BANK OF JAMAICA

2026

CONSULTATION PAPER ON THE STANDARDS OF SOUND PRACTICE

ON

OUTSOURCING ARRANGEMENTS AND THIRD-PARTY RISKS MANAGEMENT

(For licensees under the Banking Services Act)

Standards of Sound Practices are guiding principles issued by the Bank of Jamaica which set out minimum expectations of the Supervisory Authority in relation to its licensees; and against which licensees can evaluate their performance.

THIS PAGE INTENTIONALLY

LEFT BLANK

Consultation Paper on the Standard of Sound Practice on

Outsourcing Arrangements and Third-Party Risk Management

(for Licensees under the Banking Services Act)

The proposed Standard on Outsourcing Arrangements and Third-Party Risk Management is available on Bank of Jamaica's website at www.boj.org.jm.

Bank of Jamaica, Nethersole Place,

Kingston, Jamaica

(Telephone 876-922-0750 - 9; Fax 876-922-2519 or email FISDMailbox@boj.org.jm)

Table of Contents

SECTION 1: BACKGROUND

(A) Introduction

1.1 Bank of Jamaica ("The Bank") is strengthening its regulatory and supervisory framework through the issuance of this Outsourcing Arrangements and Third-Party Risk Management Standard ("the Standard"), which establishes minimum requirements and supervisory expectations for managing risks associated with outsourcing arrangements. The Standard is issued pursuant to the powers conferred on the Financial Policy Committee under the Bank of Jamaica Act.

1.2 This Standard reflects the growing reliance of licensees on outsourcing and other third-party arrangements to support the delivery of financial services, critical business functions, and technology-enabled transformation. While these arrangements may provide operational, strategic, and economic benefits, they can also create significant dependencies and introduce risks that may not be fully within the direct control of the licensee. These risks include, but are not limited to, operational, cyber, legal, compliance, concentration, and reputational risks. If not effectively governed and managed, such risks may impair the operational resilience, safety, and soundness of licensees and, in certain circumstances, contribute to broader financial stability concerns.

1.3 The objectives of this Standard are to:

a. establish minimum supervisory expectations for the governance, identification, assessment, monitoring, management, and control of risks arising from outsourcing and other third-party arrangements;
b. ensure that licensees maintain effective oversight of outsourcing and third-party arrangements and remain fully accountable for all activities, services, and functions performed on their behalf;
c. promote the operational resilience of licensees by safeguarding the continuity of important business services and ensuring that outsourcing and third-party arrangements do not undermine the ability of licensees to operate within established impact tolerances;
d. ensure that risks arising from outsourcing and third-party arrangements, including operational, cyber, legal, compliance, concentration, and reputational risks, are identified, assessed, managed, monitored, and controlled in a prudent manner;
e. support the protection of customer information, confidential data, and other sensitive information entrusted to licensees;
f. reduce the risk of excessive dependence on individual service providers, common service providers, or other third-party dependencies that may adversely affect the safety and soundness of licensees or contribute to systemic risk; and
g. ensure that outsourcing and third-party arrangements do not impair the ability of the Supervisor to exercise effective supervision, crisis

management, recovery planning, resolution planning, or other statutory functions.

1.4 This Standard recognises that technological innovation and digital transformation have increased the use of outsourcing and other third-party arrangements by licensees. Developments in cloud computing, artificial intelligence, machine learning, distributed ledger technology, and other emerging technologies may provide significant operational and strategic benefits but may also create heightened dependencies and introduce new and evolving risks. Licensees must therefore ensure that appropriate governance, risk management, operational resilience, and control frameworks are established and maintained to identify, assess, manage, monitor, and control risks arising from such arrangements.[1]

1.5 Accordingly, outsourcing arrangements must:

a. not impair the licensee's ability to comply with applicable laws, regulations, and supervisory requirements;
b. provide for the timely and effective access by the licensee and the Supervisor to information, records, systems, and other resources necessary to support oversight, supervision, and the discharge of statutory responsibilities; and
c. be governed by legally binding and enforceable arrangements that clearly allocate responsibilities and support the safe, sound, and resilient delivery of the outsourced or third-party service.

1.6 Supervisory expectations under this Standard extend to sub-outsourcing arrangements and other supply chain dependencies. Licensees must maintain appropriate oversight of outsourcing and third-party arrangements throughout the service delivery chain and ensure that risks arising from subcontractors, fourth parties, and other service dependencies are appropriately identified, assessed, managed, monitored, and controlled.

1.7 The Supervisor will apply a risk-based and proportionate approach to the supervision of outsourcing and third-party arrangements. In determining the nature, scope, and intensity of its supervisory oversight, the Supervisor will consider, among other factors, the materiality and criticality of the arrangement, the risk profile, size, nature, and complexity of the licensee, and any concentration, sectoral, or systemic risks arising from common outsourcing or third-party dependencies.

[1] For example, in the EU, the European banking Authority (EBA) issued guidelines on outsourcing arrangements and on ICT and security risk management that are designed to promote a harmonised, level-playing field in the EU banking sector. For details, see EBA (2019a) Guidelines on outsourcing arrangements, February and EBA (2019b) Guidelines on ICT and security risk management, November. At the international level, the International Organization of Securities Commissions (IOSCO), for example, issued its proposed updates to its Principles on Outsourcing for public consultation in May 2020 that comprise a set of fundamental precepts and a set of seven principles for regulated entities that outsource tasks to service providers.

(B) Legal Requirement

This section sets out the statutory provisions underpinning the requirements and expectations contained in this Standard of Sound Practice on Outsourcing Arrangements and Third-Party Risk Management ("SSP OTPRM").

Publication of Standards of Sound Practices and Making of Supervisory Rules

1.8 Under section 34FL(b)(ii) of the Bank of Jamaica (Amendment) Act, 2020, the Financial Policy Committee is empowered to determine Standards of Sound Practice for persons and bodies licensed under the Banking Services Act, 2014 ("BSA"). Further, section 132(1)(m) of the BSA requires the establishment of Supervisory Rules governing the outsourcing of key aspects of a licensee's operations.

Consistent with these statutory provisions, this SSP OTPRM sets out the Supervisor's expectations for the governance, oversight, and management of risks arising from outsourcing and other third-party arrangements, including those involving critical services, technology providers, and other external dependencies.

Non-compliance with the SSP OTPRM

1.9 Pursuant to paragraph 2(b)(iii) of Part A of the Fifth Schedule of the BSA, the Supervisor may take remedial action pursuant to section 109 of the BSA where a licensee contravenes a Standard of Sound Practice.

Notification to the Supervisor

1.10 In accordance with section 39(1)(a) of the BSA, licensees must immediately notify the Supervisor, in writing, of any matter that could materially affect the financial viability or reputation of the licensee or its financial group. Under section 55(1)(a), prior notification is required before engaging in, inter alia:

i. New businesses or products;
ii. New delivery channels for existing businesses or products;
iii. Strategic alliances;
iv. Joint ventures;
v. Co-branding initiatives; and
vi. Any other matter for which the Supervisor requires prior notification.

Supervisory Approvals

1.11 Pursuant to section 39(5), a licensee must obtain the written approval of the Supervisor before implementing any major change to its operations, strategy, or policy; this includes the establishment of material outsourcing and/or third-party arrangements.

Confidentiality Requirements

1.12 Under section 134 of the BSA, officers, agents, and any person with access to customer information are prohibited from disclosing such information, except as permitted by law. Licensees must ensure that service providers engaged under outsourcing or other third-party arrangements are contractually bound to comply with these confidentiality obligations.

Access, Inspection, and Audit Rights

1.13 Under section 67(1)(a)(ii) of the BSA, an authorised officer of the Bank is entitled, at reasonable times, to access, inspect, and examine any relevant documents, physical or electronic, relating to the operations of the licensee or any entity in its financial group. In addition, section 93(1) empowers the Supervisor to require an external auditor to expand the scope of an audit or perform specified audit procedures and report the findings in writing.

Other Applicable Statutory Obligations

1.14 The Data Protection Act, 2020.

(C) Purpose, Application, and Scope

1.15 This SSP OTPRM establishes the Supervisor's minimum expectations for the governance, oversight, and management of risks arising from outsourcing and other third-party arrangements entered into by licensees.

1.16 This Standard applies to all deposit-taking institutions and their financial holding companies licensed under the BSA. This includes outsourcing and third-party arrangements entered into by parent entities, subsidiaries, affiliates, or other group entities where such arrangements may affect the operations, risk profile, financial condition, operational resilience, or regulatory compliance of a licensee.

1.17 This Standard applies irrespective of whether the service provider is an external third party, an affiliated entity, a parent undertaking, a subsidiary, or another entity within the same corporate group. The application of this Standard must be proportionate to:

a. the size, nature, scale, and complexity of the licensee;
b. the materiality and criticality of the outsourced activity or third-party arrangement; and
c. the nature and severity of the risks arising from the arrangement.

1.18 While the intensity of oversight and controls may vary according to materiality and risk, licensees remain responsible for identifying, assessing, managing, monitoring, and controlling risks arising from all outsourcing and third-party

arrangements, including those assessed as non-material. This Standard applies to:

a. all outsourcing arrangements;
b. intragroup outsourcing arrangements;
c. cloud outsourcing arrangements;
d. cross-border outsourcing arrangements; and
e. other third-party arrangements where the nature of the relationship gives rise to risks comparable to those associated with outsourcing.

1.19 This Standard reflects evolving international supervisory expectations and industry practices relating to outsourcing, third-party risk management, operational resilience, and technology-enabled service delivery. This Standard complements other prudential, operational risk, operational resilience, cybersecurity, and governance requirements issued by the Financial Policy Committee of the Bank of Jamaica.

1.20 In developing this Standard, the Supervisor has taken into consideration relevant principles, standards, and guidance issued by international standard-setting bodies and supervisory authorities, including:

a. The Financial Stability Board (FSB);
b. The G7 Fundamental Elements for Third-Party Cyber Risk Management;
c. The International Organisation of Securities Commissions (IOSCO);
d. The Basel Committee on Banking Supervision; and
e. Other regional and international outsourcing and third-party risk management frameworks.

(D) Implementation and Transition Arrangements

1.21 These Standards take effect from the date of issuance. However, the Supervisor recognises that licensees may require a transition period, particularly where existing outsourcing contracts may not be readily amendable. Accordingly, licensees with existing outsourcing arrangements are required to:

a. Review all existing material and non-material outsourcing contracts to assess alignment with these Standards; and
b. Submit to the Supervisor, within six (6) months of the date of issuance of these Standards, a complete list of all such contracts using the template provided in the Appendix.

1.22 Licensees are expected to take appropriate action to ensure that, at a minimum, material outsourcing contracts conform to the requirements of these Standards as early as practicable. Where immediate compliance is not feasible, appropriate mitigating measures must be implemented to manage any identified risks.

1.23 In this regard, material outsourcing contracts:

a. That are due to expire within twenty-four (24) months of the date of issuance of these Standards may remain in force without amendment;

b. That are due to expire twenty-four (24) months or more after the date of issuance of these Standards should be reviewed to determine the feasibility of amending the terms to facilitate compliance with these Standards.

1.24 All new outsourcing contracts or arrangements entered into after the date of issuance must fully comply with the requirements set out in these Standards.

1.25 Where a licensee inherits outsourcing arrangements as a result of a merger, acquisition, or other corporate restructuring activity, the licensee must ensure that such arrangements are brought into compliance with these Standards at the earliest opportunity. This should occur no later than 12 months or such earlier period in which the contract, agreement, or applicable statement of work is materially amended, renewed, or extended.

1.26 Where a licensee determines that it is not feasible to revise a material contract as required under paragraph 1.23(b), the Supervisor must be notified accordingly. The licensee must also justify the inability to revise the contract and submit a plan outlining how it intends to manage and mitigate the associated risks.

(E) Consultation Notice, Process and Copyright

1.27 Pursuant to section 132(2) of the Banking Services Act (BSA), this document is being circulated to licensees under the BSA and other relevant stakeholders for public consultation. The Supervisor invites comments on the proposals contained in this SSP OTPRM.

1.28 Stakeholders are particularly encouraged to provide feedback on the consultation questions embedded in the Appendices section, which highlight key matters for consideration under the proposed framework. To enhance the usefulness of the feedback, respondents are encouraged to:

i. Indicate the specific clause or section to which each comment relates;
ii. Provide a clear rationale or identify any area of concern;
iii. Support comments with relevant data or examples, where possible; and
iv. Offer alternative regulatory or supervisory approaches that the Supervisor and the Financial Policy Committee should consider.

1.29 Comments should be submitted by email to FISDMailbox@boj.org.jm no later than the close of business on 30 October 2026.

Transition and Implementation Planning

1.30 Licensees will be afforded a transitional period, to be specified in the final document, to ensure adequate time for implementation following the conclusion of this consultative process.

1.31 Licensees should therfore begin preparing implementation plans to facilitate the timely adoption of the finalised SSP OTPRM. These plans should:

i. identify contracts and processes that may be impacted;
ii. outline any amendments or system/process changes required; and
iii. consider resource and training needs for implementation.

The Supervisor may require submission of these plans or updates thereto as part of its supervisory engagement.

SECTION 2: OUTSOURCING AND THIRD-PARTY ARRANGEMENTS

(A) Outsourcing and Third-party Arrangements

Third-party Arrangements

2.1. A third-party arrangement refers to any relationship between a licensee and a person, body, or institution that provides products, services, processes, activities, or business functions to the licensee under a contractual or other formal arrangement. Such arrangements may involve both affiliated and non-affiliated entities and may include service providers located within or outside Jamaica.

2.2. Third-party arrangements may give rise to fourth-party dependencies, where the service provider relies on subcontractors, infrastructure providers, or technology providers to deliver the contracted service. Licensees should have adequate oversight mechanisms to identify and manage risks arising from such dependencies.

Scope of Third-Party Arrangements

2.3. This SSP OTPRM applies to all products, services, processes, activities, or business functions performed by third parties on behalf of a licensee, encompassing both outsourcing and non-outsourcing arrangements.

2.4. A licensee remains fully responsible and accountable for ensuring that all activities conducted by third parties are performed in compliance with applicable laws, regulations, and supervisory expectations, as if such activities were undertaken directly by the licensee.

2.5. The engagement of third-party service providers does not diminish the responsibilities of the licensee's board of directors and senior management, who remain ultimately accountable for ensuring effective oversight, risk management, and compliance with all regulatory obligations.

Outsourcing arrangements

2.6. Outsourcing refers to any arrangement between a licensee and a third party, whether supervised or unsupervised, whereby that third party performs a product, service, process, activity, or business function which:

a. is currently performed by the licensee; or
b. could reasonably be expected to be performed by the licensee in the normal course of its operations.

2.7. Where a licensee enters into an outsourcing arrangement, the licensee must ensure that the outsourced activity is conducted in compliance with all applicable legal, regulatory, and supervisory requirements, to the same extent as if the activity were performed internally. The licensee remains fully responsible and accountable for the outsourced activity.

