OPERATIONAL RISK MANAGEMENT – MANAGEMENT OF THIRD PARTY ARRANGEMENTS

- OBSERVATIONS AND SUPERVISORY EXPECTATIONS FROM THEMATIC INSPECTIONS

INFORMATION PAPER

August 2022

Monetary Authority of Singapore

TABLE OF CONTENTS

1 Overview

1.1 Effective management of operational risk is fundamental to a financial institution's (FI) holistic risk management framework. The nature and scope of operational risk have evolved over time, given trends such as the large-scale adoption of remote working and the adoption of new technologies. The increasing reliance on third party outsourcing and non-outsourcing arrangements (collectively, "third party arrangements") has also prompted supervisory authorities to update their regulatory approaches.[1] For example, the Financial Stability Board has published the responses to a consultation on "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships", with suggestions to develop global standards on outsourcing and third party risk management, and to adopt consistent definitions and terminology.[2]

1.2 The Monetary Authority of Singapore (MAS) expects FIs to ensure that third parties they rely on for service delivery are subject to adequate governance, risk management and sound internal controls. FIs should assess the risks arising from third party services and implement controls commensurate with the nature and extent of risks. Under MAS' Guidelines on Outsourcing,[3] third party arrangements that are not defined as outsourcing should nevertheless be subject to adequate risk management and sound internal controls.

1.3 MAS' revised Technology Risk Management Guidelines[4] further set out the expectation for FIs to exercise strong oversight of arrangements with third party service providers, to ensure system resilience as well as maintain data confidentiality and integrity. Under MAS' Business Continuity Management Guidelines,[5] FIs are also expected to take into account third party dependencies when engaging third parties to support the delivery of their critical business services.

---

1 Examples of publications by the European Banking Authority, the UK Prudential Regulation Authority, and the US authorities:
- https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements
- https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss
- https://www.occ.gov/news-issuances/news-releases/2021/nr-ia-2021-74.html

2 https://www.fsb.org/2021/06/outsourcing-and-third-party-risk-overview-of-responses-to-the-public-consultation/

3 https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing

4 https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

5 https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management

1.4 Against this backdrop, MAS conducted thematic inspections on the operational risk management (ORM) standards and practices of selected banks over 2020 and 2021,[6] with a focus on third party risk management. The inspections focused on:

(a) **ORM governance and control framework** - management oversight of operational risk, organisation structure and roles of the ORM function, as well as control frameworks and policies.

(b) **Third party risk management** - governance and management oversight of both outsourcing and non-outsourcing arrangements, due diligence conducted during onboarding of service providers, as well as ongoing risk management and monitoring of these arrangements.

1.5 MAS observed that banks have generally established frameworks and processes to provide oversight of operational risk, but implementation effectiveness could be improved. Banks typically set up and integrated their ORM governance function into the overall risk management governance structure. They have also deployed a suite of tools to identify, assess and manage operational risk, and established the three lines of defence (LoD) operating model. Nonetheless, there is scope for banks to improve their analysis and management reporting of operational risk issues. There should be better articulation of key operational risk issues and trends, at both the bank-wide and key business unit levels, to identify emerging risks and determine if additional controls were necessary.

1.6 While banks have implemented a range of operational risk monitoring tools, various aspects need to be improved for these tools to be effective. For example, some banks did not sufficiently consider the non-financial impact of operational risk events or incidents[7] (ORE) in their reporting, and risk and control self-assessments[8] (RCSA). The ORM function of some banks should also provide effective and independent challenge to the risk assessments conducted by the first line of defence (1LoD).

1.7 On third party risk management, banks generally have more established frameworks and processes to manage outsourcing arrangements compared to non-outsourcing arrangements (NOAs). However, some banks fell short of expectations in management oversight and risk reporting of outsourcing activities, as well as due diligence and ongoing monitoring processes. Some examples included:

- Due diligence not completed on a timely basis and lacking the robust involvement of an independent party such as the second line of defence (2LoD);

[6] Inspections were suspended in the second half of 2020 due to the COVID-19 pandemic.

[7] Banks use different terminologies to refer to operational risk events and incidents. These are referred to as “ORE” in this paper.

[8] Banks use different terminologies to refer to their risk and control self-assessments. These are referred to as “RCSA” in this paper.

- Concentration analyses not performed;
- Key risk indicators[9] (KRI) not implemented to monitor outsourcing risk; and
- Intragroup outsourcing arrangements not subject to the relevant controls.

1.8 Banks were at different phases in leveraging technology to manage outsourcing risk. A few banks have yet to use systems, including electronic workflows and system-generated triggers, resulting in largely manual processes that are inefficient and prone to human errors. Such processes did not facilitate effective tracking and monitoring of outsourcing activities.

1.9 For NOAs, some banks did not have robust frameworks to manage such arrangements, or were at a nascent stage of developing controls to manage the associated risks. While arrangements with third party service providers, ecosystem partners and alliances may not constitute outsourcing[10], they can nevertheless expose banks to the risks of contractual non-performance, service or operational disruptions, data breaches, and compliance or conduct issues.

1.10 Banks that were still in the early stage of setting up a third party governance structure largely managed their NOAs in a decentralised manner through the respective business units [11], instead of subjecting them to the consolidated oversight of a management committee. For banks where governance frameworks were already in place, some had limited risk reporting and involvement of the independent control functions.

1.11 MAS also noted good practices in several banks, such as cultivating staff competencies in operational risk management and raising risk awareness through the roll-out of comprehensive accreditation programmes to the 1LoD and 2LoD. Some banks leveraged technology by implementing bank-wide systems and tools to better manage and monitor operational risk in an integrated manner, across all three LoDs. Some banks

---

[9] Banks use different terminologies to refer to their key risk indicators, which are established to assess and monitor exposures to various types of operational risk. Some banks refer to these as key indicators or key risk monitoring indicators. They are referred to as "KRI" collectively in this paper.

[10] Outsourcing arrangements refer to arrangements that fall within the definition specified in MAS' Guidelines on Outsourcing, i.e. an arrangement in which a service provider provides the institution with a service that may currently or potentially be performed by the institution itself and which includes the following characteristics:

(a) the institution is dependent on the service on an ongoing basis; and
(b) the service is integral to the provision of a financial service by the institution or the service is provided to the market by the service provider in the name of the institution.

NOAs refer to arrangements with service providers that fall outside the definition of outsourcing arrangements.

[11] The term "business unit" is meant broadly to include all associated support, corporate and/or shared service functions, for example Finance, Human Resources, and Operations and Technology (Basel Committee on Banking Supervision's Revisions to the Principles for the Sound Management of Operational Risk, March 2021).

also placed greater emphasis on emerging risks such as third party and cyber risks, and managed operational risk through a wider lens of non-financial risk, such as the explicit inclusion of reputational risk[12] and conduct risk.

1.12 This information paper sets out good practices relating to third party risk management that MAS expects to see in banks. All banks are expected to benchmark their practices against this paper. The design of their controls would take into consideration their specific organisational structures, business models, scale of operations and risk profiles. In the paper, the desired outcomes are summarised in the boxes and additional details are provided on certain practices through the use of case examples noted from the inspections.

1.13 While the focus of this paper is on banks, the good practices highlighted should be referenced by all FIs given that they are exposed to similar risks. Non-bank FIs are encouraged to adopt the recommended practices where relevant and appropriate to the materiality of the risks posed by their third party arrangements.

[12] Basel Committee on Banking Supervision defines operational risk in the capital framework as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk but excludes strategic and reputational risk.

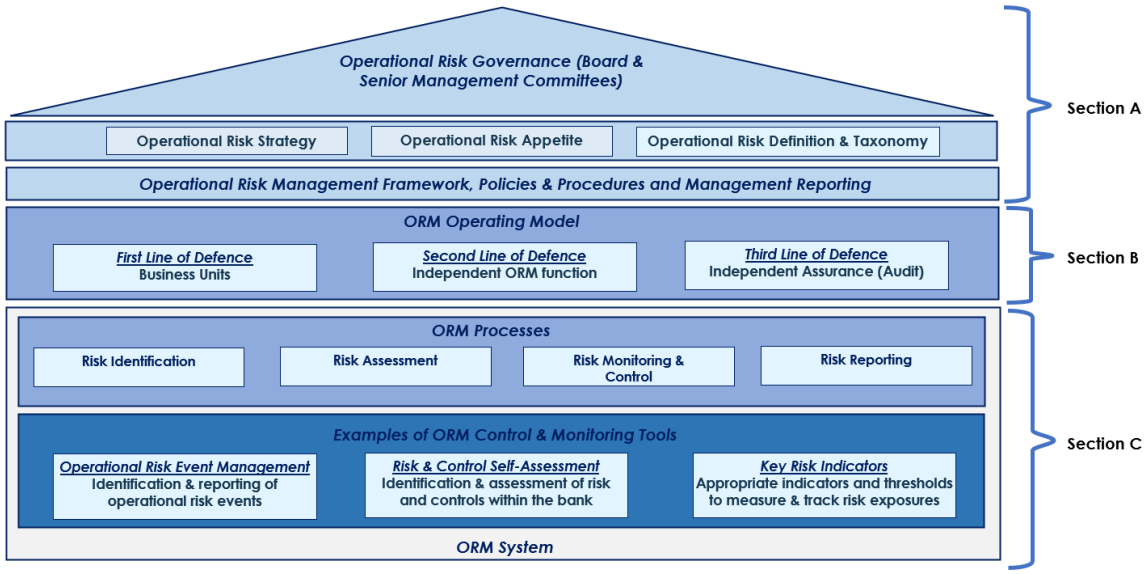
2 Operational Risk Management Governance and Control Framework

2.1 An effective and sound internal governance and control framework is critical in managing operational risk of a bank. A bank's ORM governance function should be fully integrated into its overall risk management governance structure. As part of this framework, the bank should implement sound ORM policies and standards that are appropriate for its business strategies and risk appetite.

