hardware, software, network, or other information technology ("IT") component ~~which is part of an IT infrastructure~~;

[FSM-N25 (Amendment) 2026]

"IT security incident" means an event that involves a security breach, such as hacking of, intrusion into, or denial of service attack on a ~~critical~~ system~~, or a system which compromises the security, integrity or confidentiality of any protected party information~~;

[FSM-N25 (Amendment) 2026]

"open-source component" means any software library, module, framework or tool whose source code is publicly available under open-source licences;

[FSM-N25 (Amendment) 2026]

"protected party" has the meaning given by section 2 of the Trust Companies Act 2005;

"relevant business service" means a business service of a trust company which, if disrupted, will have a significant impact on the trust company's protected parties or other financial institutions that depend on the business service;

[FSM-N25 (Amendment) 2026]

"relevant incident" means a ~~system malfunction~~ failure of any system or IT security incident, which has a severe and widespread impact on the trust company's operations, ~~or~~ materially impacts the trust company's service to its protected parties, or compromises the confidentiality of protected party information;

[FSM-N25 (Amendment) 2026]

"recovery time objective" or "RTO" means the duration of time, from the point of disruption, within which a system must be restored;

[FSM-N25 (Amendment) 2026]

"system" means ~~any hardware, software, network, or other information technology ("IT") component which is part of an IT infrastructure~~ an IT asset, or a set of interconnected IT assets, performing one or more functions within a trust company's IT infrastructure;

[FSM-N25 (Amendment) 2026]

~~"system malfunction" means a failure of any of the trust company's critical systems.~~

[FSM-N25 (Amendment) 2026]

"third-party component" means any proprietary software, hardware or services from third-party vendors.

[FSM-N25 (Amendment) 2026]

3 Except where defined in this Notice or if the context otherwise requires, the expressions used in this Notice have the same meanings as in the Act.

Technology Risk Management

4 A trust company must put in place a framework and process to identify critical systems.

5 A trust company must make all reasonable effort to maintain high availability for critical systems. The trust company must record the unscheduled downtime for each critical system, including periods of partial or intermittent disruption that affect the trust company's operations or the trust company's service to its protected parties. The trust company must ensure that the ~~maximum~~ total unscheduled downtime for each critical system ~~that affects the trust company's operations or service to its protected parties~~ does not exceed ~~a total of~~ 4 hours within any period of 12 months.

[FSM-N25 (Amendment) 2026]

6 A trust company must establish a recovery time objective ("RTO") of not more than 4 hours for each critical system. ~~The RTO is the duration of time, from the point of disruption, within which a system must be restored.~~ The trust company must ~~validate and document at least once every 12 months, how it performs its system recovery testing and when the RTO is validated during the system recovery testing~~ perform system recovery testing for each critical system at least once every 12 months to validate its ability to meet the RTO and document the test plan, how the testing was performed, and test results.

[FSM-N25 (Amendment) 2026]

7 A trust company must maintain a comprehensive and up-to-date inventory of all IT assets, including cryptographic assets, open-source components, and third-party components, in accordance with the requirements set out in Appendix A.

[FSM-N25 (Amendment) 2026]

8 A trust company must establish and maintain a framework and process to conduct regular IT risk assessments in respect of every system, the disruption of which may affect the trust company's operations or the services provided to its protected parties. The trust company must, in respect of each IT risk assessment it conducts:

(a) identify the threats to and vulnerabilities within the system;

(b) assess the risks that could arise from these threats and vulnerabilities, including the potential impact and likelihood of such risks affecting the trust company's operations or the services provided to its protected parties (the "identified risks"), in accordance with the trust company's established risk assessment criteria; and

(c) implement risk mitigation measures that are commensurate with the identified risks.

[FSM-N25 (Amendment) 2026]

9 A trust company must establish and maintain a register that records:

(a) the identified risks referred to in paragraph 8(b) that are material ("material identified risks");

(b) the risk owners who will be accountable for managing the material identified risks effectively; and

(c) the measures to mitigate the material identified risks.

[FSM-N25 (Amendment) 2026]

10 A trust company must establish and maintain key risk indicators (KRIs) to effectively monitor the material identified risks referred to in paragraph 9(a) and assess the effectiveness of the measures referred to in paragraph 9(c).

[FSM-N25 (Amendment) 2026]

11 A trust company must establish and maintain a framework and process to ensure that the capacity of its critical systems, and the systems on which those critical systems depend on, is sufficient to meet business needs, taking into account projected business growth and potential surges in protected party traffic.