2.8. Outsourcing arrangements include, but are not limited to, arrangements commonly referred to as onshoring (services performed within Jamaica), offshoring (services performed outside Jamaica), near-shoring (services performed in geographically proximate jurisdictions), or right-shoring (the strategic allocation of services across locations based on cost, efficiency, or risk considerations), and may involve services performed directly by the third party or through subcontracting or other fourth-party arrangements.

2.9. Outsourcing does not include arrangements that are ancillary in nature or that do not involve the performance of a business function on behalf of the licensee. This includes, for example, the procurement of standardised goods, utilities, or public telecommunications services, where the licensee is a user of a service rather than delegating the performance of an activity.

Material Outsourcing Arrangements

2.10. (1) A material outsourcing arrangement is an outsourcing arrangement where a defect, failure, disruption, or inadequate performance in the provision of the outsourced activity, whether on a standalone basis or in combination with other activities or functions, could have a significant adverse impact on the licensee. Materiality is determined by the impact of a failure, and not by the nature or designation of the activity.

(2) Licensees must assess and classify the materiality of every outsourcing and third-party arrangement in accordance with the methodology, criteria, and procedures set out in Section 4 (Assessment of Materiality and Criticality). Arrangements classified as material are subject to the enhanced governance, due diligence, contractual, and control requirements set out in Section 3 (Governance and Responsibility for Outsourcing) and Section 5 (Outsourcing Standards); arrangements classified as non-material remain subject to proportionate measures under this SSP OTPRM.

Scope of Outsourcing Activities

2.11. (1) For the purposes of these Standards, outsourcing must be interpreted broadly and functionally and is not limited to activities previously performed by a licensee on an in-house basis. An activity constitutes outsourcing where a licensee relies on a third party to perform a function, service, process, or activity on its behalf, irrespective of whether the licensee has historically undertaken such activity internally.

(2) An arrangement constitutes outsourcing notwithstanding that:

a. the activity has not previously been performed by the licensee, provided that such activity would reasonably fall within the scope of functions that could be undertaken by the licensee in the ordinary course of its business;
b. the licensee does not possess the capacity, expertise, systems, or resources to perform the activity internally; or
c. the activity is undertaken in connection with the introduction of new products, services, delivery channels, or in response to evolving legal, regulatory, or supervisory requirements.

(3) In determining whether an arrangement constitutes outsourcing, licensees must have regard to the substance of the arrangement, including the extent to which the activity forms part of the licensee's business operations, control environment, or regulatory obligations, and not merely its form, historical treatment, or novelty.

(4) For the avoidance of doubt, an activity constitutes outsourcing where it forms an integral part of the licensee's operations, risk management, or compliance framework and is performed by a third party on behalf of the licensee, notwithstanding that such activity may be characterised as technical, specialised, or ancillary in nature.

(5) Licensees must ensure that all outsourcing arrangements falling within the scope of this section are subject to the requirements of these Standards, including due diligence, risk assessment, contractual safeguards, ongoing monitoring, and governance oversight, commensurate with the materiality and risk profile of the arrangement.

(6) Notwithstanding the generality of this section, outsourced activities and functions may include, but are not limited to:

a. information technology operations and development (including cloud computing services, data hosting, and software-as-a-service solutions);
b. payment processing and transaction settlement;
c. customer service functions (including onshore or offshore call centre operations);
d. records and document management;

e. compliance monitoring and reporting;
f. back-office operations, data processing, and administrative support.
g. professional and advisory services integral to the licensee's regulated activities.
h. facilities management and security services that could impact the continuity or integrity of operations.
i. any other activities integral to the provision of regulated financial services (*see the appendix for additional scope*).

Non-outsourcing third-party arrangements

2.12. (1) Licensees must recognise that third-party arrangements extend beyond outsourcing relationships and that certain third-party arrangements may not meet the definition of outsourcing but may nonetheless expose the licensee to material risk. Accordingly, the scope of third-party risk management must not be limited to outsourcing arrangements.

(2) For the purposes of these Standards, a non-outsourcing third-party arrangement refers to any arrangement with a third party that does not involve the delegation of a function, service, process, or activity on behalf of the licensee, but which may expose the licensee to operational, legal, regulatory, cyber, data, reputational, or other risks.

(3) Licensees must ensure that all third-party arrangements, whether or not they constitute outsourcing arrangements, are subject to a documented, comprehensive, and risk-based framework for:
a. identification of all third-party relationships;
b. assessment of the risks arising from such relationships;
c. appropriate due diligence before engagement; and
d. ongoing monitoring and review of performance and risk exposure.

(4) In applying this framework, licensees must adopt a risk-based and proportionate approach such that the level of governance, oversight, and control applied to a third-party arrangement reflects the nature, scale, complexity, and significance of the risks posed, regardless of whether the arrangement is classified as outsourcing.

(5) Where a non-outsourcing third-party arrangement is assessed as material or high-risk, licensees must apply risk management measures commensurate with the level of risk and potential impact, including, where appropriate, enhanced due diligence, contractual safeguards, ongoing monitoring, and contingency planning.

(6) Licensees must ensure that the application of controls to third-party arrangements is driven by the level of risk and potential impact and not solely by the classification of the arrangement, recognising that outsourcing constitutes a subset of broader third-party risk.

(7) Licensees must be able to demonstrate to the Supervisor, upon request, that all third-party arrangements have been appropriately identified, assessed, and subject to controls commensurate with their risk profile, including the rationale for the level of controls applied.

General Third-Party Risk Management Framework

2.13. Licensees must implement a comprehensive third-party risk management framework that addresses risks arising from both outsourcing and non-outsourcing third-party arrangements. Licensees may adopt either:

a. a single integrated third-party risk management policy; or
b. separate policies governing outsourcing and other third-party relationships, provided that such policies are consistent, comprehensive, proportionate, and risk-based.

Assessment of Technology-Driven Outsourcing Arrangements

2.14. (1) Licensees must apply enhanced risk assessment, due diligence, and governance measures to outsourcing arrangements involving new, emerging, or advanced technologies, recognising that such arrangements may increase operational, cybersecurity, data, and systemic risks. The requirements of this section supplement, and do not replace, the general requirements applicable to all outsourcing arrangements under these Standards.

(2) For the purposes of these Standards, technology-driven outsourcing arrangements include, but are not limited to, outsourcing arrangements involving:

a. cloud computing services, including infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS);
b. artificial intelligence (AI), machine learning (ML), or other automated decision-making technologies;
c. distributed ledger technologies (DLT), including blockchain-based systems and smart contracts; and
d. other digital infrastructure services, including application programming interfaces (APIs), fintech platforms, digital identity solutions, and payment or data-sharing ecosystems.

(3) Before entering any technology-driven outsourcing arrangement, licensees must undertake a comprehensive and documented risk assessment, which must, at a minimum:

a. identify and assess risks to operational resilience, including system availability, scalability, and recovery capabilities;
b. identify and assess cybersecurity risks, including vulnerabilities, threat exposure, incident response capabilities, and access controls;
c. assess risks relating to data confidentiality, integrity, protection, and location, including compliance with applicable data protection and cross-border data transfer requirements; and

d. evaluates dependencies and concentration risks, including reliance on single, dominant, or difficult-to-substitute service providers.

(4) In conducting the assessment referred to in paragraph 6.15(3), licensees must evaluate the potential impact of the arrangement on the licensee's:

a. financial condition and soundness;
b. operational resilience, business continuity, and ability to deliver important business services; and
c. compliance with applicable laws, regulations, and supervisory requirements.

(5) Before engagement, licensees must conduct robust and proportionate due diligence on technology service providers, including an assessment of:

a. the provider's governance and organisational structure;
b. the adequacy and effectiveness of the provider's information security and control environment, including relevant policies, controls, and independent assurance or certifications where available;
c. the provider's operational resilience, including business continuity and disaster recovery capabilities; and
d. the provider's technical capability, experience, and capacity to deliver the outsourced service on an ongoing basis.

(6) Technology-driven outsourcing arrangements must be subject to appropriate internal governance and approval processes before implementation, including review by senior management and approval by the board of directors or a designated committee and, where appropriate, having regard to the materiality and risk of the arrangement.

(7) Where a technology-driven outsourcing arrangement involves artificial intelligence, machine learning, or other automated decision-making systems, licensees must ensure that such arrangements are subject to appropriate governance, oversight, and control measures, including, where relevant:

a. clearly defined ownership, accountability, and oversight for the system or model;
b. appropriate validation and testing to ensure reliability, performance, and fitness for purpose;
c. ongoing monitoring and periodic review to identify performance deterioration, unintended outcomes, or material changes in behaviour;
d. appropriate transparency, governance, and human oversight, particularly where such systems support customer-facing decisions, risk management, or regulatory compliance; and
e. independent validation and testing to ensure accuracy, reliability, and fitness for purpose.

(8) Licensees must ensure that technology-driven outsourcing arrangements are subject to controls commensurate with the complexity, criticality, and risk profile

of the technology and the outsourced activity, and are monitored, reviewed, and risk-managed throughout their lifecycle.

(9) Licensees must be able to demonstrate to the Supervisor, upon request, that adequate risk assessments, due diligence, governance approvals, and control measures have been implemented in respect of all technology-driven outsourcing arrangements, including the methodologies and criteria applied in such assessments.

Proportionality

2.15. (1) Licensees must apply the requirements of this Standard of Sound Practice on Outsourcing and Third-Party Risk Management in a proportionate manner, such that the nature, extent, and sophistication of governance, risk management, and control measures are commensurate with the size, organisational complexity, and risk profile of the licensee and its outsourcing and non-outsourcing arrangements.

(2) In applying proportionality, licensees must ensure that controls are implemented in a risk-based, practical, and scalable manner and not applied uniformly across all outsourcing arrangements.

(3) In determining the appropriate level of controls, licensees must have regard to, at a minimum:

a. the size, scale, and organisational complexity of the licensee, including the structure of the group, where applicable;
b. the nature, scope, and complexity of the licensee's business activities, including the extent of digitalisation, cross-border operations, and reliance on third-party service providers; and
c. the criticality, importance, and materiality of the outsourced activity, including its relevance to the delivery of important business services and the licensee's operational resilience.

(4) Outsourcing arrangements assessed as material or high-risk must be subject to enhanced governance, oversight, and control measures, including, where appropriate, Board or senior management oversight, robust due diligence, comprehensive contractual provisions, and effective business continuity and exit planning.

(5) Outsourcing arrangements assessed as non-material or lower risk may be subject to proportionate controls, provided that such controls remain sufficient to identify, assess, monitor, and manage the risks arising from the arrangement.

(6) Licensees must establish and maintain documented methodologies and criteria for applying proportionality, including clear linkages between the assessed materiality and risk profile of outsourcing and non-outsourcing arrangements and the corresponding governance and control measures.

(7) Licensees must ensure that the application of proportionality does not result in the underestimation or inadequate management of risks and must be able to demonstrate to the Supervisor, upon request, that the controls applied are appropriate and commensurate with the risks identified.

(8) Licensees must periodically review and, where necessary, update their assessments of materiality and proportionality, including upon:

a. changes in the licensee's business model, scale, or complexity, where necessary;
b. the introduction of new products, services, technologies, or delivery channels;
c. changes in the nature, scope, or criticality of outsourcing arrangements; or
d. the occurrence of incidents, disruptions, or emerging risks that may affect the risk profile of the arrangement.

Critical Third Parties and Critical Outsourcing Arrangements

2.16. (1) Licensees must identify and assess critical third parties across all third-party relationships, recognising that criticality may arise irrespective of whether the arrangement constitutes outsourcing.

(2) For the purposes of these Standards, a critical third party refers to any third party that is essential to the continuous, secure, and efficient delivery of important business services or to the maintenance of the licensee's operational resilience, such that a failure, disruption, or weakness in the arrangement with such third party could materially impair the operations or financial condition of the licensee, threaten its safety and soundness, or adversely affect financial stability.

(3) In determining whether a third party is critical, licensees must have regard to factors including, but not limited to:

a. the extent to which the third party supports important business services or critical operations;
b. the degree of substitutability of the third party, including the time, cost, and operational complexity required to replace the service;
c. the level of dependency on the third party, including concentration risk and interdependencies with other service providers;
d. the nature, volume, and sensitivity of data, systems, or infrastructure to which the third party has access; and
e. the potential impact of a failure or disruption on customers, counterparties, market functioning, or the broader financial system.

(4) Licensees must recognise that criticality is distinct from materiality and must not limit the identification of critical third parties to outsourcing relationships only. In this regard, materiality relates to the impact of an arrangement's failure, while criticality relates to the importance of the third party or arrangement to the continuity of important business services and operational resilience.

(5) Where an outsourcing arrangement is assessed as both material and critical, licensees must apply the highest level of governance, oversight, and control measures under these Standards.

(6) Where a third-party arrangement is assessed as critical but does not constitute outsourcing, licensees must apply governance, risk management, and control measures commensurate with the criticality and risk of the arrangement and no less robust than those applied to material outsourcing arrangements of comparable risk.

(7) Licensees must ensure that critical third-party arrangements, whether outsourcing or non-outsourcing, are subject to enhanced controls, including, where appropriate:

a. strengthened due diligence and ongoing monitoring;
b. robust contractual provisions, including access, audit, and termination rights;
c. effective business continuity and disaster recovery arrangements;
d. contingency and exit planning, including consideration of alternative providers; and
e. heightened governance oversight, including senior management or Board-level review, where appropriate.

(8) Licensees must periodically review and update their assessments of critical third parties, including upon changes in business operations, technology, service dependencies, or the risk environment, and must be able to demonstrate to the Supervisor upon request the basis for such assessments and the adequacy of the controls applied.

Important business services and Operational Resilience

2.17. (1) For the purposes of these Standards, licensees must identify and document their important business services, being those services which, if disrupted, could result in significant harm to customers, market integrity, or the safety and soundness of the licensee, or could otherwise adversely affect financial stability.

(2) In identifying important business services, licensees must adopt a forward-looking and impact-based approach, having regard to the potential consequences of disruption, including customer detriment, financial loss, reputational damage, and breaches of applicable legal, regulatory, or supervisory requirements.

(3) For each important business service identified, licensees must undertake and maintain a documented mapping of the resources and dependencies required for the delivery of such service, including, at a minimum:

a. people, including key personnel and roles responsible for the delivery of the service;

b. processes and operational workflows supporting the service;
c. technology, systems, and digital infrastructure utilised;
d. physical facilities, including branches, offices, and data centres; and
e. information and data necessary for the functioning of the service.

(4) The mapping referred to in paragraph 2.17(3) must include all relevant third-party and intra-group arrangements, whether outsourced or non-outsourced, that support, enable, or are otherwise integral to the delivery of the important business service.

(5) Licensees must identify and understand the end-to-end dependency chain for each important business service, including:
a. direct third-party service providers;
b. sub-outsourcing arrangements and other downstream dependencies, including fourth parties; and
c. interconnections between systems, service providers, and infrastructure that may give rise to concentration, contagion, or single points of failure.