2.2 This section on ORM Governance and Control Framework discusses the practices observed at banks in the following areas:

A) Governance and Management Oversight;
B) Operating Model; and
C) Control and Monitoring Processes and Tools.

The diagram below summarises the themes under ORM Governance and Control Framework that are covered in this paper.



A Governance and Management Oversight

2.3 ***Governance structure*** - Banks generally have established governance structures for oversight and monitoring of operational risk, where the Board and senior management (BSM) approve/oversee the setting of operational risk strategy and risk appetite.

2.3.1 The governance for operational risk typically comes under the ambit of a management risk committee/forum, which reports to the executive/board risk committee. With one exception, most banks set up a dedicated ORM committee, chaired by the head of ORM or the Chief Risk Officer, to give operational risk matters due

attention. These committees meet regularly to review operational risk profiles and issues, and discuss emerging concerns and necessary corrective actions.

2.3.2 The lack of a dedicated committee is itself not an issue if adequate attention is accorded to operational risk issues. For the bank without a dedicated operational risk committee, the oversight of operational risk fell within the ambit of an executive risk committee (ERC), which had broader risk management responsibilities. In this case, MAS noted that the operational risk information presented to the ERC could be improved. For example, the information should include detailed analyses of ORE trends and root causes to facilitate more comprehensive assessment of the bank's operational risk profile.

Governance framework for operational risk

Banks establish proper governance structure and framework to facilitate effective and adequate management attention on and oversight of operational risk. As part of this structure and framework, banks develop and implement sound ORM policies and standards that are appropriate for their strategies and risk appetite.

2.4 ***Operational risk appetite*** - Banks have established operational risk appetite and tolerance statements to articulate the level of operational risk they are willing to bear in achieving their strategic objectives and business plans. However, for several banks, the risk appetite was only expressed as a single broad metric, such as the percentage of operating profits or revenues they are willing to accept as losses. A single broad metric might not be sufficient to support meaningful discussions about trade-offs when addressing operational risk. High-level operational risk appetite statements should be translated to more granular metrics and indicators, which are monitored regularly. MAS noted that a few banks had included clear measurable risk indicators (e.g. number of material regulatory breaches and information security risk incidents) within their operational risk appetite framework, with tolerance thresholds that were monitored and reported to management periodically. Threshold breaches would warrant close monitoring and development of action plans to address the concerns.

Setting of operational risk appetite

Banks have a clearly defined operational risk appetite, supported by relevant indicators and thresholds, to articulate the nature, level and types of operational risk that they are willing to assume. The risk appetite is regularly reviewed to ensure it remains appropriate given changes in the business environment and operational set-up of banks.

2.5 ***Operational risk definition*** - Banks have a clear definition of operational risk that is generally in line with that defined by the Basel Committee on Banking Supervision[12] (BCBS). Some banks have adopted a wider lens on operational risk and extended the scope of their operational risk beyond the BCBS definition, for example, by including reputational risk, to have a more holistic approach to managing these risks.

2.6 ***Operational risk taxonomy*** - Banks have established a common taxonomy of operational risk terms to ensure consistency of risk identification and assessment across the three LoDs. Banks have also referenced the BCBS framework on operational loss event categories, and further distinguished operational risk exposures by event types and causes, materiality, and business units where they occur. A few banks have revised and expanded their operational risk taxonomy to give prominence to certain risks, such as cyber and third party risks, in their operational risk identification and assessment processes, given the evolving risk landscape.

Operational risk definition and taxonomy

Banks establish a clear definition of operational risk and common operational risk taxonomy for consistent risk identification, assessment, and management across business units and the three LoDs.

2.7 ***Risk management framework, policies and procedures*** - Banks have maintained policies and standards that support the implementation of their ORM framework. In addition, detailed procedures are established to guide staff on various areas of operational risk control and monitoring, such as ORE handling and reporting, conduct of RCSAs and deployment of KRIs. A few banks are enhancing the way operational risk is being managed, such as by revising their operational risk taxonomy, as part of group initiatives. BSM should exercise robust oversight of the local implementation of group initiatives and provide adequate guidance on new policy requirements and expectations.

2.8 ***Management reporting*** - Banks have instituted regular (e.g. monthly) operational risk reporting by the ORM function to the relevant risk forums and governing committees. Operational risk reporting should provide meaningful insight to BSM and support proactive risk management.

2.8.1 To illustrate, management reporting of some banks included operational risk profiles (such as operational risk loss trends, analyses of top inherent and residual risks, risk hotspots/risk maps and mitigating factors), assessment of OREs (such as analyses by event types, root causes and detailed review of significant OREs) and KRIs (such as significant breaches of KRI thresholds).

2.8.2 However, a few banks did not include an overview and detailed analyses of ORE trends and root causes. Others excluded non-financial events despite their risk impact (e.g. reputation, regulatory and/or customer impact). Not all banks paid sufficient attention to near misses[13], which are nonetheless relevant to identifying potential areas for control enhancements. There was also inadequate guidance on assessing materiality or significance of OREs for escalation to management. Furthermore, the results of RCSAs and KRIs were not adequately analysed to draw out thematic trends and concerns at both bank-wide and key business unit/business segment levels.

Management reporting on operational risk

Banks institute regular and comprehensive reports on analyses of operational risk profiles, assessments of material OREs, as well as areas of risk concerns and trends, to facilitate oversight of the operational risk landscape by Board and senior management.

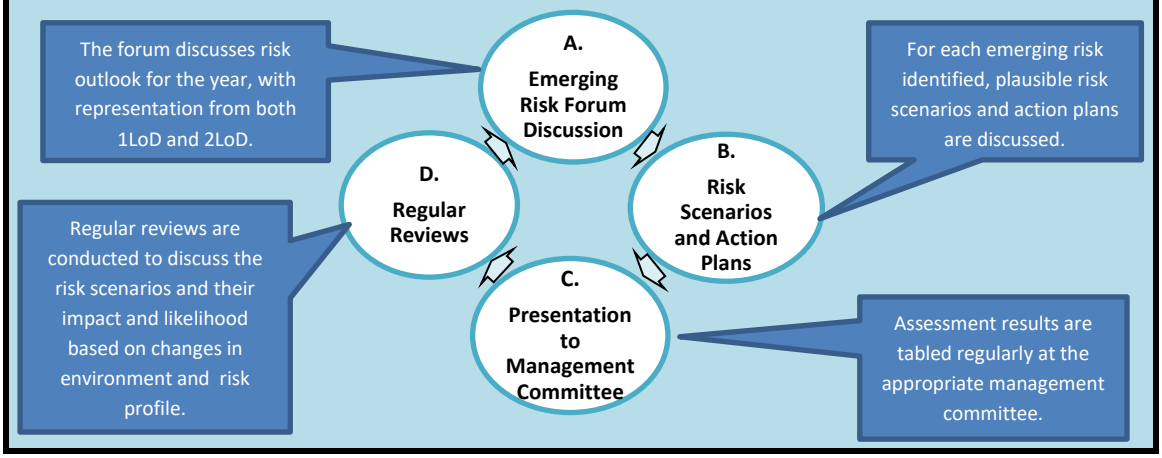
Banks perform operational risk analyses at both the organisation and key business unit/business segment levels. This allows them to systemically ensure that all material risk concerns are adequately surfaced and assessed, as well as better identify root causes and trends of concern.

2.9 ***Monitoring of emerging risk areas*** - Banks' ORM governance and control framework should remain relevant and adequate to respond to or pre-empt emerging risk trends and concerns. Banks generally conduct reviews to identify top and emerging risks to be highlighted to management, but such reviews varied in robustness. At one bank, such reviews were not regularly performed and reported to relevant management forums. Its reviews also did not include assessment of existing controls to address the heightened risks identified and mitigating plans to address any gaps. ***Case Example 1*** illustrates a good practice where a bank has set up structured governance and control processes to proactively identify and evaluate top and emerging risk issues and trends. This process helps the bank to develop pre-emptive measures based on plausible operational risk scenarios. The assessments are regularly performed and presented to appropriate management committee for discussions.

[13] A near miss is generally defined by banks as a type of ORE where some or all established internal controls to mitigate the risk did not operate as intended, but the risk impact has been avoided due to chance, rapid recovery or other external factors.