[FSM-N25 (Amendment) 2026]

12 A trust company must establish and maintain a framework and process to continuously monitor all critical systems to detect and respond to issues affecting their performance or security in a timely manner. The trust company must ensure that the framework and process include, at a minimum:

(a) defined indicators and thresholds that trigger alerts; and

(b) response procedures and remedial actions that are commensurate with the nature and potential impact of the identified issues.

[FSM-N25 (Amendment) 2026]

13 A trust company must implement effective controls to prevent unauthorised changes from being made to any system.

[FSM-N25 (Amendment) 2026]

14 A trust company must establish and maintain a framework and process to assess the risks arising from any proposed change to a system which may affect the trust company's operations or the services provided to its protected parties, prior to implementation. The trust company must, in its assessment, evaluate the potential impact arising from the failure or incorrect implementation of the proposed change, including the impact on upstream and downstream systems. The trust company must implement risk mitigation measures that are commensurate with the risks identified.

[FSM-N25 (Amendment) 2026]

15 A trust company must carry out testing for all changes to critical systems and ensure that the scope and rigour of testing are commensurate with the risks posed by the changes. The trust company must have in place effective measures to recover the critical system if a problem arises during or after change implementation.

[FSM-N25 (Amendment) 2026]

16 A trust company must ensure the availability of data supporting relevant business services. The trust company must maintain an immutable or offline backup of such data for data recovery in the event the data is corrupted, tampered with, or made inaccessible, so as to enable timely and reliable resumption of its services.

[FSM-N25 (Amendment) 2026]

17 A trust company must establish and maintain an incident management framework and process which include, at a minimum:

(a) the roles, responsibilities and persons primarily responsible for responding to an IT incident in respect of any system which has any impact on the trust company's operations or services to its protected parties;

(b) procedures to collect and preserve evidence for investigation purposes;

(c) procedures to notify the trust company's senior management upon identification of the IT incident to enable informed decision-making; and

(d) procedures to assess whether stakeholders and the trust company's protected parties need to be notified of the IT incident and where notification is necessary, ensure they are promptly notified of the details relating to the nature, impact and expected resolution of the IT incident.

[FSM-N25 (Amendment) 2026]

~~7~~18 A trust company must notify the Authority as soon as possible, but not later than 1 hour, upon the discovery of a relevant incident.

~~8~~19 A trust company must submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow, from the discovery of the relevant incident. The report must contain —

(a) an executive summary of the relevant incident;

(b) an analysis of the root cause which triggered the relevant incident;

(c) a description of the impact of the relevant incident on the trust company's –

i. compliance with laws and regulations applicable to the trust company;

ii. operations; and

iii. service to its protected parties; and

(d) a description of the remedial measures taken to address the root cause and consequences of the relevant incident.

~~9~~20 A trust company must implement effective IT controls to protect protected party information from unauthorised access or disclosure.

[FSM-N25 (Amendment) 2026]

Effective Date

~~10~~21 This Notice shall take effect on 10 May 2024.

***Notes on History of Amendments**:

1. FSM-N25 (Amendment) 2026 with effect from xx 2026

Appendix A

1. Minimum information for each IT asset

Field	Descriptor
Name	Unique tag or identifier for the IT asset following organisational naming convention
Type	Type of IT asset, e.g. hardware, software, network, or other IT component;
Model and version information	Specific details of the IT asset, e.g. hardware model number, software version number, and current patch level
Supported system(s)	Systems supported by this IT asset
Criticality of supported system(s)	Criticality classification of systems supported by this IT asset based on the impact of their unavailability (e.g. critical system)
Owner	Person or department responsible for the IT asset, e.g. individual staff member, business unit, or organisational division
Parties responsible for maintenance, including external parties	Groups responsible for IT asset upkeep, e.g. internal IT teams, business units, external vendors, or third-party service providers

2. Additional information for certain types of IT assets

A trust company must, in addition to the minimum information required in paragraph 1, include the following information in its inventory:

Asset type	Details
Cryptographic asset	Cryptographic algorithm and key length used
Open-source component	Supplier name, version, the IT assets or components that rely on the software, and all direct and indirect dependencies, together with their relationships
Third-party component	Vendor name, version, the IT assets or components that rely on the software or hardware, and all direct and indirect dependencies, together with their relationships

[FSM-N25 (Amendment) 2026]

3. List of Questions