(6) Licensees must establish, document, and maintain an impact tolerance for each important business service, defined as the maximum level of disruption to the service, including duration and extent, that the licensee can tolerate before such disruption would:

a. materially impair the licensee's operations or financial condition;
b. threaten the safety and soundness of the licensee; or
c. cause significant harm to customers, counterparties, market integrity, or financial stability.

(7) In setting impact tolerances, licensees must consider relevant quantitative and qualitative metrics, including, where appropriate, maximum tolerable downtime, service availability thresholds, transaction processing capacity, recovery time objectives, and the nature and severity of potential customer harm.

(8) Licensees must take reasonable and proportionate measures to ensure that they can remain within established impact tolerances, including under severe but plausible disruption scenarios, such as cyber incidents, system failures, third-party outages, natural disasters, or other operational disruptions.

(9) Licensees must regularly test and validate their ability to remain within impact tolerances through appropriate scenario analysis, stress testing, and business continuity exercises, and must take timely remedial action where deficiencies or vulnerabilities are identified.

(10) Licensees must ensure that the identification of important business services, the mapping of dependencies, and the setting of impact tolerances are

subject to appropriate governance and oversight, including periodic review by senior management and, where appropriate, the Board or a designated committee.

(11) Licensees must periodically review and update the identification of important business services, dependency mappings, and impact tolerances to reflect changes in business activities, technology, third-party arrangements, and the evolving risk environment, and must be able to demonstrate to the Supervisor, upon request, the adequacy and effectiveness of such processes.

(B) Affiliates and Intragroup Outsourcing

2.18. Intragroup outsourcing arrangements are subject to the same regulatory and supervisory expectations as outsourcing arrangements involving non-affiliated third parties and must not be regarded as inherently less risky solely by virtue of being undertaken within a financial group.

2.19. Licensees must recognise that intragroup outsourcing may give rise to heightened or distinct risks, including, but not limited to:

a. arrangements that are not conducted on an arm's length basis;
b. actual or potential conflicts of interest between the licensee, its customers, and the affiliated service provider;
c. limitations on the licensee's ability, and by extension the Supervisor's ability, to effectively oversee, supervise, or influence the affiliated service provider; and
d. the absence of formal contractual arrangements or the inadequate enforcement of intra-group agreements.

2.20. Licensees must assess and manage the risks arising from intragroup outsourcing arrangements in a manner commensurate with the nature, scale, complexity, and risk profile of the arrangement, having regard to the degree of control and influence exercised over the affiliated service provider. In assessing such control and influence, licensees must consider, where relevant:

a. the degree of integration between the licensee's governance arrangements and the group's Board, committees, internal control functions, and other relevant governance structures;
b. the allocation of senior management and/or board of directors' responsibilities across the group;
c. the licensee's ability to direct, modify, escalate, or terminate the arrangement to ensure compliance with applicable legal, regulatory, and supervisory obligations; and
d. the robustness, consistency, and enforceability of group-wide policies, controls, and business continuity arrangements.

2.21. Where a licensee can demonstrate a high degree of control and influence over an affiliated service provider, the Supervisor may permit a proportionate

application of certain intragroup outsourcing requirements. Any such proportionate treatment must be exceptional, risk-based, and subject to the licensee demonstrating that equivalent governance, control, oversight, and risk management outcomes are achieved.

2.22. Without prejudice to paragraph 2.20, the following minimum requirements apply to all material intragroup outsourcing arrangements:

a. a formal outsourcing or service-level agreement must be executed and maintained, clearly defining the scope of services, responsibilities of the parties, service standards, sub-contracting conditions, escalation arrangements, and the legal nature of the relationship;
b. the licensee must conduct and document an assessment of the affiliated service provider's ability, capacity, resources, and organisational structure to deliver the outsourced activity in a sound, resilient, and compliant manner;
c. a documented and tested business continuity and disaster recovery plan must be maintained in respect of the outsourced activity;
d. a defined and documented process for ongoing monitoring, oversight, and performance review of the arrangement must be implemented; and
e. contractual arrangements must ensure that the Supervisor has timely and unrestricted access, upon request, to all books, records, systems, data, personnel, and other information relevant to the outsourced activity, to enable effective supervision.

2.23. Where a material intragroup outsourcing arrangement is established at the group level, whether centrally or for multiple group entities, the licensee must notify the Supervisor in advance and ensure that such arrangement remains subject to the applicable requirements of these Standards.

(C) Offshore Outsourcing

2.24. The requirements and expectations set out in this SSP OTPRM apply to outsourcing arrangements undertaken both within Jamaica and on a cross-border basis. Cross-border outsourcing arrangements remain subject to all applicable requirements of these Standards and, by reason of their additional complexity and risk, may require enhanced controls and oversight.

2.25. Licensees must recognise that cross-border outsourcing may give rise to heightened risks relative to domestic outsourcing arrangements, including, but not limited to:

a. differences in legal and regulatory frameworks, including data protection, confidentiality, contractual enforceability, insolvency, and prudential requirements;
b. jurisdictional challenges arising from the legal system of the service provider's location, including constraints relating to contract enforcement, asset access, insolvency, and regulatory cooperation;

c. limitations in monitoring, oversight, incident response, or the timely activation of business continuity and recovery arrangements; and
d. country risk, including political, economic, legal, social, or geopolitical developments that may adversely affect the service provider's ability to perform the outsourced activity.

2.26. For cross-border outsourcing arrangements, licensees must apply enhanced due diligence in accordance with paragraph 5.6, together with the following additional requirements specific to the cross-border context:
a. conduct and maintain a documented country risk assessment for each cross-border outsourcing arrangement, including consideration of political, economic, legal, regulatory, and operational conditions in the relevant jurisdiction;
b. clearly define the governing law, dispute resolution arrangements, and enforceability mechanisms applicable to the outsourcing agreement;
c. ensure, on an ongoing basis, that the arrangement does not impair the ability of the licensee or the Supervisor to access, supervise, review, reconstruct, or obtain promptly all books, records, systems, data, and other information relevant to the outsourced activity, and that such books, records, and key operational data remain capable of being produced in English within a reasonable period upon request;
d. promptly notify the Supervisor of any legal, regulatory, or operational development in the foreign jurisdiction that may materially impair access, oversight, performance, or supervisory effectiveness, including any request by a foreign authority for access to customer information; and
e. ensure that the heightened legal, operational, and jurisdictional risks identified under this paragraph and paragraph 5.6 are reflected in strengthened contractual safeguards and reviewed as part of the ongoing monitoring and periodic reassessment required under paragraphs 4.6, 4.17, and 6.7.

2.27. Where a cross-border outsourcing arrangement is material, the Supervisor may impose enhanced supervisory requirements, including additional reporting, periodic country risk assessments, contingency planning documentation, independent assurance, or third-party audit reports.

2.28. The Supervisor may, where necessary, engage in supervisory cooperation or information sharing with relevant foreign supervisory or regulatory authorities to support effective oversight of cross-border outsourcing arrangements, where applicable.

2.29. In the case of cross-border intragroup outsourcing arrangements, licensees must ensure that:
a. a comprehensive and up-to-date inventory of all such arrangements is maintained, including clear identification of those assessed as material;

b. documented service-level agreements are maintained for all such arrangements and include, where relevant, performance standards, escalation arrangements, audit rights, and sub-outsourcing controls;
c. appropriate governance and oversight arrangements are in place, including transparency over further intra-group dependencies and any external subcontracting; and
d. documented escalation arrangements are maintained to ensure that operational issues, control weaknesses, or supervisory concerns can be escalated to relevant group functions and addressed in a timely manner.

(D) Sub-contracting of Outsourced Tasks

2.30. For the purposes of these Standards, "sub-outsourcing" refers to an arrangement whereby a third-party service provider engaged by a licensee further transfers, in whole or in part, the performance of an outsourced activity, service, or function to another third party.

2.31. Licensees must recognise that sub-outsourcing, including chain outsourcing, may heighten risks in outsourcing arrangements, including by:
a. reducing the licensee's ability to effectively identify, monitor, and manage risks, particularly where complex chains of sub-outsourced parties span multiple jurisdictions; and
b. introducing or increasing dependencies on third parties that the licensee may not have visibility over and may not have independently selected or approved.

2.32. A service provider must not sub-contract, in whole or in part, an outsourced activity without the prior written approval of the licensee, where such sub-contracting is material to the outsourced activity or may materially affect the risk profile of the arrangement.

2.33. As part of the due diligence process, a licensee must assess the capacity, capability, financial soundness, operational resilience, and control environment of any proposed sub-contractor to deliver the relevant services, activities, or functions on a continuous and compliant basis.

2.34. Licensees must ensure that they retain full, prompt, and effective access to all data, records, systems, and other information maintained by sub-contractors, regardless of location, legal form, or contractual tier.

2.35. Written agreements for material outsourcing arrangements must explicitly state whether sub-outsourcing is permitted. Where sub-outsourcing is permitted, such agreements must:
a. identify any activities that are prohibited from being sub-outsourced;

b. establish the conditions under which sub-outsourcing may occur, including the obligation of the service provider to oversee and monitor its sub-contractors so that all obligations owed to the licensee are continuously met;
c. require the service provider to obtain the licensee's prior written approval before transferring customer information, confidential information, or material operational data to a sub-contractor;
d. require the service provider to notify the licensee in advance of any proposed material sub-outsourcing arrangement or material change thereto, including changes to key sub-contractors, subcontracting locations, or notification periods, sufficiently in advance to allow the licensee to assess the impact and exercise any approval, objection, or termination rights;
e. provide the licensee with the right to approve, object to, or impose conditions on proposed material sub-outsourcing arrangements or material changes thereto; and
f. provide the licensee with the contractual right to suspend, restrict, or terminate the outsourcing arrangement where sub-outsourcing materially increases risk, impairs control, or is undertaken without the licensee's approval or required notification.

2.36. Circumstances in which a licensee may consider exercising its contractual rights under paragraph 2.35(f) include, but are not limited to:
a. the service provider updates its list of material sub-contractors without notifying the licensee and includes a sub-contractor with a history of serious operational, control, or data security failures;
b. a sub-contractor fails to grant the licensee or an authorised independent auditor timely access to relevant operations, systems, records, or data related to the outsourced activity;
c. a significant incident at a sub-contractor results in disruption beyond the licensee's impact tolerances for important business services;
d. the sub-contractor repeatedly causes failure to meet agreed service levels, control standards, or key performance indicators;
e. the sub-contractor becomes subject to insolvency, enforcement action, or legal proceedings that materially impair service continuity; or
f. post-incident remediation is inadequate or fails to address material deficiencies within an appropriate timeframe.

Oversight of Sub-outsourcing

2.37. For outsourcing arrangements that are material, critical, or otherwise involve material sub-outsourcing risk, licensees must:
a. assess the risks associated with sub-outsourcing before entering the outsourcing arrangement;
b. determine whether the sub-outsourced activity meets the materiality or criticality thresholds set out in these Standards, including its impact on operational resilience and the continuity of important business services;

c. ensure that the primary service provider has the capacity, capability, and governance arrangements necessary to oversee its sub-contractors in accordance with the licensee's policies and these Standards;
d. ensure that contractual obligations applicable to the primary service provider, including obligations relating to confidentiality, access, audit, resilience, compliance, and business continuity, are appropriately flowed down to sub-contractors; and
e. clearly specify in the outsourcing agreement whether sub-outsourcing is permitted and, if so, the conditions under which it may occur.

2.38. In determining the appropriate oversight approach, licensees must consider whether the sub-outsourced activity involves access to customer information, confidential information, critical systems, or important business services, and whether additional safeguards, including encryption, segregation of duties, resilience controls, or contingency measures, are required. Where sub-outsourcing is undertaken on a cross-border basis, licensees must assess the legal, data protection, operational, and regulatory implications in each relevant jurisdiction.

(E) Concentration of Outsourcing Tasks

2.39. Licensees must recognise that concentration risk may arise where multiple outsourcing or third-party arrangements create excessive dependence on a common service provider, shared infrastructure, or interconnected supply chain. Such concentration may amplify operational risk at both the institutional and sectoral level and, in certain circumstances, may give rise to systemic risk.

2.40. Concentration risk may arise, including, but not limited to, where:
a. a service provider becomes unable to perform services that are critical or material to a significant number of licensees, resulting in simultaneous disruption across multiple institutions;
b. a flaw, vulnerability, or control failure in a product, platform, or service relied upon by multiple licensees simultaneously affects multiple institutions;
c. a shared application, software dependency, or technology vulnerability enables unauthorised access to, disruption of, or compromise of the systems or data of multiple licensees; or
d. multiple licensees depend on a common provider of business continuity, disaster recovery, cloud, telecommunications, or other critical support services, such that simultaneous demand may exceed the provider's operational capacity.

2.41. Licensees must periodically assess and manage concentration risks arising from outsourcing and broader third-party dependencies at both the institutional and, where relevant, group level. This includes:

a. assessing the degree of reliance on individual service providers and groups of connected or affiliated service providers;
b. identifying concentration risk, vendor lock-in, and substitutability constraints arising from multiple arrangements with the same provider or with connected providers;
c. identifying common dependencies across otherwise unrelated service providers, including shared sub-contractors, cloud infrastructure, software components, or other fourth-party dependencies;
d. assessing dependencies on service providers that are highly specialised, proprietary, dominant, or otherwise difficult to substitute; and
e. assessing geographic concentration risk, including where critical outsourced activities or key third-party services are concentrated in a single jurisdiction, region, or operational hub.

2.42. Licensees must establish and maintain appropriate strategies to monitor and, where necessary, mitigate concentration risks arising from outsourcing and third-party dependencies. Such strategies may include, where appropriate:
a. conducting scenario analysis to assess the impact of the failure, disruption, or degradation of a dominant or common service provider;
b. diversifying service providers, infrastructure dependencies, or recovery arrangements for critical or material services, where feasible and proportionate;
c. assessing whether service providers maintain adequate business continuity, incident response, recovery capacity, and surge capability in scenarios involving simultaneous disruption affecting multiple clients; and
d. participating in collective testing, industry exercises, or coordinated resilience assessments, where appropriate.

2.43. Licensees should, where appropriate, engage with peer institutions, financial groups, and relevant industry bodies to identify emerging concentration risks, promote resilience, and support sound practices for managing systemic dependencies on common providers.

SECTION 3: GOVERNANCE AND RESPONSIBILITY FOR OUTSOURCING

Governance

3.1. The responsibilities of the Board of directors and senior management of a licensee must not be outsourced. Accordingly, the Board and senior management retain full responsibility, accountability, and legal liability for all outsourced activities to the same extent as if such activities were undertaken internally.

3.2. Licensees remain fully accountable for compliance with all applicable legal, regulatory, and supervisory obligations, regardless of whether an activity is outsourced.