CASE EXAMPLE 1

Structured governance and control processes are established as part of a proactive and robust approach to identify and monitor top and emerging operational risks faced by the bank.



Monitoring of emerging risks

As the operating environment continues to evolve, banks identify, assess and report on top and emerging risks regularly to management. This provides a forward-looking assessment of operational risk trends and banks' readiness to manage the risks. Banks ensure that their governance and control frameworks remain relevant and adequate to respond to emerging risk trends.

B Operating Model

2.10 ***Three lines of defence model*** - In line with a sound risk governance framework, the three LoDs adopted by banks in their operating model are (i) business units; (ii) independent ORM function; and (iii) independent assurance or audit. MAS noted a good practice where a bank has taken a proactive approach to operationalise a consistent and coordinated three LoD operating model at the organisation level. This involves having clear communication on respective roles and responsibilities of the three LoDs, identifying enhancement areas and ensuring effective training. The efforts are facilitated by a dedicated workgroup that prioritises initiatives and provides updates to management.

2.10.1 To promote operational risk awareness and a strong risk culture within 1LoD, a few banks implemented processes to encourage and incentivise 1LoD staff to self-identify operational risk issues proactively. These self-identified issues are independently tracked by the ORM function, as an indicator of staff risk awareness and effectiveness of training, and reported to management.

2.10.2 ***Case Example 2*** describes a good practice where structured certification programmes and performance assessment framework have been rolled out to uplift staff's operational risk competencies across the organisation.

CASE EXAMPLE 2

Bank implements structured and comprehensive certification programmes to strengthen staff's operational risk competencies and raise the level of proficiency.

Objectives

- To embed ORM into daily business operations, by inculcating strong risk awareness and risk culture across business units.
- To facilitate and guide business units in implementing ORM policies and utilising ORM tools to manage operational risk exposures.

Programme

- E-learning training modules and classroom programmes with certification awarded upon a certain pass rate.
- Annual refresher training and attestations.

Assessment

- Structured ORM-related key performance indicators incorporated in the scorecard of certified personnel.
- ORM function provides inputs on yearly ORM-related performance assessment.

ORM operating model

Banks observe the principle of three LoDs in their operational risk control set-up, and gain assurance that the operating model is effectively implemented to identify and manage operational risk.

While the implementation of the three LoD model can vary across banks, there is clear delineation of roles and responsibilities, and appropriate segregation of roles across the three LoDs. Banks promote operational risk awareness and strong risk culture within the business units as the 1LoD.

2.11 ***ORM function set-up and reporting structure*** - Banks should set up a clear operational risk control structure that is independent and adequately resourced to fulfill its mandate. MAS observed that all banks have set up a dedicated ORM function as a 2LoD. This function typically reports independently to a risk management functional head, such as the Chief Risk Officer. However, the roles and responsibilities, mandate, and size of the ORM function vary across banks. Operating models range from centralised (where the responsibility for managing various operational risk areas reside in a single ORM function) to decentralised (where the management of various operational risk areas comes under

the purview of different functions or subject matter experts i.e., SMEs[14]). Regardless of the model adopted, there should be clarity in terms of accountability, and the ORM function should maintain a comprehensive view of all significant operational risk exposures and issues across the organisation. The ORM function should also be headed by individuals of sufficient seniority and stature, who are vested with adequate authority to effectively perform their duties.

Set-up and mandate of ORM function

Banks' ORM function is independent, adequately resourced and vested with appropriate authority to carry out its responsibilities effectively. The organisational and reporting structure supports ORM's ability to act as an effective challenge to the assessment and management of operational risk by the 1LoD, and contribute to the promotion of operational risk training and risk awareness across the organisation.

The resourcing of ORM function takes into account its mandate, as well as the nature, size, complexity and risk profile of the bank. For banks that adopt a decentralised ORM operating model where multiple units have responsibility for ORM, banks ensure clarity of accountability and effective ORM by these units collectively.

2.12 ***Robustness of ORM function*** – Among other things, the typical responsibilities of the independent ORM function include:

i) Developing operational risk policies and standards within the ORM framework for approval by the relevant Board and management committees;
ii) Assessing and reporting operational risk profiles, issues and trends to the appropriate Board and management committees;
iii) Working with 1LoD to establish guidance on appropriate operational risk monitoring tools and mechanisms;
iv) Providing independent oversight to the implementation of the ORM framework and controls by 1LoD;
v) Reviewing and challenging the risk identification and assessments performed by 1LoD; and
vi) Enhancing operational risk expertise and awareness across the bank.

MAS expects the ORM function to provide effective challenge to the operational risk identification and assessment performed by 1LoD, which is the risk owner. To achieve this, the ORM functions in some banks are directly involved in the ORM processes, for example by being part of the ORE recording and reporting workflow. Others take on the role of

[14] Some common examples of SMEs or functional specialists are in the areas of information security, business continuity management and physical security. Definition and criteria for SMEs may differ from bank to bank.

reviewer, with coverage of all cases or on a sampling basis. Regardless of the approach taken, there should be adequate oversight on the operational risk monitoring and control processes by the ORM function. MAS noted that some ORM functions did not perform sampling checks on RCSAs or had not included all relevant operational risk taxonomies in their reviews. Others did not perform independent reviews to ascertain that non-financial OREs or operational risk issues, including their risk impact and related mitigating action plans, were adequately assessed, monitored and reported.

Robustness of ORM function

Banks' ORM function performs robust and independent review and challenge to the risk identification and evaluation performed by 1LoD, as well as the implementation effectiveness of ORM tools.

C Control and Monitoring Processes and Tools

2.13 ***Operational risk control and monitoring framework and processes*** - Banks have established various ORM tools and mechanisms, such as RCSAs, KRIs and ORE management, to monitor, assess and report on operational risk profiles and trends. These tools also highlight areas of operational risk concerns that banks may face. Banks have established policies and guidance to implement these operational risk control and monitoring tools/mechanisms, including:

i) Risk identification, assessment and monitoring methodology, criteria and process;
ii) Handling and management of OREs;
iii) Conduct, monitoring and approval of risk assessments;
iv) Determination and approval of risk and control indicators;
v) Establishment of thresholds (bank-wide and business unit-level) applicable for each ORM mechanism/tool; and
vi) Reporting and follow-up on key areas of operational risk, exceptions and remediation.

2.13.1 *Operational risk systems/databases* - Banks have put in place systems/databases to facilitate operational risk monitoring and reporting. Several banks have adopted a central core system that houses various modules/applications to support the different operational risk monitoring and management processes. At the time of the inspections, a few banks were in the process of enhancing their system capabilities to allow better linkages between different modules.[15] Banks that rely on fragmented systems/tools or

[15] An example is the management of OREs and RCSAs which could be housed in different modules in the system. Having system interface between the modules could facilitate the relevant OREs to be linked and considered in the respective RCSAs.

manual workarounds in their operational risk monitoring and reporting are more prone to errors, which in turn impacts the quality and timeliness of risk monitoring and reporting. MAS encourages banks to continue investing in system capabilities to achieve more effective operational risk data capture, monitoring and reporting.

2.13.2 *Data quality* - Data quality checks (on accuracy, completeness and timeliness) are generally performed by banks. MAS noted a particularly proactive approach where system-generated reports that flag data discrepancies or exceptions in operational risk processes, including data collection and risk assessment, are independently reviewed to ensure that issues are addressed. Examples of issues flagged by this process included erroneous mapping of risk types to OREs, discrepancies between ORE data and data on their financial impact, as well as omission of mitigating action plans for high risk issues or areas. Regular attestations are also required from the data-generating units.

2.13.3 *Setting appropriate thresholds* - MAS noted instances where global thresholds were used to determine the impact rating of OREs, or whether an event required escalation or should be considered in control assessments, without adequate consideration of local operating environment. These thresholds might not be appropriate or meaningful in the context of the Singapore operations, where the size, scale and operational risk profile meaningfully differed from the group.

Operational risk control and monitoring tools

Banks deploy an adequate set of control and monitoring tools/mechanisms to identify, assess and monitor operational risk. There are robust oversight and independent reviews by 2LoD on the effectiveness of the implementation of the tools and mechanisms by 1LoD.

Thresholds used in operational risk monitoring take into consideration the operating environment and risk profile of the Singapore operations. Banks that adopt group thresholds review their appropriateness for the local activities. Thresholds are reviewed periodically to provide assurance on their continued relevance and effectiveness.

2.14 ***ORE management***[16]- Banks generally consider both financial and non-financial OREs, including near misses, in their ORE management and reporting framework. The datasets recorded in the banks' operational risk system typically include event dates (occurrence date, discovery date and recording date), event types and root causes, as well as the financial impact of loss events and risk impact for non-financial events. Such data facilitates banks' evaluation of their risk profile and control effectiveness. However, a few banks narrowly focused their ORE management on financial loss events, omitting

[16] The thematic inspections focused on non-technology related OREs.

significant non-financial ones, in the recording and assessment of operational risk. The ORE dataset was hence inadequate in supporting the performance of comprehensive monitoring and trend analyses of OREs, including their root causes.