3.3. The Board must:
   a. establish and promote an appropriate governance and control environment, including a clearly defined risk appetite and tolerance for outsourcing and third-party arrangements; and
   b. remain responsible for the effective oversight of risks arising from outsourcing and third-party arrangements, including by:
      i. understanding the institution's reliance on material or critical outsourced services and third-party arrangements; and
      ii. ensuring that effective governance, risk management, and internal control systems are implemented to identify, monitor, and manage risks arising from such arrangements.

3.4. Management information relating to outsourcing and third-party arrangements submitted to the Board must be presented in a clear, consistent and timely manner, and with sufficient detail, to enable the Board to effectively oversee such arrangements, meaningfully challenge management, and make informed decisions in the discharge of its responsibilities.

Shared responsibility outsourcing arrangements

3.5. Where responsibility for the performance of outsourced services is shared between the licensee and the service provider, licensees must:
   a. clearly define, document, and understand the allocation of responsibilities between the parties; and
   b. ensure that such allocation is consistent with applicable legal, regulatory, and supervisory obligations and does not result in control, compliance, or accountability gaps.

3.6. Licensees must recognise that shared responsibility arrangements may arise in a range of outsourcing models, including cloud computing arrangements, and

must ensure that responsibilities for governance, security, compliance, operational resilience, and incident management are clearly allocated, understood, and enforceable.

3.7. Licensees must apply a risk-based approach to shared responsibility arrangements, including in respect of access management, operational resilience, and business continuity.

3.8. Illustrative examples of shared responsibility arrangements, including in the cloud service model section.

Non-Outsourceable Activities and Responsibilities

3.9. A licensee may outsource the performance of certain activities, functions, or processes to a third party, provided that such outsourcing is consistent with safe and sound operations and does not impair the licensee's ability to remain responsible for its regulated business. However, a licensee must not outsource any activity, function, or responsibility where doing so would materially undermine its governance, impair its ability to exercise independent judgement, weaken its system of internal control, or result in the effective delegation of responsibility that properly rests with the Board, senior management, or the licensee itself.

3.10. Outsourcing must not result in the licensee becoming an "empty shell" that lacks the operational substance, management capacity, or control functions necessary to conduct its business safely and soundly. A licensee must at all times retain sufficient substance, competence, and authority to direct its affairs, oversee outsourced and third-party arrangements, and comply with all applicable legal, regulatory, and supervisory obligations.

3.11. A licensee must not outsource the responsibilities of its Board. The Board remains ultimately accountable for the safety and soundness of the licensee and must not delegate its fiduciary, strategic, or oversight responsibilities to any third party. This includes responsibility for approving and overseeing the licensee's business strategy, risk appetite, governance arrangements, internal control framework, outsourcing and third-party risk management framework, and policies governing material activities and risks. The Board may obtain advice, technical support, or independent assurance from external parties, but it must retain responsibility for decision-making, oversight, challenge, and accountability.

3.12. A licensee must not outsource the responsibilities of senior management. Senior management remains responsible for the day-to-day management of the licensee, the implementation of Board-approved strategies and policies, and the effective oversight and control of outsourced and third-party arrangements. This includes responsibility for operational management, escalation and remediation

of issues, management of material incidents, implementation of internal controls, and ensuring that outsourced activities are conducted in a safe, sound, and compliant manner.

3.13. A licensee must not outsource the accountability and responsibility for its risk management function. While external parties may provide specialist advice, analytical support, or technical services, the licensee must retain responsibility for identifying, measuring, monitoring, managing, and reporting risks, and for maintaining an effective enterprise-wide risk management framework. Accountability and Responsibility for setting risk limits, determining risk appetite, assessing risk exposures, approving risk treatment measures, and escalating material risk issues must remain with the licensee.

3.14. A licensee must not outsource accountability for compliance with applicable legal, regulatory, prudential, and supervisory obligations. The licensee remains responsible and accountable for ensuring compliance with all applicable laws, regulations, standards, rules, directives, and supervisory expectations, irrespective of whether operational support is obtained from a third party. This includes responsibility for maintaining an effective compliance function, monitoring compliance, managing regulatory obligations, and ensuring timely and accurate regulatory reporting.

3.15. A licensee must not outsource accountability for its internal audit function. Internal audit must remain independent, objective, and accountable to the Board or Audit Committee for assuring the adequacy and effectiveness of governance, risk management, and internal controls. A licensee may engage external specialists to support or supplement internal audit activity in limited circumstances, but ownership of the internal audit plan, scope, findings, reporting, and assurance conclusions must remain with the licensee.

3.16. A licensee may outsource operational support in performing regulated tasks, but it must not outsource accountability and responsibility for compliance with applicable legal and regulatory obligations. The licensee remains fully responsible for compliance with all statutory, prudential, conduct, tax, reporting, sanctions, consumer protection, data protection, and other legal obligations applicable to its business. Outsourcing must not diminish the licensee's accountability to the Supervisor, customers, counterparties, or any competent authority.

3.17. A licensee may obtain third-party support in relation to customer onboarding, screening, transaction monitoring tools, or other supporting processes, but it must not outsource responsibility for compliance with applicable anti-money laundering, counter-financing of terrorism, and counter-proliferation financing. Responsibility for customer due diligence, ongoing monitoring, sanctions compliance, suspicious transaction reporting, escalation of unusual or suspicious

activity, and compliance with applicable AML/CFT/CPF obligations must remain with the licensee.

3.18. A licensee must not outsource decisions that require the exercise of judgement, discretion, or authority that properly rests with the Board, senior management, or control functions. This includes, but is not limited to:

a. approval of risk appetite, risk limits, and material risk exposures;
b. approval of credit policy and material credit decisions;
c. approval of products, business lines, and strategic initiatives;
d. approval of material and non-material outsourcing and non-outsourcing arrangements;
e. approval of regulatory submissions, attestations, and certifications;
f. approval of capital, liquidity, and recovery decisions;
g. approval of material incident response, escalation, and remediation decisions; and
h. decisions relating to customer treatment, complaints escalation, or conduct matters where judgement is required.

A third party may support analysis or provide recommendations, but decision-making authority must remain with the licensee.

3.19. A licensee must not outsource ownership of its internal policies, governance arrangements, risk management framework, control environment, or internal standards. Third parties may provide advisory, technical, drafting, or benchmarking support, but responsibility for establishing, approving, implementing, and maintaining the licensee's internal policies and control frameworks must remain with the licensee.

3.20. A licensee must not outsource responsibility for the oversight, monitoring, and management of its outsourcing and third-party arrangements. The licensee must retain sufficient internal capability and expertise to:

a. conduct due diligence;
b. assess and manage third-party risks;
c. monitor performance and compliance;
d. challenge service providers;
e. oversee subcontracting arrangements;
f. assess incidents, weaknesses, and control failures;
g. implement contingency measures; and
h. execute exit, transition, or in-sourcing plans.

3.21. A licensee must not outsource any arrangement in a manner that prevents it from effectively overseeing, controlling, or exiting the arrangement.

3.22. A licensee must not outsource any activity in a manner that results in the effective transfer of the licence, regulated business, or regulated discretion to a third party.

3.23. A licensee must not outsource any activity where doing so would result in a third party effectively:
   a. conducting licensed business in place of the licensee except as allowed under the Agent Banking Framework;
   b. exercising core regulated discretion on behalf of the licensee without effective oversight;
   c. assuming control of the licensee's regulated operations; or
   d. undermining the legal, operational, or prudential substance of the licensee.

3.24. Outsourcing must not be used to circumvent licensing, governance, accountability, or prudential requirements.

3.25. A licensee may outsource the performance of a task, but it must not outsource responsibility for that task. Outsourcing does not transfer accountability. A licensee remains fully responsible for all outsourced and third-party arrangements and for ensuring that such arrangements are prudently managed, effectively controlled, and conducted in a manner consistent with applicable legal, regulatory, and supervisory requirements.

3.26. The Supervisor will hold the licensee, and where appropriate its Board and senior management, accountable for any failure arising from an outsourced or third-party arrangement, irrespective of whether a third party performed the relevant activity. The Supervisor's expectations, and the licensee's obligations under law, remain fully applicable to all outsourced and third-party arrangements.

Outsourcing Policy

3.27. The Board must approve, oversee, and periodically review a written outsourcing policy governing outsourcing arrangements and, where applicable, other material third-party arrangements.

3.28. The outsourcing policy must be aligned and integrated with relevant internal policies and frameworks, including, where applicable, business model and strategy, Business continuity, Conflicts of interest, Data protection, Information and communication technology (ICT), Information and cyber security, Operational resilience, and Risk management.

3.29. Licensees must ensure that relevant third-party service providers are made aware of applicable internal policies, standards, and control requirements relevant to the outsourced activity.

3.30. Where internal policies contain sensitive information or such information subject to the requirements of section 5 (F), licensees may disclose only those portions necessary to inform the service provider's responsibilities, provided that such limitation does not impair the service provider's ability to comply with the

licensee's requirements. Such disclosure does not diminish the licensee's accountability for outsourced activities.

3.31. Business continuity and contingency planning must address, at a minimum, the deterioration of outsourced services to unacceptable levels, the insolvency, failure, or disruption of a service provider, and jurisdictional, legal, or political risks arising in the service provider's location.

3.32. The outsourcing policy may be documented as a standalone policy or integrated within broader governance, risk, or operational risk frameworks, provided that it remains clearly identifiable, comprehensive, and proportionate to the licensee's size, complexity, and risk profile.

3.33. The outsourcing policy must, at a minimum, address:

a. governance and accountability arrangements, including Board oversight, senior management responsibilities, and the roles of business lines and control functions;
b. risk assessment, due diligence, and materiality classification requirements;
c. supervisory notification, escalation, and internal approval requirements;
d. ongoing oversight and performance monitoring, including incident reporting, service level monitoring, independent review, audit, and renewal processes;
e. business continuity, contingency planning, and exit planning for material arrangements; and
f. recordkeeping and documentation requirements.

Record-Keeping of Outsourced and Third-Party Arrangements

3.34. Licensees must maintain comprehensive, accurate, and current records of all outsourcing and third-party arrangements, clearly identifying those assessed as material, critical, or otherwise high-risk.

3.35. Such records must be sufficient to enable the licensee and the Supervisor to assess at a minimum, concentration risk, jurisdictional and geographic risk, and aggregate risk exposure across the institution or, where applicable, the group.

3.36. Licensees must maintain an Outsourcing and Third-Party Register containing, at a minimum:

a. all outsourcing and other third-party arrangements;
b. classification of each arrangement by materiality, criticality, and risk; and
c. such other information as may be determined by the Supervisor.

3.37. The Outsourcing and Third-Party Register must be submitted to the Supervisor at least annually.

3.38. Licensees must provide the Supervisor, upon request, with such additional information as may be reasonably required for the effective supervision of outsourcing and third-party arrangements.

SECTION 4: ASSESSMENT OF MATERIALITY

Under this section of the SSP OTPRM, the Supervisor expects licensees to:

a. *assess the materiality and, where relevant, criticality of each outsourcing and third-party arrangement;*
b. *conduct due diligence commensurate with the nature, materiality, criticality, and risk profile of the arrangement; and*
c. *assess and manage the risks arising from each outsourcing and third-party arrangement on an ongoing basis.*

Application of Materiality Assessments

4.1. A licensee must determine the materiality of each outsourcing or third-party arrangement using a documented, risk-based methodology that is appropriate to the nature, scale, complexity, and risk profile of the arrangement and of the licensee's business.

4.2. In assessing materiality, a licensee must apply sound judgement and must not rely solely on fixed quantitative thresholds, financial metrics, or cost-based measures in determining whether an arrangement is material.

4.3. A licensee must ensure that the assessment of materiality is based on the potential impact of a failure, disruption, weakness, or defect in the arrangement, having regard to the criteria set out in paragraphs 4.10 and 4.11, and not merely the size, cost, or commercial value of the arrangement. For the avoidance of doubt, an arrangement must not be treated as non-material merely because the underlying activity is perceived to be routine, technical, ancillary, or capable of being characterised as a 'back-office' or 'support' function; arrangements that support critical systems, important business services, or key operational processes must be assessed as material notwithstanding the apparent nature of the underlying function.

4.4. Quantitative indicators may be used to support the assessment of materiality, including indicators relating to cost, transaction volumes, customer impact, operational dependency, substitutability, financial exposure, concentration, or transition risk, but such indicators must serve only as supporting inputs and must not be treated as determinative.

4.5. Materiality and criticality assessments must be undertaken at the level of the individual licensee. Where such assessments are also performed on a group-

wide basis, licensees must independently assess the materiality and criticality of each arrangement having regard to their own business activities, operational dependencies, risk appetite and risk profile.

Timing and Frequency of Assessments

4.6. Licensees must assess the materiality and, where relevant, criticality of each outsourcing and third-party arrangement:
   a. before entering into the arrangement;
   b. periodically thereafter, including as part of scheduled review processes;
   c. where there is a material increase in the scale, scope, reliance, or dependency associated with the arrangement; and
   d. where there is a material change affecting the service provider, sub-contractor, or operating environment that may alter the risk profile of the arrangement.

4.7. Where a licensee reasonably expects that an arrangement currently assessed as non-material may become material, the licensee must take reasonable steps to ensure that the arrangement is managed in accordance with the requirements applicable to material arrangements before the relevant threshold is crossed.

4.8. Where a non-material arrangement may become material under a severe but plausible stress scenario, including in circumstances of disruption, contingency, or heightened dependency, licensees must consider whether enhanced controls are warranted having regard to the potential impact on operations, customers, or important business services.

Criteria for Assessing Materiality

4.9. Licensees must establish and maintain a documented and consistently applied methodology for assessing the materiality of outsourcing and third-party arrangements.

4.10. In assessing materiality, licensees must consider whether a failure, disruption, weakness, or defect in the arrangement could adversely affect, inter alia:
   a. the licensee's ability to comply with applicable legal, regulatory, or supervisory obligations;
   b. the safety and soundness of the licensee, including its financial or operational resilience;
   c. the continuity of important business services;
   d. customers, counterparties, or market integrity; or
   e. financial stability, where relevant.

4.11. In applying paragraph 4.9, licensees must consider, where relevant, inter alia:
   a. the importance of the relevant business function or service;
   b. the potential impact on customers, counterparties, and key business lines;

c. the substitutability of the service provider and the feasibility, cost, and timing of transition, replacement, or in-sourcing;
d. the financial significance of the arrangement;
e. the extent to which the arrangement affects internal controls, regulatory compliance, or operational resilience;
f. dependencies or interconnections with other business functions, service providers, or systems;
g. legal, reputational, confidentiality, and data integrity risks; and
h. concentration risk, including aggregate exposure to a service provider or group of connected providers.

4.12. Licensees must classify an arrangement as material where one or more of the criteria in paragraphs 4.9 or 4.10 indicate that failure, disruption, or weakness in the arrangement could have a material adverse impact on the licensee, its customers, important business services, or financial stability. Arrangements classified as material are subject to the enhanced governance, due diligence, contractual, and control requirements set out in Section 3 and Section 5, commensurate with their risk; arrangements assessed as non-material remain subject to the proportionate measures required under this SSP OTPRM.

4.13. A licensee must not classify an arrangement as non-material solely because it falls below an internal financial, operational, or quantitative threshold where the failure, disruption, weakness, or defect in that arrangement could nevertheless materially impair:
a. the continuity of important business services;
b. the licensee's safety and soundness;
c. compliance with applicable legal, regulatory, or supervisory obligations;
d. customer outcomes, market integrity, or confidence in the licensee; or
e. operational resilience or financial stability, where relevant.

4.14. In applying the materiality assessment methodology, a licensee must presume an arrangement to be material where the arrangement:
a. supports or enables an important business service;
b. supports a critical business line, core banking function, or payments activity;
c. involves the processing, storage, transmission, or protection of customer information or sensitive data at scale;
d. supports compliance with legal, regulatory, prudential, AML/CFT, sanctions, or reporting obligations;
e. supports a control function, including risk management, compliance, finance, or internal control processes;
f. gives rise to material concentration risk, including reliance on a dominant provider, a connected group of providers, or a common market utility;
g. is highly integrated with internal systems, infrastructure, or other material service providers such that disruption could give rise to cascading operational impacts; or

h. would be difficult, costly, or time-consuming to replace, transition, substitute, or in-source without material disruption.

4.15. Where a licensee determines that an arrangement falling within paragraph 4.14 is not material, the licensee must document the basis for that determination in sufficient detail to demonstrate that the arrangement does not give rise to material prudential, operational, customer, conduct, concentration, or systemic risk.

4.16. The Supervisor may require a licensee to classify any outsourcing or third-party arrangement as material where the Supervisor considers that a failure, disruption, weakness, or defect in the arrangement could give rise to heightened prudential, operational, legal, conduct, concentration, reputational, or systemic risk, irrespective of the licensee's internal classification.

4.17. A licensee must review materiality assessments periodically, and in any event where there is a material change in the scope, nature, risk profile, dependency, concentration, criticality, substitutability, or operational relevance of the arrangement, and must promptly revise the classification where appropriate. A licensee must be able to demonstrate to the Supervisor, upon request, the basis for its materiality classifications and the adequacy of the controls applied, including the methodology, assumptions, and judgement used.

Notification and Approvals

4.18. Licensees must assess, at an early stage in the planning process, whether a proposed outsourcing or third-party arrangement may give rise to any requirement for notification to, consultation with, or approval from the Supervisor under the Banking Services Act.

4.19. Where notification, consultation, approval, or non-objection is required, licensees must engage the Supervisor sufficiently in advance of implementation to allow for supervisory review and, where necessary, approval or non-objection.

4.20. In connection with any such engagement, licensees must be prepared to:
a. provide such information as the Supervisor may reasonably require; and
b. take such remedial or follow-up action as may be necessary, including enhancing due diligence, governance, contractual safeguards, or risk controls, and, where necessary, delaying implementation until supervisory concerns have been addressed.

SECTION 5: KEY OUTSOURCING STANDARDS

(A) Due Diligence Standards

This section outlines the Supervisor's expectations and requirements regarding due diligence in the selection and monitoring of a service provider and the service provider's performance. These expectations are intended to ensure that licensees maintain effective risk management and operational resilience throughout the outsourcing lifecycle.

Pre-Contract Due Diligence

5.1 Licensees must conduct comprehensive and documented due diligence on all prospective third-party service providers before entering into any outsourcing or material third-party arrangement. Such due diligence must be proportionate to the nature, scale, complexity, and materiality of the proposed arrangement.

5.2 Where practicable, a licensee must identify, assess, and maintain awareness of alternative or substitute service providers capable of delivering the outsourced service, to mitigate concentration risk and reduce the risk of vendor lock-in. This assessment must consider the feasibility, cost, timing, and operational implications of transitioning to such providers.

5.3 Where no viable or effective alternative provider exists, a licensee must implement enhanced risk management measures to address the resulting dependency. These measures must include, at a minimum, robust business continuity and disaster recovery arrangements, credible contingency plans, and comprehensive exit strategies designed to ensure that important business services can continue to be delivered, or restored within established impact tolerances, in the event of disruption, failure, or termination of the service provider.

5.4 In selecting a service provider, licensees must exercise due care, skill, and diligence and must be satisfied that the service provider possesses:

a. adequate technical competence and expertise;
b. sufficient financial soundness and sustainability;
c. appropriate legal capacity and authorisations to perform the outsourced activity; and
d. the operational capability to perform the service reliably under normal and stressed conditions.

5.5 For all material outsourcing arrangements, licensees must conduct enhanced due diligence, which must include, at a minimum:

a. assessment of the service provider's ownership structure, financial condition, and group affiliations;

b. evaluation of the provider's corporate governance framework, internal controls, and risk management practices;
c. verification of any required regulatory licences or approvals regarding the service or activity being provided by the service provider;
d. assessment of the provider's operational resilience, including business continuity and disaster recovery capabilities;
e. evaluation of the provider's information security and data protection controls, particularly where customer data or sensitive information is involved;
f. analysis of the risk of vendor lock-in, including dependence on proprietary systems, platforms, or infrastructure;
g. screening for sanctions, enforcement actions, or fit and proper concerns; and
h. assessment of sub-outsourcing arrangements, including dependencies on subcontractors and other fourth-party providers.

5.6 Where outsourcing or third-party arrangements involve cross-border service providers, licensees must conduct additional due diligence, including:
a. assessment of the legal and regulatory framework of the jurisdiction in which the service provider operates, and of the provider's capacity to comply with Jamaican legal, regulatory, and supervisory expectations;
b. evaluation of risks arising from extraterritorial laws, including those affecting data access, confidentiality, and privacy, and confirmation that confidentiality obligations owed under Jamaican law and contractual arrangements remain enforceable notwithstanding the laws of the foreign jurisdiction;
c. assessment of the enforceability of contractual rights and supervisory actions;
d. evaluation of the ability of the licensee and the Supervisor to conduct effective audits, inspections, or supervisory reviews, and to access, reconstruct, or obtain in a timely manner all books, records, systems, and data relevant to the outsourced activity;
e. identification of any restrictions on data transfer, storage, or repatriation;
f. verification of the provider's authorisations or registrations required to perform the service; and
g. confirmation of adherence to recognised international standards, including information security and operational resilience frameworks.

Ongoing Due Diligence and Monitoring

5.7 Licensees must establish and maintain ongoing due diligence and monitoring frameworks to ensure that service providers continue to meet contractual, regulatory, and operational requirements throughout the duration of the arrangement.

5.8 The frequency and intensity of monitoring must be risk-based and reflect the materiality and criticality of the arrangement.

Performance Monitoring and Escalation

5.9 Licensees must establish clear, documented criteria for:

a. monitoring service provider performance;
b. identifying breaches of contractual or regulatory obligations; and
c. escalating issues for timely remediation.

Such criteria must include defined thresholds or triggers that may result in remedial actions, enhanced oversight, or termination of the outsourcing arrangement.

Minimum Monitoring Requirements

5.10 Ongoing monitoring must include, at a minimum:
a. clearly defined and measurable service level agreements (SLAs);
b. periodic performance reviews and internal assessments;
c. independent audits or assurance reviews, where appropriate;
d. regular reporting by the service provider on performance, incidents, and risks;
e. defined consequences or penalties for failure to meet agreed performance standards; and
f. access to relevant records, logs, and systems for audit, forensic analysis, or supervisory review.

Governance of Due Diligence

5.11 Licensees must ensure that:
a. due diligence is conducted by competent and qualified personnel with appropriate expertise;
b. relevant internal functions, including risk management, compliance, legal, and technology, are involved in the due diligence process; and
c. a centralised function, committee, or governance structure is established or incorporated into existing governance framework to oversee third-party risk assessments, vendor selection and approval, performance monitoring and documentation and reporting.

Resilience and Scenario Assessment

5.12 As part of due diligence and ongoing monitoring, licensees must assess the service provider's resilience to severe but plausible disruptions, including:
a. cyber incidents and technology failures;
b. pandemics or public health emergencies;
c. geopolitical or jurisdictional instability; and
d. natural disasters or other external shocks.

5.13 Where a licensee engages a service provider for multiple services, the licensee must assess its aggregate exposure to that provider and implement appropriate safeguards to mitigate concentration risk, single points of failure and systemic dependencies.

5.14 Licensees must maintain comprehensive and up-to-date records of all due diligence activities, including:

a. risk assessments and evaluation reports;
b. vendor selection criteria and decision-making processes;
c. internal approvals, including board or management committee decisions; and
d. ongoing monitoring reports and performance evaluations.

Such records must be made available to the Supervisor upon request.

5.15 Where a service provider commits a material breach of legal, regulatory, or contractual obligations, or where such breach materially affects the licensee:

a. the licensee must notify the Supervisor promptly upon becoming aware of the breach; and
b. the licensee must implement immediate remedial actions to mitigate the impact of the breach.

5.16 Licensees must maintain an up-to-date register of all subcontractors and fourth-party providers involved in delivering outsourced and third-party services. This register must be made available to the Supervisor on an annual basis.

Governance and In-House Capability

5.17 The in-house expertise, resources, and operational capacity that a licensee must retain in respect of outsourcing and third-party arrangements, including the capability to oversee such arrangements, manage the associated risks, and ensure regulatory compliance, are set out in paragraph 3.20.

(B) Outsourcing Agreement

This section outlines the Supervisor's expectations and requirements regarding an outsourcing agreement. A legally binding written contract between a licensee and a service provider is a critical foundation of the outsourcing relationship. Contractual provisions reduce the risks of non-performance and support the resolution of disputes about the scope, nature, or quality of services provided. Written agreements also facilitate effective oversight by the licensee and the Supervisor.

5.18 A licensee must enter into a legally binding written contract with each third-party service provider for every outsourcing and non-outsourcing arrangement. The agreement must establish a clear and enforceable framework governing the rights and obligations of the parties and must be proportionate to the nature, scale, complexity, and materiality of the outsourced or non-outsourced activity.

5.19 Outsourcing agreements must:

a. ensure that the licensee retains effective control over the outsourced activity;

b. provide sufficient flexibility to allow for renegotiation, amendment, or termination where necessary; and
c. enable the licensee to comply fully with all applicable legal, regulatory, and supervisory requirements.

5.20 Outsourcing agreements must include provisions that allow for timely amendment to reflect:
a. changes in applicable laws or regulations;
b. evolving supervisory expectations; or
c. material changes in the licensee's risk profile or operational requirements.

5.21 Where a master services agreement (MSA) governs multiple outsourcing arrangements, the licensee must ensure that:
a. each outsourced service is clearly defined and documented; and
b. detailed service descriptions are set out in annexes, schedules, or addenda.

5.22 A separate standalone agreement is not required where the MSA adequately captures all required contractual elements.

5.23 Outsourcing agreements must not include any provision that:
a. restricts or impairs the ability of the Supervisor to exercise its supervisory or oversight functions;
b. limits the licensee's ability to comply with its regulatory obligations; or
c. restricts the licensee's or the Supervisor's access to data, systems, premises, or personnel relevant to the outsourced activity.

5.24 Licensees must apply minimum contractual provisions across all outsourcing arrangements regardless of materiality and jurisdictions.

Minimum Contractual Provisions

5.25 Each outsourcing agreement must, at a minimum, clearly define the respective roles, responsibilities, and obligations of the licensee and the service provider and must include the following provisions:
a. Scope and Description - a clear description of the outsourced function, activity, or service, including any ancillary or supporting services.
b. Term and Duration - the commencement date, duration, renewal terms, and conditions for termination.
c. Governing Law - the governing law of the agreement and the jurisdiction applicable to dispute resolution.
d. Financial Terms - all applicable fees, pricing structures, and payment obligations.
e. Dispute Resolution - clear dispute resolution mechanisms, including escalation procedures and, where applicable, arbitration or judicial processes.

f. Sub-Outsourcing Provisions - where sub-outsourcing is permitted, the agreement must include:
    i. conditions under which sub-outsourcing may occur;
    ii. a requirement for prior written consent of the licensee;
    iii. obligations relating to confidentiality, data protection, and security;
    iv. confirmation that the primary service provider retains full responsibility for performance, where applicable; and
    v. the right of the licensee to assess and monitor the provider's oversight of subcontractors.
g. Location of Services and Data - the agreement must specify:
    i. the jurisdictions in which services will be performed;
    ii. the locations where data will be stored, processed, or transmitted; and
    iii. requirements for prior notification and approval of material changes to such locations.
h. Data Protection and Information Security - contractual safeguards must ensure the confidentiality, integrity, availability, and security of data, including:
    i. compliance with applicable data protection laws, including the Data Protection Act;
    ii. data lifecycle management requirements; and
    iii. minimum cybersecurity standards and controls.
i. Performance Monitoring - the agreement must include:
    i. clearly defined service level agreements (SLAs) and key performance indicators (KPIs);
    ii. mechanisms for monitoring, reporting, and reviewing performance; and
    iii. procedures for remediation of performance failures.
j. Reporting Obligations - the service provider must be required to:
    i. provide performance and risk reports; and
    ii. notify the licensee promptly of any material developments, including incidents, breaches, or disruptions.
k. Insurance Requirements - where appropriate, the agreement must require the service provider to maintain adequate insurance coverage against operational risks.
l. Business Continuity and Disaster Recovery - the agreement must require the service provider to:
    i. maintain and test business continuity and disaster recovery plans; and
    ii. ensure alignment with the licensee's impact tolerances for important business services.
m. Data Access and Retrieval - the agreement must include provisions to ensure that the licensee retains full ownership of data, data can be retrieved promptly in a usable format upon request, and data remains accessible in the event of insolvency, disruption, or termination.
n. Compliance with Laws and Regulations - the service provider must be required to comply with all applicable laws and regulations and supervisory expectations in all relevant jurisdictions.

o. Regulatory Cooperation and Access - the agreement, in relation to the outsourced activity, must require the service provider to:
    i. cooperate fully with the Supervisor and its authorised representatives;
    ii. provide access to records, data, systems, and personnel; and
    iii. permit audits, inspections, and supervisory reviews.
p. Audit and Inspection Rights in relation to the outsourced activity- the licensee must have the right to:
    i. audit and inspect the service provider's operations; and
    ii. obtain independent assurance reports where appropriate.
q. Incident Management - where applicable, the agreement must include:
    i. procedures for identifying and managing operational or security incidents;
    ii. defined escalation timelines; and
    iii. notification requirements for incidents affecting the licensee.
r. Termination and Exit Provisions - the agreement must include clear termination rights, including:
    i. termination for breach of contract, law, or regulation;
    ii. termination where risk tolerances are exceeded;
    iii. termination for sustained performance failures; and
    iv. termination where continued outsourcing would threaten the safety and soundness of the licensee or ongoing disruption.
s. Exit Strategy and Transition - the agreement must support an orderly exit, including:
    i. transition assistance by the service provider, where applicable;
    ii. transfer of data and services without disruption; and
    iii. continuity of important business services during transition.
t. Unacceptable Contractual Limitations - where a service provider is unwilling or unable to agree to contractual terms that enable the licensee to meet its legal and supervisory obligations, the licensee must:
    i. notify the Supervisor promptly; and
    ii. refrain from entering into, or terminate, the arrangement.