2.14.1 *Impact thresholds for ORE management* - Most banks have established thresholds to guide the recording of OREs. These are typically based on loss amount for financial events and risk impact for non-financial ones. A few banks have adopted a more comprehensive approach that requires all OREs to be recorded regardless of the loss amount or risk impact. Additional thresholds are set for management reporting, where OREs of higher risk impact are escalated to BSM. Banks generally require immediate escalation of OREs (same day or within 24 hours) that are of significant risk to the bank.

2.14.2 *Timelines for recording OREs* - Banks usually require OREs to be logged in their ORE systems within three to 10 business days from event discovery date. As part of assessing if potential loss events should be defined and recorded as near misses, similar industry norms of three to 10 business days for loss recovery period[17] are observed. A few banks have taken a more stringent approach by requiring logging of OREs and defining recovery period for near misses to be within the same day or by the next business day. Other banks implemented timelines that were way above industry norms. For example, recovery period for near misses of 45 calendar days was noted, and OREs were required to be logged only 20 calendar days after they were booked in the financial records. Delays were also noted in the financial booking of OREs (of up to six months), and the recording and independent assessment of OREs (of up to 45 days). These practices could result in OREs being reported to management on a delayed basis, or financial losses being recognised late. To instill discipline, some banks have established timelines for closure of OREs in their systems. These timelines are systematically tracked, and late cases reported to management. In addition to recording near misses, one bank had an additional category of "averted" OREs for events that were prevented by existing controls, to enrich its loss trend analysis.

[17] The loss recovery period generally refers to the period within which financial losses from the OREs are fully recovered from date of occurrence or recognition.

Management of OREs

Banks maintain a comprehensive ORE dataset that contains consistent and standardised risk event information, including root causes, to facilitate trend analyses and identification of potential risk hotspots. Such datasets also provide useful inputs to self-assessment of operational risk exposures and control effectiveness.

Banks include both financial and non-financial OREs in the recording and assessment of operational risk, as the latter could also be indicative of control weaknesses and vulnerabilities. Banks establish processes to record, evaluate and report OREs to management in a timely manner.

2.15 ***RCSAs*** - Business units perform RCSAs on a periodic basis, to identify key processes and assess their inherent and residual risks. The process also involves evaluating the design and effectiveness of controls. Banks typically analyse the outcomes of RCSAs from different perspectives, such as by business unit, function, risk taxonomy or process type. Such assessments reflect a point-in-time view of the inherent and residual risks, as well as the mitigating action plans to reduce risks to acceptable levels. Control effectiveness is typically assessed through control testing for specified sampling periods, such as monthly or quarterly.

2.15.1 *Implementation of RCSAs* - MAS noted room for improvement in banks' implementation of RCSAs. Some banks only performed testing and monitoring of control effectiveness and/or the periodic re-assessment of inherent risks for higher risk processes. While it is reasonable in general to adopt a risk-based approach to the assessment of risks and testing of control procedures, banks should also have mechanisms to ensure that the coverage is sufficiently large to gain assurance. To illustrate, the number of processes being tested in one bank only constituted 1% of the population, as the bulk of the processes had medium or low inherent risk. Other observations included the lack of a structured process to determine the impact of non-financial OREs on control effectiveness, and omitting significant OREs in the RCSAs. Such practices could potentially impede the holistic assessment of control effectiveness and the residual operational risk.

2.15.2 *Risk assessment of new initiatives* - The introduction of new processes, or changes to existing processes arising from new initiatives, products or outsourcing arrangements, may impact a bank's operational risk. One bank has a good practice where end-to-end operational risk assessments are performed by 1LoD to assess the operational risk and mitigating controls for new initiatives. Such assessments, which require approval by 2LoD, promote a robust approach to operational risk assessment.

Performance of RCSAs

Banks ensure that RCSA frameworks adequately cover relevant processes. Where banks apply a risk-based approach towards assessing risks or testing of control procedures, there are safeguards to gain assurance that the coverage is sufficient and effective to identify the relevant risks.

2.16 ***KRIs*** - Banks generally have established KRIs and corresponding thresholds at both bank-wide and key business unit/business segment level, to monitor significant risk areas, with breaches reported to BSM. MAS expects banks to have robust controls over the establishment, regular review and monitoring of KRIs. Examples of KRIs include material OREs, regulatory breaches, overdue audit issues and staff turnover. KRIs should be monitored against pre-established thresholds or triggers (e.g. "green", "amber" or "red" statuses), with action plans developed for threshold or trigger breaches. One bank did not require regular reviews of bank-wide KRIs by appropriate function to ensure that they remained appropriate. Another bank relied on regional indicators instead of establishing KRIs and thresholds that were appropriate for the local operations.

Implementation of KRIs

Banks establish and monitor KRIs at both the key business unit/business segment and bank-wide levels. The latter allows banks to identify common themes across units, and provides a comprehensive view of potential risks the banks are facing. This also allows banks to identify areas of operational risk concerns and trends, and formulate mitigation plans.

Banks regularly review the appropriateness and relevance of KRIs, in line with evolving operational risk environment.

3 Third Party Risk Management

3.1 Banks have adopted different governance approaches towards the management of third party risk. Some banks have an integrated governance framework that covers both outsourcing and non-outsourcing arrangements, while others maintain distinct frameworks. Banks' outsourcing risk governance and control frameworks are generally more developed and mature, due in part to longer-standing supervisory expectations. Controls over outsourcing arrangements and NOAs are discussed in this paper under Section A and Section B respectively.

3.2 Banks outsource processes or functions that they typically perform themselves to reap benefits such as cost-savings.[10] Common areas being outsourced by banks include middle- and back-office operations, archival and storage of data and records, and printing services. Banks also enter into arrangements with third parties to collaborate or provide services that do not fall within the definition of outsourcing. These include certain types of arrangements where banks partnered with third parties to provide additional service platforms to customers to drive new business initiatives. The risks introduced by such NOAs may not be any less material than outsourcing arrangements. Banks should not overlook the risks arising from its engagement of third parties, especially if the disruption of these arrangements could impact the delivery of critical services to the bank and/or customers.

A Controls over Outsourcing Arrangements

3.3 This section on controls over outsourcing arrangements describes the practices in:

I) Governance and Management Oversight;
II) Due Diligence (Onboarding and Periodic Reviews); and
III) Ongoing Risk Management and Monitoring.

I) Governance and Management Oversight

3.4 ***Outsourcing governance structure and framework*** - Banks should establish proper governance and management oversight framework to provide BSM with a bank-wide view of outsourcing risk, to ensure that the risk undertaken is in line with the bank's strategies and risk appetite. Most banks have a dedicated management committee to govern outsourcing arrangements, with some delegation of authority to working groups/forums. A few banks have tasked the oversight of outsourcing to an ORM committee, which has a broader mandate. Although a dedicated management committee is not itself required, banks with dedicated outsourcing management committee were

generally observed to accord greater management attention and exercise more effective oversight over outsourcing risk.

3.4.1 *Committee quorum and chairperson* - The outsourcing committee is typically chaired by management personnel that oversees a 2LoD function, such as head of ORM function or Chief Risk Officer. Where the chair is from the 1LoD, mitigating controls are observed, such as requiring the chairperson to abstain from decision-making relating to his/her line business/function. MAS noted cases where the committee quorum did not explicitly require representation from risk management or 2LoD functions. Having representation from 2LoD functions safeguards against situations where risk and control considerations are subordinated to those of business and profit instead of being balanced.

3.4.2 *Approval framework* - MAS expects banks to establish a proper framework and processes for senior management to evaluate the materiality and risks from prospective and existing arrangements. In one bank, the heads of business units were tasked to approve onboarding of service providers. There was no involvement of 2LoD, and senior management/the management committee overseeing operational/outsourcing risk. Other banks required only certain types of outsourcing arrangements to be tabled to or approved by the relevant management forum, which did not facilitate a holistic and comprehensive view of outsourcing risk by management. On existing arrangements, some banks did not apprise the relevant management committee/forum of periodic reviews performed, for purpose of risk oversight by management. As a result, endorsement of outsourcing risk rested largely within the line functions (or 1LoD), and thematic and inter-dependent risk issues across outsourcing arrangements may not be identified and deliberated. While banks may adopt a risk-based approach, the absence of appropriate reporting of new arrangements and periodic reviews of existing ones may impede management's holistic oversight of outsourcing risk undertaken by the bank.

3.4.3 *Approval process* - MAS noted instances where outsourcing arrangements had commenced without obtaining the requisite approvals and completing due diligence. Some of these arrangements were material, and had commenced for extended time periods without being subject to the necessary ongoing monitoring controls. At one bank, poor attendance rates were noted at the outsourcing forum where non-material arrangements were approved and material ones reviewed, which was indicative of the low priority accorded to outsourcing matters. In addition, a few banks did not have a systematic process to track the satisfactory resolution of approval conditions set by the committee/control functions. Banks should tighten the controls surrounding the approval process for outsourcing arrangements, and continually review their effectiveness.