5.26 Licensees must periodically review outsourcing agreements to ensure continued compliance with applicable laws and regulations, supervisory expectations and evolving risk conditions.

5.27 Licensees must maintain documented exit strategies for all material outsourcing arrangements and must periodically test the effectiveness of such strategies to ensure continuity of important business services.

5.28 All outsourcing and non-outsourcing agreements must comply with the laws of Jamaica, including but not limited to the Data Protection Act, and must not conflict with the licensee's regulatory and supervisory obligations.

(C) Outsourcing Data Security

Scope and Application

5.29 This section sets out the requirements and expectations of the Supervisor regarding the protection, management, and location of data accessed, processed, stored, or transmitted by third-party service providers. For the purposes of this section, data includes, but is not limited to:

a. confidential, institution-sensitive, and transactional data;
b. other personal and customer information;
c. externally sourced or open-source data used in financial services; and
d. systems and infrastructure used to process, store, or transmit such data.

These requirements apply to all outsourcing and third-party arrangements, whether material or non-material, involving access to or transfer of data.

Roles and Responsibilities

5.30 Where an outsourcing or third-party arrangement involves access to, or transfer of, data, the licensee must clearly define, document, and understand the responsibilities of all parties involved. Licensees must, at a minimum:

a. classify data based on its sensitivity, confidentiality, and criticality;
b. identify and assess legal, operational, reputational, and compliance risks associated with the data;
c. establish and agree on required levels of data confidentiality, integrity, and availability; and
d. obtain documented assurances from service providers regarding the lawful collection, processing, and use of data, where applicable.

5.31 A licensee must comply with the requirements set out in paragraphs 5.32 to 5.39 to satisfy the obligation in paragraph 5.30(d).

5.32 A licensee must ensure that any service provider that collects, accesses, processes, stores, transmits, or otherwise handles data on its behalf does so in a lawful manner and in compliance with all applicable data protection requirements.

5.33 A licensee must obtain documented assurances from the service provider confirming that:

a. all data has been lawfully collected and is processed on a valid legal basis;
b. data is processed solely for authorised and specified purposes as instructed by the licensee;
c. appropriate measures are in place to ensure the confidentiality, integrity, availability, and security of data;
d. data is not disclosed or transferred to unauthorised parties without the prior approval of the licensee and in accordance with applicable law; and

e. data is retained, archived, and securely disposed of in accordance with applicable legal and regulatory requirements.

5.34 The documented assurances referred to in paragraph 5.33 must be formal, enforceable, and verifiable, and must be reflected, where appropriate, in legally binding agreements, including contractual provisions, data processing agreements, or equivalent arrangements.

5.35 Licensee must ensure that outsourcing or third-party arrangements involving the processing of personal data are structured in a manner consistent with the requirements of Jamaica's Data Protection Act, including, where applicable, clearly defining the roles and responsibilities of the licensee as data controller and the service provider as data processor.

5.36 A licensee must not assume that a service provider complies with applicable data protection requirements. The licensee must undertake appropriate due diligence and obtain sufficient information and evidence to assess the service provider's data governance framework, policies, controls, and capabilities before entering into the arrangement.

5.37 A licensee must ensure that it retains the ability to monitor, assess, and enforce the service provider's compliance with applicable data protection obligations on an ongoing basis, including through audit rights, reporting requirements, and access to relevant information.

5.38 A licensee remains fully responsible and accountable for compliance with all applicable data protection obligations in respect of data processed under any outsourcing or third-party arrangement. Outsourcing does not transfer or diminish the licensee's legal, regulatory, or supervisory responsibilities.

5.39 Where deficiencies, breaches, or weaknesses in a service provider's data protection practices are identified, the licensee must take prompt and effective remedial action, including escalation, remediation, or termination of the arrangement, where appropriate, to ensure continued compliance and protection of data.

5.40 Licensees must not delegate regulatory or legal responsibility for data to any third-party service provider. The licensee remains fully accountable for ensuring compliance with:

a. applicable laws, including the Data Protection Act; and
b. all regulatory and supervisory requirements of the Supervisor.

5.41 Licensees must identify, assess, and manage risks associated with data handled by third parties, including risks relating to unauthorised access, data breaches or leakage, data loss or unavailability, theft, misuse, or unauthorised disclosure and data corruption, manipulation, or integrity failures.

5.42 Licensees must implement a risk-based data classification framework that categorises data according to its sensitivity and criticality. At a minimum, classifications must include confidential or restricted data, customer and personal data, sensitive or strategic institutional information and transactional or payment data.

5.43 Data classification and protection requirements must be embedded in:
a. outsourcing and third-party risk management policies;
b. information and communication technology (ICT) frameworks;
c. business continuity and disaster recovery arrangements; and
d. operational resilience frameworks.

5.44 In determining the location of data, licensees must assess risks associated with:
a. storage or processing of data in foreign jurisdictions;
b. use of cloud or distributed infrastructure; and
c. reliance on shared or multi-tenant environments.

5.45 In assessing data location risks, licensees must consider:
a. legal and regulatory frameworks in the host jurisdiction;
b. potential restrictions on data access, transfer, or repatriation;
c. the ability of the licensee and the Supervisor to access data in a timely manner; and
d. risks to data confidentiality, integrity, and availability.

5.46 The Supervisor may require licensees to restrict or avoid processing data in certain jurisdictions or implement additional safeguards where equivalent levels of data protection cannot be assured.

5.47 Licensees must implement robust data protection measures covering all stages of the data lifecycle, including data in transit, data in memory, and data at rest.

5.48 Regardless of the nature and materiality of the arrangement, security controls must include, at a minimum:
a. secure configuration and system management, including cloud configurations;
b. encryption and secure cryptographic key management;
c. identity and access management, including controls for privileged users;
d. monitoring and mitigation of insider threats;
e. logging and audit trails for data access and system activity;
f. incident detection, response, and reporting mechanisms;
g. data loss prevention and recovery capabilities;
h. logical segregation of data in shared environments;
i. secure network architecture, including firewalls and intrusion detection systems;
j. ongoing training of personnel handling sensitive data;

k. continuous monitoring and independent assurance of service provider controls;
l. investigation and remediation of data security incidents; and
m. secure deletion or destruction of data upon termination of the arrangement.

5.49 Where material risks are identified, the Supervisor may require a licensee to:
a. conduct independent security assessments; or
b. provide third-party audit reports or certifications demonstrating the effectiveness of security controls.

5.50 Where encryption is used, licensees must ensure that:
a. encryption methods are robust and aligned with recognised industry standards;
b. cryptographic keys are securely generated, stored, and managed; and
c. access to encrypted data is appropriately controlled.

5.51 Where licensees engage standardised service providers (including large cloud providers), and the provider does not offer fully customisable controls, the licensee must:
a. assess whether the provider's baseline controls meet regulatory and operational requirements; and
b. ensure that such controls are at least equivalent to, or more robust than, those implemented internally.

(D) Business Resilience, Continuity, Disaster Recovery and Exit Plans

This section sets out the Supervisor's expectations for licensees to establish and maintain robust frameworks for resilience, continuity, and exit planning, covering both internal operations and third-party arrangements. These frameworks must protect proprietary and client-related data, ensure the continuity of important business services, and enable the licensee to recover or transition operations in the event of disruption.

Scope and Objective

5.52 Licensees must establish and maintain robust frameworks for business resilience, business continuity, disaster recovery, and exit planning in respect of all material outsourcing and critical third-party arrangements. These frameworks must ensure that the licensee is able to:
a. protect proprietary, confidential, and customer data;
b. maintain the continuity of important business services within established impact tolerances; and
c. recover, transfer, or exit outsourced services or other third-party arrangements in an orderly manner in the event of disruption, failure, or termination.

Business Continuity and Contingency Arrangements

5.53 Licensees must ensure that all material outsourcing agreements contain detailed and enforceable provisions addressing:

a. business continuity and contingency arrangements;
b. service provider responsibilities during disruptions, including cyber incidents, system failures, natural disasters, and operational outages; and
c. orderly transfer of services to the licensee or an alternate provider in the event of failure, insolvency, or termination of the service provider.

Such arrangements must ensure continuity without undue disruption, legal impediment, or any unreasonable action.

5.54 Licensees must develop and maintain a documented contingency plan for each material outsourcing arrangement. At a minimum, such plans must address:

a. the adequacy of the service provider's business continuity and disaster recovery capabilities;
b. coordination between the licensee's and service provider's continuity, recovery, and crisis management arrangements; and
c. internal escalation, response, and recovery procedures in the event of service disruption, degradation, or failure

5.55 All material outsourcing arrangements must be incorporated into the licensee's:

a. business continuity planning framework;
b. disaster recovery framework; and
c. operational resilience framework.

5.56 Licensees must ensure that service providers maintain robust information security, cyber resilience, and disaster recovery programmes appropriate to the nature, scale, and criticality of the outsourced service.

5.57 Outsourcing agreements must require service providers to:

a. maintain minimum information security standards appropriate to the outsourced service;
b. implement and maintain effective cybersecurity controls across all systems and platforms used in service delivery;
c. conduct periodic internal and independent testing of cybersecurity and resilience controls;
d. maintain data backup, restoration, and disaster recovery capabilities appropriate to the service;
e. apply equivalent security and resilience standards to subcontractors and dependent technologies, including open-source components;
f. conduct periodic resilience testing under severe but plausible disruption scenarios; and
g. align cybersecurity controls with recognised international standards and frameworks.

5.58 Licensees must ensure that service providers are contractually required to notify the licensee promptly of being aware of any material operational or security incident affecting the outsourced or the third-party service within a prompt timeline specified in the contract. Such notification must include, at a minimum:
   a. the nature and scope of the incident;
   b. the date and time of occurrence and detection;
   c. the systems, services, or data affected;
   d. immediate containment and remediation actions taken; and
   e. measures implemented to prevent recurrence.

5.59 Service providers must test backup, recovery, and restoration arrangements at least annually, or more frequently where warranted by the nature, criticality, or risk profile of the service. The results of such testing must be made available to the licensee and material deficiencies must be remediated promptly.

5.60 A licensee must obtain the prior non-objection of the Supervisor before entering into any outsourcing or third-party arrangement involving:
   a. a cross-border disaster recovery site; or
   b. a shared or multi-tenant disaster recovery environment supporting a material outsourced service.

5.61 For the purposes of paragraph 5.60:
   a. a cross-border disaster recovery site means any disaster recovery, backup, failover, or recovery infrastructure located outside Jamaica and relied upon to support the continuity, recovery, or restoration of systems, data, operations, or important business services; and
   b. a shared or multi-tenant disaster recovery environment means any disaster recovery, backup, failover, or recovery environment that is shared with, or used concurrently by, multiple customers, institutions, or tenants and is not dedicated exclusively to the licensee.

5.62 A licensee must not enter into, implement, or become operationally reliant upon an arrangement referred to in paragraph 5.60 unless the Supervisor has provided its prior non-objection.

5.63 In seeking the non-objection of the Supervisor under paragraph 5.60, a licensee must provide sufficient information to enable supervisory assessment of the arrangement, including, where applicable:
   a. the nature, scope, and materiality of the outsourced service supported by the arrangement;
   b. the jurisdiction in which the disaster recovery site or environment is located;
   c. the legal, regulatory, operational, and geopolitical risks associated with that jurisdiction;
   d. the recovery architecture, including recovery time objectives, recovery point objectives, and service dependencies;

e. the extent to which the recovery environment is shared, including any resource contention, concentration, or capacity constraints;
f. segregation, resilience, security, and access controls;
g. business continuity, contingency, and failover arrangements;
h. testing frequency, testing outcomes, and evidence of recovery capability;
i. contractual protections, including access, audit, notification, and termination rights; and
j. any other information the Supervisor may require.

5.64 A licensee must demonstrate, to the satisfaction of the Supervisor, that the arrangement will not impair the licensee's ability to maintain operational resilience, recover important business services within established impact tolerances, or comply with applicable legal, regulatory, and supervisory obligations.

5.65 A licensee must ensure that any arrangement referred to in paragraph 5.60 is subject to enhanced due diligence, heightened oversight, and periodic review commensurate with the nature, complexity, and risk of the arrangement.

5.66 The Supervisor may impose conditions, restrictions, or additional supervisory requirements as part of its non-objection where it considers this necessary to address heightened operational, concentration, legal, data, or systemic risk.

5.67 Licensees must ensure that business continuity and disaster recovery arrangements for all material outsourcing and other third-party arrangements are designed to support the continued delivery of important business services within established impact tolerances.

5.68 For each material outsourcing and third-party arrangement, licensees must maintain a documented Business Continuity Plan (BCP) that is proportionate to the materiality and criticality of the outsourced service. The BCP must be scalable to severe but plausible disruption scenarios and must be subject to periodic testing.

5.69 All material outsourcing arrangements must be subject to joint business continuity and disaster recovery testing involving both the licensee and the service provider at least annually, where applicable.

5.70 Licensees must develop and maintain a documented exit strategy for each material outsourcing and other third-party arrangement. Exit strategies must distinguish between:
a. non-stressed exits, including contract expiration, strategic change, or voluntary migration; and
b. stressed exits, including provider failure, insolvency, cyber disruption, legal impediment, or another severe operational event.

5.71 Exit strategies must, at a minimum:

a. identify viable alternative service arrangements, including transfer to another provider or repatriation in-house;
b. define the roles, responsibilities, decision points, and escalation procedures for executing the exit;
c. identify staffing, financial, technical, and operational resources required to execute the exit;
d. ensure continuity of important business services during transition; and
e. ensure continued compliance with all legal and regulatory obligations during the transition period.

5.72 Licensees must take reasonable steps to maintain exit readiness, including:

a. maintaining current data portability arrangements;
b. assessing alternate provider readiness;
c. ensuring interoperability and recoverability of systems and data; and
d. maintaining contractual provisions necessary to support orderly transition.

5.73 Licensees must develop, and document stressed exit strategies for all material outsourcing arrangements and must, where feasible, test such strategies periodically. The objective of stressed exit planning is to ensure continued service delivery under severe but plausible disruption. Stressed exit strategies may include:

a. transition of the outsourced activity to an alternative provider;
b. repatriation of services, systems, or data in-house;
c. temporary bridging arrangements;
d. contractual continuation or transitional support arrangements; and
e. access to escrow arrangements, including source code, documentation, or infrastructure, where appropriate.

5.74 Licensees must periodically test exit strategies in a manner proportionate to the materiality and risk of the arrangement. Testing may include:

a. validation of backup or alternate service capabilities;
b. data reconciliation and migration testing;
c. simulation of provider disruption scenarios; and
d. operational testing of transition procedures.