Outsourcing governance structure and framework

Banks establish a proper governance structure and framework for adequate management oversight and attention on risks arising from outsourcing arrangements, to ensure that risks undertaken are in line with the banks' strategies and risk appetite.

In the adoption of a risk-based approach, banks ensure that their approval framework facilitates management's evaluation of the materiality and risks from existing and prospective outsourcing arrangements. Processes that support the evaluation and approval of outsourcing arrangements are sufficiently robust and effective.

3.5 ***Outsourcing risk appetite and risk taxonomy*** - BSM should set a suitable risk appetite to define the extent of risk that the bank is willing to assume from its outsourcing arrangements. Some banks did not have a specific risk appetite statement for outsourcing risk, or had risk appetite statements that were narrowly focused on a single indicator, such as overdue periodic reviews. Such frameworks did not provide adequate guidance to staff on management's view towards outsourcing. A few banks have adopted the good practice of setting out comprehensive outsourcing appetite frameworks. Their frameworks stipulate the types and level of risks that the banks are willing to take, the expectations on service providers and service recipients, as well as the areas for which there is little or no tolerance, for example, data loss or fraud by service providers. These frameworks and the expectations were clearly and consistently communicated to staff.

Setting of appropriate outsourcing risk appetite

Banks establish a suitable strategy and risk appetite to define the nature and extent of risk that they are willing and able to assume from their outsourcing arrangements.

3.6 ***Management reporting*** - Most banks report the risk profiles of outsourcing arrangements to management, which includes non-intragroup vis-à-vis intragroup, material vis-à-vis non-material arrangements, outsourcing arrangements by nature/purpose and whether they involve customer information. At one bank, significant outsourcing risk issues (e.g. regulatory breaches, material control exceptions, prolonged breaches of performance standards by service providers, and unresolved operational incidents) were not reported to the outsourcing committee. This was due in part to the absence of clear guidelines on the reporting of outsourcing matters by 1LoD, and a lack of effective challenge by 2LoD. Banks also perform regular updates to management on outsourcing KRIs. However, inadequacies were noted in this area. A few banks did not have KRIs to cover pertinent aspects, such as service level agreement breaches, while another bank only reported consecutive KRI breaches.

Management reporting on outsourcing

Banks have effective processes in place to enable a comprehensive bank-wide view of risk exposures arising from outsourcing. There is regular reporting to management on outsourcing risk profiles, significant outsourcing issues and KRIs, to facilitate oversight of outsourcing risk landscape, trends and concerns.

II) Due Diligence (Onboarding and Periodic Reviews)

3.7 ***Due diligence requirements*** - Banks have established policies and procedures on the due diligence requirements[18] and checks to be conducted over the life cycle of an outsourcing arrangement from onboarding, to periodic review, to termination. Some banks assign risk ratings to outsourcing arrangements when the service providers are onboarded. This facilitates the application of a risk-based approach as discussed below.

3.7.1 *Adoption of a risk-based approach* - Banks generally adopt a risk-based approach and impose more stringent due diligence requirements on higher risk outsourcing arrangements (e.g. more frequent onsite visits and periodic reviews). For lower risk arrangements, certain assessments may be waived (e.g. financial viability assessments) or performed at reduced frequency (e.g. biennial periodic reviews instead of annual).

3.7.2 *Evaluation process at onboarding* - At onboarding, banks would evaluate a service provider's business reputation and financial strength, as well as its risk management and controls in areas such as physical and information security, business continuity and compliance with applicable rules and regulations. Banks generally involved relevant subject matter experts (SMEs) such as legal, compliance and information technology, to provide assessments on their expertise areas as part of the onboarding due diligence process. For cross-border arrangements involving data sharing, one bank has a dedicated function and workflows to manage the heightened legal and regulatory risks.[19] MAS observed instances where there were large time gaps of up to ten months between the completion of due diligence documentation and the approval/review by SMEs/outsourcing committee. This could result in approvals being granted based on out-dated information.

3.7.3 *Establishment of clear guidance* - A few banks have established clear and comprehensive guidance on due diligence requirements over the life cycle of outsourcing arrangements, as illustrated in ***Case Example 3***. The type of approvals to be obtained,

[18] Due diligence requirements include deliverables or control tasks such as site visits, information security assessments, conduct of service review meetings etc.

[19] The bank applies this control to both outsourcing arrangements and NOAs.

assessments to be performed, due diligence documentation to be completed/furnished, as well as required frequencies, are clearly specified.

CASE EXAMPLE 3

Bank sets out a clear and comprehensive matrix on the approving authorities and due diligence requirements, from onboarding and periodic reviews of outsourcing arrangements to termination.

Examples of Approval and Due Diligence Requirements		Onboarding		Periodic Review				Termination	
		Non-Intragroup	Intragroup	Material		Non-Material		Non-Intragroup	Intragroup
				Non-Intragroup	Intragroup	Non-Intragroup	Intragroup		
Approval	Head of Business Unit	Yes	No	Annual	Annual	Annual	Once every 2 years	Yes	Yes
	Management								
Due Diligence	Due Diligence Review								
	Onsite Visit								
	Independent Audit								
2LoD/SMEs	ORM Review Form								
	Legal Review Form								
	Compliance Review Form								
	IT Review Form								
Performance	Service Performance Report								
Post Implementation Reviews	Post Approval Assessment								
Termination	Termination Checklist								

NB : Responses under first row are for illustrative purpose only.

3.8 ***Materiality and other risk assessments*** - Banks perform various types of risk assessments during onboarding of new arrangements and subsequent reviews.

3.8.1 *Materiality assessments* - Under MAS' Guidelines on Outsourcing, banks are to ascertain the materiality of an arrangement, which includes considerations of the criticality of the outsourcing to business operations and the amount of customer information shared with vendor. Material arrangements are to be subject to more stringent controls and monitoring. Some banks provide good guidance to staff on the factors to consider for purpose of materiality determination, such as financial, regulatory and customer impact. The guidance includes thresholds and illustrations of arrangements that ought to be classified as material. For example, thresholds on regulatory fines, and situations that could attract significant regulatory scrutiny or severe regulatory action such as revocation/suspension of banking activity are articulated to guide staff's materiality assessment of the regulatory impact of an arrangement.

3.8.2 *Other risk assessments* - Some banks require more granular risk assessments to be performed on outsourcing arrangements, where risk ratings are assigned (e.g. on a scale of 1 to 5). The risk assessments take into account the various types of potential risks that the outsourcing may introduce. Banks consider factors such as complexity of the arrangement, type and sensitivity of data involved, reputational impact, and potential

legal and regulatory implications. The risk ratings will impact the pre-contract due diligence requirements and ongoing control tasks to mitigate the associated risks. Some banks also require risk ratings to be performed on specific aspects, such as third party security risk reviews on service providers' information security risk.

3.9 ***Post-implementation reviews*** - Banks are expected to perform comprehensive post-implementation reviews of new outsourcing arrangements after the commencement of services, or when amendments are made to the arrangements. Such reviews consider any significant issues noted following the commencement or revision of the arrangements, and identify risks that may not be evident or foreseen at the pre-contract stage. Some banks did not require second level checks on the quality of the post-implementation reviews performed by the business units. There was also no process to track the timely completion of the reviews, or to escalate any overdue reviews to an appropriate management forum.

3.10 ***Periodic reviews and engagement of SMEs*** - Banks should undertake periodic reviews and re-perform risk assessments of outsourcing arrangements to identify new risks as they arise. Such reviews provide assurance that outsourcing risk management policies and procedures are effectively implemented. MAS noted instances where the periodic review template did not incorporate a number of key components pertaining to the outsourced activity, such as the service provider's business continuity management measures, physical and information security controls, and results of site visits. At one bank, periodic reviews of outsourced service providers also did not consider performance issues. Another bank did not require the engagement of relevant SMEs in the periodic reviews. As the reviews were only signed off by the business unit head, there was no assurance that aspects such as information security controls were adequately reviewed.

3.11 ***Onsite visits to outsourced service providers*** - Most banks have procedures in place for onsite visits.

3.11.1 One bank had established a comprehensive site visit framework to provide guidance on the key areas to be assessed, such as business continuity management, physical security controls, as well as operational controls and processes. The framework detailed the type of checklists to be completed and the parties involved. Risk ratings for each area and an overall site visit rating were assigned.

3.11.2 Banks may adopt a risk-based approach by setting the scenarios or criteria that warrant onsite visits. These could include consecutive breaches of service standards, poor internal audit ratings or the occurrence of incidents that had resulted in major financial/reputational impact to the bank. However, some banks adopted an overly simplistic approach by requiring site visits only for certain types of arrangements, such as

printing services, without considering the risks and impact posed by other service providers.

Due diligence (onboarding and ongoing reviews)

Banks specify clear requirements, and provide comprehensive guidance, on the due diligence and risk assessment processes for the onboarding of new outsourcing arrangements and periodic reviews of existing ones. Such processes are commensurate with the risks involved, where adequate consideration is given to risk factors such as arrangements that involve sharing of customer data. Banks institute the necessary checks and balances to ensure that these requirements and processes are adequately tracked for compliance in a timely manner.