5.75 For material cloud outsourcing arrangements, licensees must assess resilience requirements and implement appropriate safeguards, which may include:

a. geographically distributed data centres;
b. redundant infrastructure across availability zones or regions;
c. hybrid or multi-cloud configurations;
d. alternate providers or fallback arrangements; and
e. on-premises recovery capabilities, where appropriate.

5.76 In determining resilience measures, licensees must apply a proportionate approach, having regard to:

a. the size and complexity of the licensee;
b. the materiality and criticality of the outsourced service; and
c. the operational and financial consequences of disruption.

Governance of Continuity and Exit Planning

5.77 Continuity and exit planning must commence at the pre-outsourcing stage and must include:
a. identification of viable alternatives;
b. estimation of transition time, cost, and resource requirements; and
c. definition of triggers, thresholds, and escalation criteria for recovery or exit.

5.78 Licensees must clearly assign responsibility for the development, testing, maintenance, and activation of continuity and exit plans. Responsibilities must include appropriate involvement of:
a. relevant business units;
b. risk management and compliance;
c. technology and operations; and
d. senior management.

5.79 Licensees must designate clear approval and activation authority for continuity and exit plans. Plans must define measurable thresholds, including:
a. maximum allowable downtime;
b. minimum service functionality levels;
c. financial and operational thresholds; and
d. impact tolerance limits.

5.80 Unless otherwise expressly stated in this paragraph, the exit-strategy requirements set out in paragraphs 5.70 to 5.79 apply equally to critical or material services outsourced outside Jamaica. In addition to those requirements, an offshore exit strategy must be tested periodically, and no less than once every two years.

5.81 Offshore exit strategies must be approved by the Board of Directors, or a delegated Board committee, and must be made available to the Supervisor upon request.

5.82 Licensees must review and update continuity and exit plans periodically to reflect:
a. lessons learned from testing or incidents;
b. changes in provider capabilities or operating models;
c. changes in the licensee's business model or risk profile; and
d. new technological, geographic, or operational alternatives.

5.83 Licensees must identify and mitigate operational risks arising from the testing of continuity and exit arrangements, including risks relating to:
a. data exposure;

b. service disruption;
c. control failure; and
d. unintended operational impacts.

(E) Access, Audit, and Information Rights

The Supervisor expects licensees to ensure that the Supervisor, its appointed auditors, and the licensee itself can promptly obtain, upon request, all information relevant to contractual compliance and/or regulatory oversight for outsourced tasks. This should include, where necessary, access to data, IT systems, premises, and personnel of service providers involved in the outsourced or third-party arrangements.

Scope and Objective

5.84 Licensees must ensure that the Supervisor and any authorised representatives can obtain, promptly upon request, all information necessary to support:
a. effective supervision and regulatory oversight;
b. monitoring of contractual compliance;
c. ongoing risk management and assurance; and
d. recovery, resolution, and operational resilience planning.

5.85 All outsourcing and third-party agreements must grant the licensee, the Supervisor, and their authorised representatives sufficient rights of access to obtain information necessary to:
a. verify compliance with contractual, legal, regulatory, and supervisory obligations;
b. support effective oversight and risk management of the arrangement;
c. assess operational resilience, business continuity, and security controls; and
d. support supervisory, recovery, or resolution actions where necessary.

5.86 For the purposes of paragraph 5.85, access rights must, where relevant, extend to:
a. data, records, systems, applications, networks, premises, personnel, and supporting infrastructure used in delivering the outsourced or third-party service;
b. internal policies, procedures, and control frameworks relevant to the outsourced activity, including those relating to data governance, information security, and operational resilience;
c. results of relevant internal testing, vulnerability assessments, penetration testing, and control reviews;
d. corporate, ownership, financial, and governance information relevant to the service provider's capacity and risk profile; and
e. relevant premises, personnel, and external assurance providers of the service provider.

5.87 A licensee must not regard contractual access, information, and audit rights as sufficient solely because such rights are documented in the outsourcing or third-party agreement. A licensee must ensure that such rights are capable of being

exercised in practice and are exercised periodically and effectively, in a manner proportionate to the nature, materiality, and risk profile of the arrangement, to obtain meaningful assurance that the service provider:

a. performs the outsourced or third-party service in accordance with contractual requirements and agreed service levels;
b. complies with applicable legal, regulatory, and supervisory obligations;
c. operates in a manner consistent with the licensee's risk management expectations and internal control requirements; and
d. maintains appropriate operational resilience, including incident response, business continuity, and recovery capabilities.

5.88 The exercise of access, information, and audit rights under paragraph 5.87 may include, where appropriate:

a. reviewing records, reports, control evidence, and other relevant documentation;
b. assessing independent assurance reports, certifications, audit findings, and remediation actions;
c. validating the effectiveness of controls, service performance, and compliance with contractual obligations;
d. testing incident management, business continuity, disaster recovery, and resilience capabilities;
e. assessing the oversight and management of subcontractors or other dependent third parties;
f. conducting targeted reviews, thematic assessments, or control testing; and
g. exercising direct audit, inspection, or access rights, whether remotely or on-site.

5.89 The frequency, scope, and depth of such oversight must be commensurate with the nature, scale, complexity, materiality, and risk of the arrangement.

5.90 For material or higher-risk arrangements, particularly those supporting important business services, sensitive data, regulatory obligations, or critical operations, a licensee must apply enhanced oversight and more substantive assurance measures sufficient to identify, escalate, and remediate deficiencies in a timely manner.

5.91 A licensee must maintain adequate records evidencing the exercise of access, information, and audit rights, including the scope of reviews undertaken, issues identified, actions required, and remediation outcomes.

5.92 At a minimum, outsourcing and third-party agreements must provide the licensee with the right to:

a. conduct reviews, assessments, and audits directly or through qualified independent assessors;
b. obtain and review internal and external audit reports relevant to the outsourced or third-party service;

c. require timely remediation of control weaknesses, contractual breaches, or legal and regulatory deficiencies; and
d. verify that confidentiality, integrity, and security controls remain effective.

5.93 Outsourcing and third-party agreements must preserve the rights of the Supervisor to:
a. request or require independent audits, reviews, or examinations of outsourced or third-party services;
b. obtain internal and external audit reports relevant to the outsourced or third-party arrangement;
c. access books, records, systems, documentation, and supporting information maintained by the licensee or the service provider;
d. access relevant premises and personnel where necessary for supervisory purposes; and
e. verify that outsourcing and third-party arrangements do not impair effective supervision, recovery planning, or resolution planning and implementation.

5.94 Licensees must conduct periodic audits or assurance reviews of outsourced and material third-party arrangements to assess:
a. adequacy of internal controls;
b. compliance with contractual obligations;
c. compliance with applicable legal and regulatory requirements; and
d. the effectiveness of operational resilience, business continuity, and security controls.

5.95 Audit and assurance activities may include:
a. onsite audits conducted by the licensee or its appointed assessors;
b. offsite reviews, including desk-based assessments;
c. independent third-party assurance reports;
d. pooled audits, where appropriate; and
e. certifications or attestations supported by adequate testing and verification.

5.96 Where licensees rely on third-party certifications, attestations, or assurance reports, licensees must assess whether such reports:
a. are sufficiently comprehensive in scope to address relevant systems, controls, and services;
b. provide timely and current assurance over the control environment;
c. are prepared by suitably qualified, competent, and independent professionals; and
d. include sufficient testing, validation, and evidence consistent with recognised industry standards.

5.97 Reliance on third-party reports, certifications, or pooled audit arrangements does not remove the obligation of the licensee to retain and exercise the contractual right to:
a. obtain additional information;

b. request supplementary assurance; and
c. conduct direct or on-site audits where warranted.

5.98 Where pooled audits are used, the licensee remains individually responsible for:
a. assessing the adequacy and relevance of the pooled audit findings; and
b. taking appropriate action to address any risks, deficiencies, or control weaknesses identified.

5.99 Outsourcing and third-party agreements must include provisions ensuring that, following termination of the arrangement:
a. the licensee and the Supervisor retain continued access to books, records, and information relevant to the outsourced or third-party service;
b. data, records, and documentation are transferred in accordance with exit and wind-down arrangements;
c. records are not withheld, destroyed, or rendered inaccessible, including in the event of fee disputes, insolvency, or litigation; and
d. data retention and disposal practices remain consistent with applicable legal, regulatory, and supervisory requirements.

(F) Confidentiality

Scope and Objective

5.100 Licensees must take all reasonable and appropriate measures to ensure that service providers protect the confidentiality of information relating to the licensee, its customers, and its operations. Confidential information must be protected against intentional, accidental, unlawful, or unauthorised access, use, disclosure, alteration, loss, or destruction, whether in physical, electronic, or other form. These requirements apply to all outsourcing and third-party arrangements involving access to confidential, proprietary, customer, transactional, or other sensitive information.

General Confidentiality Requirements

5.101 At a minimum, outsourcing and third-party agreements must:
a. prohibit the service provider, its employees, agents, and subcontractors from accessing, using, or disclosing confidential information except to the extent strictly necessary to perform the contracted service;
b. impose equivalent confidentiality obligations on all subcontractors, agents, and other dependent service providers engaged in the delivery of the service; and
c. require the secure return, disposal, deletion, or destruction of confidential information upon termination of the arrangement, subject to applicable legal and regulatory record retention requirements.

5.102 Licensees remain fully responsible for ensuring that confidential information shared with, accessed by, or processed by a service provider is protected in accordance with:

a. applicable legal and regulatory requirements; and
b. the licensee's own confidentiality, information security, and data governance obligations.

The use of a third-party service provider does not transfer responsibility for the protection of confidential information.

5.103 Licensees must ensure that service providers implement effective, proportionate, and risk-based measures to safeguard confidential information against unauthorised access, disclosure, misuse, loss, or compromise. Such measures must take into account:

a. the nature, sensitivity, and criticality of the information;
b. the materiality and risk profile of the arrangement; and
c. applicable legal and regulatory obligations, including but not limited to section 134 of the Banking Services Act and the relevant provisions of the Data Protection Act.

5.104 Licensees must identify and assess confidentiality, privacy, and disclosure risks as part of the due diligence process for all outsourcing and third-party arrangements. Such assessment must consider:

a. the type and sensitivity of information involved;
b. the service provider's access to customer, proprietary, or other information;
c. the adequacy of the service provider's confidentiality and security controls; and
d. risks arising from subcontracting, cross-border transfers, or shared infrastructure.

5.105 Outsourcing and third-party agreements must include appropriate contractual provisions to ensure:

a. confidentiality of information;
b. lawful and secure processing of information;
c. appropriate segregation and protection of customer and proprietary information; and
d. compliance with all legal, regulatory, and supervisory confidentiality obligations.

5.106 The transfer of customer information by a licensee to a service provider must:

a. be lawful and conducted in accordance with the Data Protection Act and other applicable legal requirements;
b. be limited to what is necessary for the provision of the outsourced or third-party service; and
c. not adversely affect the rights or protections afforded to customers.

5.107 Where customer consent is required by law for the transfer, use, or processing of customer information, licensees must ensure that such consent is obtained lawfully and documented appropriately. Such consent may be obtained:

a. at the commencement of the customer relationship through the relevant customer agreement; or
b. before the proposed transfer, use, or disclosure of the customer's information.

5.108 Licensees must notify the Supervisor without undue delay upon becoming aware of any incident, breach, or adverse development in an outsourcing or third-party arrangement that materially affects:

a. the confidentiality of information;
b. the security or integrity of customer information; or
c. the licensee's compliance with legal or regulatory confidentiality obligations.

This includes unauthorised access to, disclosure of, or loss of confidential information by the service provider or its subcontractors.

5.109 Outsourcing and third-party agreements must include explicit representations, warranties, and undertakings from the service provider, and any subcontractor, confirming that they will comply with:

a. all applicable privacy, confidentiality, and data protection laws in the jurisdictions in which they operate; and
b. all legal, regulatory, and supervisory requirements relevant to the outsourced or third-party service, including those applicable in Jamaica where the service affects the licensee's obligations under Jamaican law.

5.110 Outsourcing and third-party agreements must include provisions allowing the licensee to terminate the arrangement where the service provider, or any subcontractor:

a. commits a material breach of confidentiality, privacy, or data protection obligations;
b. fails to remediate such breach within a reasonable period; or
c. otherwise exposes the licensee to material legal, regulatory, operational, or reputational risk.

SECTION 6: CLOUD COMPUTING

Scope and Application

6.1. This section sets out additional requirements and supervisory expectations applicable to outsourcing and other third-party arrangements involving cloud computing services. This section must be read together with, and in addition to, all other applicable provisions of this SSP OTPRM.

6.2. Unless otherwise expressly stated in this section, all requirements applicable to outsourcing and third-party arrangements under this SSP OTPRM apply equally to cloud computing arrangements. This section applies only to risks that are specific to, or materially heightened by, the use of cloud computing services.

6.3. For the purposes of this SSP OTPRM, cloud computing refers to a model that enables ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources, including networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction.

6.4. Cloud computing generally comprises:
   a. Essential Characteristics, which include: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.
   b. Deployment Models, which include private cloud, community cloud, public cloud and hybrid cloud.
   c. Service Models, which include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

6.5. In addition to the general risk assessment requirements set out in this SSP OTPRM, licensees must assess risks specific to cloud computing arrangements, including:
   a. concentration risk arising from dependence on a limited number of cloud service providers;
   b. risks arising from shared infrastructure and multi-tenancy, including logical segregation and cross-customer exposure;
   c. operational dependencies on cloud control planes, orchestration layers, and provider-managed infrastructure;
   d. vendor lock-in and constraints on substitutability arising from proprietary tooling, formats, or architectures;
   e. risks affecting portability and interoperability of systems, applications, and data;
   f. jurisdictional fragmentation arising from distributed processing, storage, or backup arrangements across multiple locations; and
   g. limitations on visibility, control, customisation, or assurance arising from standardised cloud operating models.

6.6. In assessing the materiality of a cloud arrangement, licensees must consider, in addition to the general materiality criteria set out in this SSP OTPRM:
   a. whether the cloud arrangement supports an important business service;
   b. the degree of operational dependency on the cloud service provider;
   c. the extent to which disruption of the cloud arrangement may impair the licensee's ability to operate within impact tolerances;
   d. the extent of dependency on provider-specific architecture, tooling, or services; and

e. the substitutability of the cloud service, including the feasibility, cost, and time required to transition to an alternative arrangement.

6.7. Licensees must assess risks arising from the distributed and dynamic nature of cloud data processing, storage, and backup arrangements, including:
   a. the jurisdictions in which data may be stored, processed, transmitted, or replicated;
   b. legal and regulatory constraints affecting data access, transfer, or recoverability across those jurisdictions;
   c. risks arising from data fragmentation across multiple legal or operational environments; and
   d. whether the geographic distribution of data may impair supervision, operational resilience, recovery, or resolution.

6.8. Licensees must assess and manage concentration risk arising from cloud computing arrangements, including risks arising from:
   a. dependence on a single cloud service provider;
   b. concentration in a limited number of cloud service providers across the financial sector, where applicable;
   c. reliance on common infrastructure, geographic regions, or availability zones;
   d. concentration in common provider-managed services, dependencies, or software layers; and
   e. dependence on provider-specific technologies that materially reduce substitutability.

   Where such risks are material, licensees must implement appropriate mitigating measures, including diversification, redundancy, fallback arrangements, or other proportionate safeguards.

6.9. The Supervisor may require enhanced reporting or additional mitigating measures where cloud concentration risks may give rise to sectoral or systemic vulnerabilities.

6.10. Licensees must assess and manage risks affecting the portability and interoperability of systems, applications, configurations, and data in cloud computing arrangements. Licensees must ensure, proportionate to the nature and materiality of the arrangement, that:
   a. data can be extracted in a usable, complete, and industry-standard format;
   b. systems and applications can be migrated, reconfigured, or re-established within an acceptable timeframe;
   c. dependencies on proprietary services, tooling, interfaces, or configurations are identified and managed; and
   d. technical, legal, and operational barriers to portability are identified and mitigated.

6.11. In addition to the operational resilience requirements set out elsewhere in this SSP OTPRM, licensees must assess whether cloud arrangements require additional safeguards to address cloud-specific resilience risks, including:

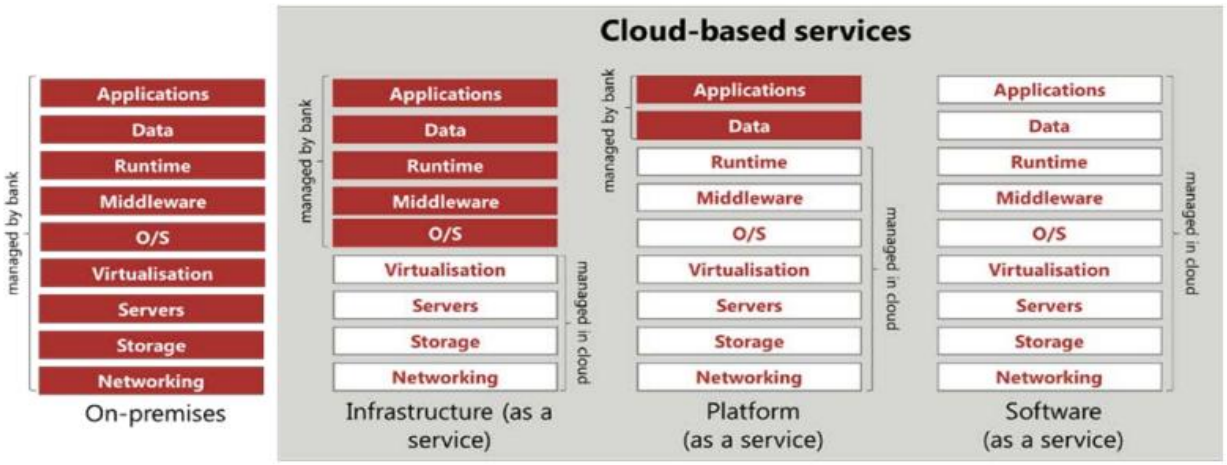
a. concentration of workloads in a single region or availability zone;
b. dependency on cloud control planes or provider-managed orchestration services;
c. resilience of identity and access management dependencies;
d. resilience of provider-managed network, storage, and monitoring layers; and
e. risks arising from shared service failures across multiple customers.

Where appropriate, licensees must implement proportionate safeguards to mitigate such risks, including regional resilience strategies, redundancy across availability zones, workload segmentation, or other technically appropriate resilience measures.

6.12. For all material cloud arrangements, the licensee must provide the Supervisor with the following assessments:

a. the risk assessment;
b. the materiality assessment;
c. the concentration and substitutability assessment; and
d. any other information necessary to assess whether the arrangement is consistent with this SSP OTPRM and the licensee's obligations under applicable law.

6.13. The table below illustrates the distinct features of each service model:



APPENDICES:

APPENDIX I

Application Requirements for Outsourcing Arrangements

11.2. Licensees must obtain the Supervisor's prior written approval before entering into any outsourcing arrangement. This requirement applies equally to:

a. Cloud outsourcing arrangements;

b. Non-cloud outsourcing arrangements;

c. An external third-party service provider; and

d. Intragroup outsourcing arrangements (including domestic or cross-border arrangements with a parent, subsidiary, affiliate, or other related entity).

11.3. Intragroup outsourcing arrangements are not exempt from these requirements. Licensees must ensure that such arrangements:

a. are subject to the same governance, due diligence, and contractual standards as arm's-length outsourcing;

b. address the specific risks associated with related-party dependency, potential conflicts of interest, operational concentration, and cross-border supervisory access, where applicable; and

c. include documented service-level obligations enforceable by the licensee.

Minimum Documentation Requirements

11.4. For the purpose of obtaining such approval, licensees must submit to the Supervisor a complete application containing, at a minimum, the following information and documentation:

a. Governance and Risk Assessment

i. Board-approved business case for the proposed arrangement, including:

1. strategic rationale and expected benefits;
2. analysis of alternatives considered; and
3. justification for the selected service provider.

ii. Materiality and criticality assessment (see Section 3 of this SSP OTPRM), detailing:

1. inherent risks;

2. potential financial, operational, legal, and reputational impacts; and
3. mitigating controls in place.

iii. Due diligence report on the service provider, addressing:

1. reliance on common infrastructure, platforms, or personnel;
2. financial soundness and operational capability;
3. business continuity and disaster recovery capabilities;
4. cross-border operational and regulatory restrictions;
5. legal and regulatory compliance history; and
6. additional consideration for intragroup, service level prioritisation in times of group-wide stress and reliance on other intragroup arrangements.

iv. Written opinions from Legal, Risk, Compliance, or other relevant operational functions on the operational suitability of the arrangement and the legal and supervisory soundness of the arrangement that it meets all applicable legal, regulatory, and supervisory requirements.

v. A formal attestation of compliance with the requirements of this SSP OTPRM.

b. Contractual and Legal Safeguards

i. Draft contractual documentation, including:

1. Service Level Agreements;
2. Non-Disclosure Agreements;
3. confidentiality provisions in compliance with Section 134 of the BSA; and
4. termination and exit management provisions.

ii. For intragroup arrangements, a written service delivery agreement setting out:

1. scope of services, service-level obligations and cost allocation methodology;
2. escalation and dispute-resolution processes; and
3. confirmation of service provision priority during stress events.

iii. Details of any sub-outsourcing arrangements, including but not limited to jurisdiction, regulatory status, and oversight measures.

c. Operational Resilience and Continuity

i. An Operational resilience assessment, including:

1. The contingency plan to maintain service at an acceptable level in the event of disruption.
2. The business continuity and disaster recovery capabilities of the service provider.
3. For offshore or cross-border arrangements, an assessment of:
    a. legal, regulatory, and data-protection framework in the host jurisdiction;
    b. supervisory access restrictions; and
    c. confirmation of the Supervisor's ability to access information and exercise supervisory oversight.

ii. Evidence of the evaluation of the robustness and adequacy of the information and communication framework for the initiative, including:

1. cyber resilience measures;
2. a record of any cyber-related incidents within the last 12 months, together with remedial actions taken;

iii. A data breach management plan, including remedies, communication protocols, roles and responsibilities, and accountability arrangements.

iv. Data-flow mapping (where data or processes cross borders), identifying controls to safeguard confidentiality, integrity, and availability.

d. Performance Monitoring and Oversight

i. Evidence of the licensee's capacity to monitor and oversee the service provider on an ongoing basis.

ii. Proposed KPIs, KRIs, and escalation thresholds for managing the outsourced arrangement.

e. Service Provider Profile

i. Details of the service provider, including:

1. ownership and governance structure including directors and key shareholders;
2. key management and technical personnel;
3. whether subcontractors will be engaged;
4. the jurisdiction in which the service provider and any subcontractors are registered or licensed; and
5. any potential or actual conflicts of interest.

ii. For intragroup arrangements, written group-level commitment to maintain service provision in stress scenarios, including resolution, restructuring, or insolvency of the provider.

f. Cloud-Specific Requirements (where applicable)

i. The cloud service model (IaaS, PaaS, SaaS) and deployment model (public, private, hybrid, community).

ii. Name of the cloud service provider and any parent company.

iii. Description of the activities and data to be outsourced.

iv. Countries where:

1. the service will be performed; and
2. data will be stored or processed.

16. Service commencement date, contract renewal date and last contract renewal date (if applicable), and governing law.

i. Cloud service provider's business continuity arrangements and the licensee's exit strategy.

ii. Evidence of the licensee's capacity to monitor the outsourced cloud activity effectively.

g. Additional Information

i. Any other information that may assist the Supervisor in assessing the outsourcing proposal.

ii. The Supervisor may request further information or clarification at any stage of its assessment. Failure to provide complete and accurate information may delay or prevent the granting of approval.

h. Renewals and Amendments

In the case of contract renewals or amendments, licensees must:

i. notify the Supervisor in writing;

ii. identify any changes to the scope, materiality, or risk profile of the arrangement; and

iii. submit updated due diligence, materiality assessment, and contractual documentation, where applicable.

i. Ongoing Obligations

i. Licensees must maintain an updated Outsourcing Register at institution and group level, containing all outsourcing arrangements (material and non-material) as outlined in Section 6 of this SSP OTPRM.

ii. *The Supervisor reserves the right to request additional information, impose conditions, or refuse an application where it determines that the arrangement poses undue risk to the licensee's safety, soundness, or compliance with supervisory requirements.*

APPENDIX II

Additional Examples of Outsourcing Arrangements

11.5. The Supervisor considers the following, when performed by a third party, as examples of outsourcing arrangements for the purposes of this Standard. This list is illustrative, not exhaustive:

i. *Middle and back-office operations – payroll processing, custody operations, quality control, purchasing.*

ii. *Document processing – cheques, credit card and bill payments, bank statements, corporate payments, customer statement printing.*

iii. *Information systems hosting – software-as-a-service (SaaS), platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS).*

iv. *Information systems management and maintenance – data entry and processing, data centres, facilities management, end-user support, local area networks, help desks, information security operations.*

v. *Human resource management – benefits and compensation administration, staff recruitment and appointments, training and development.*

vi. *Loan administration – loan negotiations, processing, collateral management, collections.*

vii. *Application processing – policies, loan originations, credit cards.*

viii. *Marketing and research – product development, data warehousing and mining, media relations, call centres, telemarketing.*

ix. *Professional services related to regulated activities – risk management, accounting, internal audit, actuarial, compliance.*

x. *Support services – archival and storage of data and records.*

xi. *Customer service relations – customer onboarding, service desks, complaint handling.*

11.6. The Supervisor may determine that other services constitute outsourcing where they meet the definition in Section 2 of this SSP OTPRM.

Mapping of Minimum Application Requirements by type of Outsourcing Arrangement

Requirement	Cloud Outsourcing	Non-Cloud Outsourcing	Intragroup Outsourcing
Board-approved business case	Required	Required	Required
Materiality & criticality assessment	Required (must address cloud-specific risks, e.g., data sovereignty, portability)	Required	Required (must consider group-wide dependencies)
Due diligence report	Must include provider's security certifications, regulatory standing, operational resilience	Must include provider's operational capacity, financial standing	Must include assessment of group entity's capability, independence, and prioritisation in stress events
Legal & compliance opinions	Required – include data protection & cross-border compliance	Required	Required – must confirm enforceability of intragroup agreements
Attestation of compliance with SSP-OTRM	Required	Required	Required
Draft contract, SLA, NDA	Must include cloud-specific audit, access, and exit provisions	Must include audit, access, and exit provisions	Must include binding service obligations, cost-allocation, dispute resolution
Confidentiality clauses (BSA s.134)	Required (covering data in transit, at rest, in use)	Required	Required
Sub-outsourcing arrangements	Must disclose all known sub-providers	Must disclose sub-providers	Must disclose if other group entities will subcontract work
Contingency plan / BCP	Cloud-specific disaster recovery & failover plan	Service continuity plan	Group service continuity & fallback
Cross-border legal assessment	Required (data & service location)	If service performed/stored offshore	If group entity located offshore
Data-flow mapping	Required	Required if handling sensitive customer data	Required if data flows across borders within the group
Performance monitoring capacity	Required – cloud performance KPIs & SLAs	Required – service delivery KPIs & SLAs	Required – intragroup performance metrics
Provider profile	Required – ownership, governance, parent company	Required – ownership, governance	Required – ownership, governance, group structure
Cloud service model & deployment type	Required	N/A	N/A unless group offers cloud services

Business continuity arrangements (provider)	Required – provider's cloud BCP & recovery time	Required – provider's BCP	Required – group BCP
Exit strategy	Required – ability to repatriate or migrate data & services	Required	Required
Ongoing register of outsourcing arrangements	Required	Required	Required
Notification of renewals/amendments	Required	Required	Required

Centralised Register of Outsourcing Arrangements

11.7. Requirement to Maintain a Register:

a. Licensees must maintain and keep up-to-date a Centralised Register of all outsourcing arrangements, whether material or non-material, including intragroup arrangements.

b. The register must be maintained at institution and group level, where applicable, and must be readily available to the Supervisor upon request.

11.8. Purpose:

a. The register will:

i. *Facilitate regulatory oversight;*

ii. *Support risk management and governance of outsourcing arrangements;*

iii. *Enable tracking of materiality changes over time;*

iv. *Provide a consolidated view of the institution's outsourcing landscape.*

11.9. Minimum Information Requirements:

a. The register must contain, at a minimum, the information set out in the template below:

Centralised Register of Outsourcing Arrangements – Template								
Name of Service Provider	Parent Company of Service Provider	Outsourced Service	Materiality of service (material/non-material)	Short Description of Arrangement	Country from which Service is Provided	Applicable Laws Governing the Contract	Expiry/Renewal date of Contract or Outsourcing Agreement	Estimated Annual Spending on Arrangement

11.10. Additional Guidance

a. Materiality – Licensees must indicate whether the outsourcing arrangement is considered material in accordance with the Assessment of Materiality and Criticality requirements under this SSP-OTRM.

b. Short Description – Provide a concise description of the activity or function outsourced, including its scope and purpose.

c. Country from which Service is Provided – Include the primary country or countries where the service provider operates or where the service is delivered from.

d. Applicable Law – Specify the governing law of the outsourcing contract.

e. Expiry/Renewal Date – Indicate the date on which the contract is due to expire or is next scheduled for renewal.

f. Estimated Annual Spend – Record the approximate annual cost of the outsourcing arrangement, including any fixed and variable components.

11.11. Updating the Register

a. The register must be updated immediately upon entering into a new outsourcing arrangement, amending an existing arrangement, renewing, or terminating an arrangement.

b. Materiality assessments must be reviewed annually or upon any significant change to the outsourced activity.