Banks enlist relevant SMEs to determine if the technical elements of risks pertaining to an outsourcing arrangement are adequately considered.

3.12 ***Staff training and competencies*** - Banks should ensure that staff who are responsible for managing outsourcing arrangements and relationships with service providers have the necessary skills to carry out their duties. Some banks have developed structured programmes with tailored role-based training, and require the completion of training modules within a specified time period, as well as annual refreshers. Other banks have instituted certain eligibility criteria (e.g. seniority) for the appointment of staff to manage outsourcing relationships. Individual arrangements may also be tagged to a management staff for higher level accountability. One bank established a structured process to assess the performance of appointed personnel through key performance indicators. Action plans, such as the need for additional training, are raised to close any gaps noted.

Staff competencies in managing outsourcing relationships

Banks ensure that staff appointed for managing outsourcing arrangements are sufficiently trained and have the necessary seniority and competencies to discharge their responsibilities.

III) Ongoing Risk Management and Monitoring

3.13 ***Outsourcing control function*** - Most banks set up a control function to oversee the performance of control tasks such as reviews on outsourcing arrangements and due diligence requirements, as well as reporting of outsourcing risk issues to management. This function typically resides in a 2LoD function (e.g. ORM function) or is set up as a standalone unit that reports into an outsourcing governance role that is independent of the business unit. However, for some banks, this function resided within the 1LoD, which

is not ideal given the potential conflict of interests. Some of the weaknesses discussed earlier under the governance and due diligence sections[20] pointed to a need for this control function to provide stronger oversight on outsourcing activities. For example, some banks commenced outsourcing arrangements without proper due diligence and approval. Significant outsourcing risk issues, including issues involving regulatory breaches, were not escalated to management. In addition, conditions set by approval authorities on outsourcing arrangements and post-implementation reviews were not systematically tracked by independent parties.

Control framework for outsourcing arrangements

Banks establish a structured framework for ongoing monitoring and control of outsourcing arrangements, with adequate involvement of independent parties to provide effective challenge and oversight to business units that originate the outsourcing arrangements.

3.14 ***Ongoing monitoring of service performance and relationships with service providers*** - Banks monitor the service performance and developments at the service providers through regular service review meetings and review of service performance reports. Service providers are also required to notify banks of any breaches in performance standards at agreed timelines, depending on the severity of the breach.

3.14.1 *Monitoring service performance* - To ensure the effectiveness of service review meetings, a few banks have established structured templates to set out the expected outcomes for such meetings. For example, a bank's meeting template has a performance metric dashboard that tracks indicators such as performance reports, audit and risk issues, staff turnover and training. Another bank requires business units to lodge service review related documents, such as review meeting records, service level report and service provider scorecard, at stipulated frequencies.

3.14.2 *Monitoring changes in relationships with service providers* - The risk of an outsourcing arrangement may evolve over time. New developments at the service providers, an increase in volume of the service outsourced, or the addition of sub-contractors may introduce additional risks to the bank. A few banks have implemented structured processes to identify and document such changes. MAS observed a good practice where a bank deploys a system workflow to require business units to identify material changes to the relationships upon renewal or amendment of existing contracts.[21] Another bank uses a detailed checklist to guide business units to identify and document

[20] Section I Governance and Management Oversight and Section II Due Diligence (Onboarding and Periodic Reviews).

[21] This control is applied to both outsourcing arrangements and NOAs.

changes to the organisation, policies, systems, business continuity plans, amongst others, of the service providers. Where there are material changes to the arrangements, due diligence is required to be re-performed.

3.15 ***Outsourcing KRIs and heatmap*** - Banks typically monitor service providers and their arrangements on a bank-wide basis to obtain a holistic view of outsourcing risk.

3.15.1 *KRIs* - Banks commonly implement KRIs to monitor outsourcing related risks. These KRIs are monitored and reported to the relevant committee or management for attention. Examples of KRIs include:

- Number/percentage of service level agreement breaches;
- Overdue remediation of audit findings;
- Outstanding information security reviews; and
- Significant operational losses or "near miss" events occurring at the service providers.

However, the outsourcing KRIs of a few banks were either very limited, or embedded within operational risk indicators that did not address the specific risk areas relating to outsourcing. Consequently, there were inadequate KRIs to flag emerging outsourcing concerns or vulnerabilities. Some banks also excluded intragroup arrangements from the scope of KRIs, even though they constituted a considerable proportion of their outsourced activities.

3.15.2 *Heatmap risk assessment* - MAS observed a good practice where a bank has a heatmap risk assessment framework to map out the inherent risk, control environment and residual risk of its material outsourcing arrangements. The assessments are performed and rated using a four-point scale, namely, "green", "yellow", "amber" and "red". The information is presented to the management regularly, and provides a good overview of the bank's outsourcing risk. Areas of concern, such as poor audit ratings, breaches in service performance and customer's complaints, are considered in the assessment process and necessary mitigating actions taken.

3.16 ***Concentration risk analyses*** - MAS expects banks to establish a framework to regularly monitor and analyse concentration risk to service providers, based on metrics that are relevant to their outsourcing risk profile.

3.16.1 This is important to highlight potential vulnerabilities that arise from over-dependence on specific service providers, and to put in place contingency plans to ensure operational continuity should such service providers experience disruptions.

3.16.2 Concentration analyses are typically performed at two levels. At the individual service provider level, concentration analysis is performed during onboarding to assess if the onboarding would result in excessive reliance on the service provider (e.g. for multiple

types of services or by multiple units within the bank). This is typically subject to periodic reviews. At the bank-wide level, analyses are performed from different perspectives, such as top service providers by contract value or number of service level agreements, or by type of services and functions being outsourced. Some banks did not perform bank-wide concentration analyses, while others only conducted them on an ad-hoc basis. A few banks relied on the concentration risk framework at the regional/global level, without having a good perspective of the risk of the Singapore operations. ***Case Example 4*** shows a bank's concentration risk analyses, that include analyses of various dimensions of geographical concentration to address the risk arising from a significant extent of overseas intragroup outsourcing.

CASE EXAMPLE 4

Bank analyses various aspects of outsourcing concentration risk, and monitors metrics for different types of outsourcing arrangements.

Quarterly updates are provided to management on concentration risk landscape. Analyses are performed on the nature and materiality of outsourced services, business sector involved and geographical location.

Non-intragroup Outsourcing Service Provider	Intragroup Outsourcing Service Provider
Analysis by third parties providing more than one unique service ▪ *By nature of outsourced service* ▪ *By materiality of outsourced service*	*Analysis by geographical location, business sector and type of outsourced services* ▪ *Top operating geographical location* ▪ *Geographical concentration risk by business sector* ▪ *Geographical concentration risk by type of outsourced services*

3.17 ***Use of systems and tools*** - Banks are at different phases of implementing systems for the management of outsourcing arrangements and to alert the responsible units on upcoming monitoring control tasks that are falling due. Some banks use a single system, while others use a suite of systems and tools to capture the different process steps. One bank was in the process of implementing an integrated system to manage the workflows and ongoing monitoring control tasks over the full life cycle of third party arrangements. A few banks relied largely on manual processes and spreadsheets to monitor various control tasks, which could be more susceptible to errors. Such banks should consider investing in systems and tools that support more efficient and effective tracking of deliverables.

3.18 ***Independent audits*** – Banks are expected to ensure that audits and/or expert assessments of its outsourcing arrangements are conducted by parties independent of the unit or function performing the outsourcing arrangement.[22] However, MAS noted situations where the independent audit expectation was fulfilled by reviews performed

[22] Paragraph 5.9 of MAS' Guidelines on Outsourcing.

by the 1LoD function/in-business control personnel. Certain reviews by specific SMEs were also only performed in their capacity as a risk domain expert, hence the scope was too narrow and limited to cover all the relevant potential risks.

3.18.1 One bank had a good practice of adopting a structured set of audit standards as baseline requirements, to ensure that sound audit standards are consistently applied bank-wide. For audit reports that did not meet the established standards, gaps identified would have to be documented and justifications provided if the report was nevertheless assessed to be acceptable for use. External auditors would be engaged in instances if there were gaps in the audit coverage.

3.18.2 Most banks institute risk-based independent audit requirements on their outsourced service providers, for example, by subjecting non-material arrangements to a longer audit cycle.

Ongoing risk monitoring and controls

Banks are proactive in managing relationships with outsourced service providers, and apply more rigorous controls for higher risk arrangements. As the nature, materiality and complexity of outsourcing arrangements may evolve over time, the ongoing monitoring framework should be sufficiently robust to consider and manage such changes.

Banks have adequate tools to monitor outsourcing risk. Significant risk trends identified from KRI and heatmap assessments, concerns (such as overdue remediation of risk/audit issues, service level breaches or overdue periodic reviews), as well as concentration analyses are reported to management.

B Controls over Non-Outsourcing Arrangements

3.19 This section on controls over NOAs describes the practices observed at banks under the following areas in a third party risk management framework:

I) Identification and Risk Categorisation;
II) Governance and Management Oversight; and
III) Due Diligence and Ongoing Monitoring.

I) Identification and Risk Categorisation

3.20 MAS expects banks to establish a robust risk management and control framework to govern third party arrangements that are not defined as outsourcing. The movement restrictions imposed during the COVID-19 pandemic highlighted the importance for banks to understand their third party dependencies better.

3.21 ***Identification of third party dependencies*** - Banks deal with a wide range of third party business partners and service providers. Such relationships could range from provision of professional services such as audit or advisory services (e.g. law firms), to business collaborations where there is sharing of customer data by the bank, or provision of financial services on behalf of the bank. Some arrangements may even involve multiple parties with different roles. As a first step, banks should establish a complete inventory of their third party relationships, so that they have a holistic view of their third party risk.

3.22 ***Risk categorisation of third party dependencies and risk criteria*** - Different NOAs will introduce different risks and the bank's dependence on each arrangement for its day to day operations will vary. Banks should thus critically assess and risk categorise the NOAs to better determine the corresponding due diligence and ongoing monitoring requirements. Examples of assessment criteria used by banks to guide such determination include whether there is sharing of confidential bank or customer information, and/or whether the service provider supports critical functions or presents key risks, such as regulatory and information security risks, to the bank. Regardless of the approach taken, banks should ensure that the framework and criteria used are sufficiently robust to identify all NOAs that pose risks to the banks and subject them to adequate governance and controls.

Risk identification and categorisation of third party dependencies

Banks have a third party risk management and governance framework to manage their non-outsourcing third party dependencies.

Banks identify and inventorise a comprehensive list of NOAs, and categorise them based on their nature and risk characteristics.

Banks establish clear criteria to risk assess their NOAs, so as to determine the governance and due diligence requirements that they should be subject to. Adequate consideration is accorded to risk factors such as arrangements that involve sharing of customer data.

II) Governance and Management Oversight

3.23 ***Governance and risk management framework*** - BSM should subject their NOAs to adequate and risk-proportionate governance, with independent controls to provide oversight. This includes determining an appropriate governance committee where the level of oversight and monitoring is commensurate with the risks posed to the bank. Where a bank has more than a single framework to cover its third party activities,[23] the bank should ensure that taken together, the scope of coverage is sufficiently comprehensive to address all relevant third party risk.

3.23.1 *Implementation of governance structure* - At the time of the thematic inspections, banks were at varying stages of establishing and implementing the governance and risk management frameworks to manage NOAs. Some banks were in the process of setting up their governance structure and mandating the responsible management committee to provide the oversight on NOAs, with the supporting risk management and control processes not fully operationalised yet. Generally, banks have either expanded the mandate of existing outsourcing committees to include NOAs, established third party committees with centralised oversight on both outsourcing arrangements and NOAs, or set up distinct governance structures and committees to oversee outsourcing arrangements and NOAs. Similarly, on risk management frameworks, some banks have a single third party risk management framework for both outsourcing arrangements and NOAs, while others maintain distinct policy frameworks. The different approaches are acceptable, as long as the risks of outsourcing arrangements and NOAs are adequately addressed. For banks that do not yet have a framework to manage NOAs, MAS expects these to be put in place expeditiously.

[23] For example, some banks maintain separate frameworks for ecosystem partnerships, and business partnerships with third parties on provision of digital wallet services.

3.23.2 *Coverage of governance framework* - The third party risk management frameworks of some banks were not comprehensive in their coverage. For example, a few banks excluded certain types of NOAs, such as tie-ups with payment service providers and ecosystem partnerships, even though these arrangements posed potential reputational and/or legal risks (e.g. during times of non-availability of applications/services provided). Another bank applied an overly restrictive criteria in determining the NOAs that would be subject to the due diligence requirements, potentially resulting in a very limited number of NOAs being monitored and risk-managed.

3.23.3 In banks where the governance frameworks were in the process of being implemented or were not sufficiently comprehensive, the NOAs were managed in a decentralised manner by the business units. This meant that they did not have a consistent governance and control framework, and the 2LoD function was not involved even though there could be material risks being posed to the bank.

Implementation of risk management and governance frameworks for NOAs

Banks have a governance committee to exercise oversight of NOAs. Banks also establish risk-appropriate governance and risk management frameworks, including due diligence requirements, to manage risks arising from NOAs in a holistic manner.

3.24 ***Management reporting*** - MAS expects management reporting on third party activities to be adequate, timely and contain appropriate risk information. This is to facilitate a comprehensive view of third party risk trends and concerns by management, so that informed decisions on corrective actions could be taken if required. Some banks have established processes to regularly report on third party risk, such as third party risk profile and KRIs, ranging from monthly to quarterly frequencies. However, in a few banks, there was no regular reporting on key risk aspects such as vendor-related issues, data incidents or performance breaches, with only indicators relating to outstanding control tasks being covered. One bank reported gaps in ongoing monitoring controls with respect to NOAs only to the regional forum, but not to local management. For banks whose governance frameworks were being developed at the time of the inspections, they had yet to establish regular management reporting.

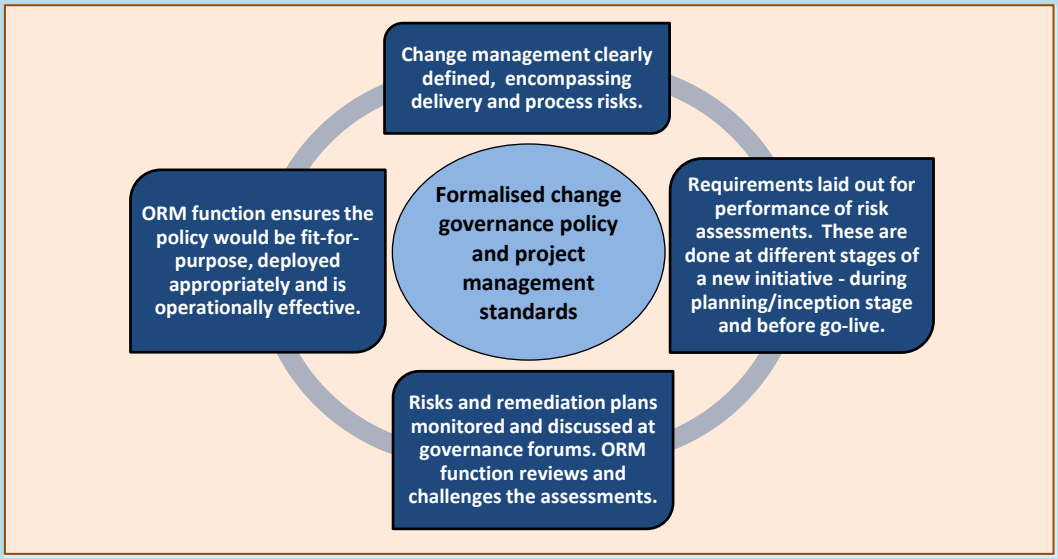
Management reporting on third party risk

Banks ensure adequate management oversight through regular and timely reporting on risk profiles and performance of NOAs. Significant issues such as expired periodic reviews, vendor incidents, performance breaches, and KRI breaches, are regularly reported to the relevant governing forum. An appropriate party (e.g. a 2LoD unit) provides the necessary checks and balances on the reporting process.

3.25 ***Change management*** - New operational risks may be introduced when engaging new NOAs to offer services to customers or entering unfamiliar markets, as such moves may entail changes to existing procedures or systems. If not well managed, the changes could lead to operational lapses or data integrity issues. Banks generally manage the impact of changes arising from onboarding of new NOAs as part of their business-as-usual or new product approval processes. ***Case Example 5*** illustrates a good practice where a bank has a clear change management policy with procedures that provide clarity to staff on what is needed.

CASE EXAMPLE 5

Bank has formalised a set of structured governance and control framework and procedures on change management, with active involvement from independent units.



Change management

Banks have sound change management policies and procedures to manage risks arising from new NOAs. There is clear allocation of roles and responsibilities across the three LoDs with change implementation subject to independent controls and oversight.

III) Due Diligence and Ongoing Monitoring

3.26 Banks should have structured due diligence processes and ongoing monitoring controls that are commensurate with the risk and complexity of the third party relationships. Most banks adopt a risk-based approach where more stringent due diligence requirements and controls, for example more frequent reviews and additional monitoring tasks, are imposed on higher risk NOAs throughout the life cycle of the relationships.

3.27 ***Due diligence processes*** - Banks have generally set out the due diligence processes for onboarding of new NOAs and periodic reviews of existing arrangements. Given that NOAs involve various types of third parties, such as business partners and service providers, banks' due diligence processes should be wide enough to cater to different types of engagements. As part of the due diligence process, banks identify and assess key risks associated with the NOAs, including business reputation, financial strength, risk management, business continuity management and information security of the service providers. For cross-border arrangements involving data sharing, one bank has a dedicated function and workflows to manage the heightened legal and regulatory risks.

3.27.1 *Risk assessment methodologies* – As with the risk assessment for outsourcing arrangements, banks would likewise determine the risk of an NOA, which could include an assessment of the materiality[24] of the arrangement. A few banks use a risk rating scale (e.g. 1 to 5) for each risk element of the NOA (e.g. information security, regulatory compliance) and an overall rating. However, MAS noted that some banks' assessment methodologies did not place a heavier weight on higher risk factors, such as where confidential information is involved, or a critical function is being supported (with the exception of technology-related arrangements). In these banks, NOAs assessed to be "high" risk constituted a low proportion of the banks' NOAs, which could indicate insufficient prudence.

3.27.2 *Execution of contracts* - Banks should enter into contractual agreements with third parties only after the due diligence and risk assessments are duly completed, and any risks identified are adequately addressed or mitigated with action plans. MAS observed instances where some banks executed contracts with business partners/service providers or commenced the arrangements before completing the necessary due diligence and risk assessments. For one bank, remediation actions of obtaining the requisite due diligence approvals were prolonged, taking more than a year.

3.27.3 *Group-wide arrangements* - It is not uncommon for banks to have NOAs providing services to more than one location or office of the banking group. For onboarding and periodic review of such arrangements, banks may leverage the information and outcomes from group-wide risk assessments performed by the banking group/parent company. MAS observed instances of inadequate local involvement as the bank did not take steps to be kept apprised of the outcomes of the group assessment during periodic reviews. MAS expects adequate involvement of the Singapore unit in group assessments to evaluate if there are country-specific requirements that need to be considered, or if there are any changes in the group assessments that may impact local operations. Examples of

[24] As part of assessing the risks of the arrangement, the business unit would need to assess its materiality to the bank. Criteria include whether the bank's business operations or reputation would be materially impacted in the event of service unavailability or any unauthorised access of customer information.

country-specific requirements included compliance with technology risk or business continuity management requirements.

3.28 ***Periodic reviews*** - Banks conducted periodic reviews and re-performed NOA risk assessments using a risk-based approach, where more frequent reviews are performed for higher risk arrangements. MAS noted some instances where such reviews were not robustly performed. For example, periodic reviews did not include a holistic view of service level agreement issues over the period of review to assess if there was deterioration in performance standards. Some reviews were limited to checks on shareholders and directors. In one bank, periodic reviews were not conducted in a timely manner as the business units were solely responsible for tracking the due dates, with no oversight by an independent 2LoD function.

3.29 ***Independent oversight*** - MAS expects banks to have independent oversight of onboarding of new NOAs and periodic reviews, as part of the due diligence processes. Independent oversight is exercised on a few fronts.

3.29.1 *Involvement of SMEs* - SMEs are involved in the risk assessment of NOAs, to ensure proper identification and mitigation of key risk concerns associated with these relationships. SMEs typically review areas such as physical security, information security and business continuity management, before new third parties are onboarded, as well as during periodic reviews, if there are material changes or trigger events. This is important as the outcome of the risk assessments determines the rigor of the due diligence and ongoing monitoring requirements. The extent of SME involvement varied among the banks, with some relying heavily on the business units to determine whether to consult the relevant SMEs. One bank did not have processes to systematically track that conditions imposed by SMEs were met based on agreed timelines.

3.29.2 *Independent checks* - Given the wide scope of NOAs, it is not practical for an independent party to oversee the engagement of each NOA directly. Nonetheless, independent oversight can be exercised through risk-based reviews and checks conducted by an independent party to validate the business units' own assessment. Not all banks have such checks to provide effective challenge to business units on the due diligence and risk assessments performed on NOAs. At other banks, such checks were found to be ineffective or inadequate, leading to control gaps. For example, it was not evident at one bank that the necessary approval on data sharing to ensure compliance with legal and regulatory requirements was obtained prior to commencement of the NOA. In another bank, erroneous entries in third party risk assessments by business units that resulted in inaccurate risk rating and classification of the arrangements were not detected for as long as two years.

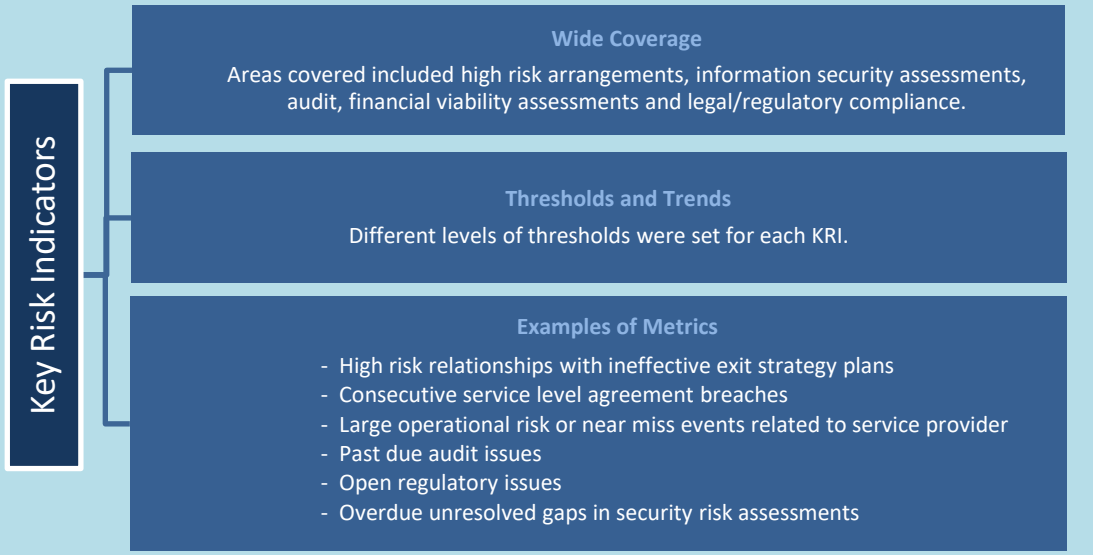
3.30 ***Ongoing monitoring of NOAs*** - Banks are expected to perform ongoing monitoring of the service or performance delivery of NOAs to gain assurance of the adequacy of controls by service providers, and their ability to comply with agreed service levels. The monitoring is exercised through service review meetings with service providers, review of service performance reports, and being notified of performance breaches or incidents. Higher risk NOAs would be subject to more stringent monitoring, such as more frequent service review meetings. However, not all banks establish such requirements or guidance clearly. There were situations where business units had the discretion to determine the frequency of these meetings and the areas to assess. Consequently, the reviews conducted for high risk arrangements were only premised on service level agreement reports received from service providers, without discussions on other relevant risk areas such as material audit issues. Banks should also be cognisant that the risk of NOAs may evolve over time, and re-perform risk assessments as needed. At one bank, risk assessments of affected partnerships were not re-performed despite the occurrence of regulatory changes that constituted a trigger event. As a result, there was a delay in re-classifying several arrangements from "non-material" to "material", and the arrangements were not subject to more stringent due diligence and review requirements.

3.31 ***Third party KRIs*** - MAS expects banks to implement adequate KRIs to monitor the performance of their NOAs, especially the higher risk ones. Some common risk metrics include service level agreement breaches, vendor incidents, regulatory breaches, expired contracts, and overdue reviews/control tasks. A few banks had not established regular KRIs, as their third party risk management frameworks were still being developed at the time of the inspections. One bank had allowed timelines of more than six months before an outstanding control or gap remediation was deemed overdue and considered as a KRI breach. Such undue timelines could impede timely identification of potential risk issues relating to the NOAs. ***Case Example 6*** illustrates a good practice where a bank had a comprehensive set of indicators, which included granular metrics to raise warning signals of heightened risks affecting NOAs. The KRIs are used to actively monitor trigger events or adverse developments at the business partners or suppliers.[25]

[25] This set of indicators also applies to outsourcing arrangements.

CASE EXAMPLE 6

Bank has comprehensive KRIs to monitor third party risk, with granular indicators that serve as warning signals of heightened risks affecting an arrangement.



3.32 ***Third party risk taxonomy and heatmaps/risk scorecards*** - Besides regular reporting to management on third party activities, such as onboarding of new NOAs, third party risk profiles and KRI breaches, it is also useful for banks to have an overall assessment of their third party risk at the organisation level. Some banks include a dedicated third party risk component to its risk taxonomy to facilitate a consolidated view of their third party risk.[26] This third party risk taxonomy covers aspects such as disruption of third party service delivery and oversight risk to provide a holistic view of inherent third party risk and related control effectiveness. ***Case Example 7*** shows a good practice of a risk scorecard that is presented to a management forum regularly. The scorecard provides a snapshot on the overall level of third party risk posed to the bank, as well as risk ratings of key areas of concern.

[26] This includes the risks of both outsourcing arrangements and NOAs.

CASE EXAMPLE 7

Bank has a risk scorecard that provides a holistic view of the overall level of third party risk posed to the organisation.

A. Control Summary		
Overall Rating – Red/Amber/Green		
Examples of Metrics	**Rating (R/A/G)**	**Description#**
Third party related audits	G	*No overdue open audit issues.*
Arrangements commenced without approval	R	*Several arrangements commenced without formal approval.*
Periodic reviews	G	*No overdue periodic review.*
Operational risk events	A	*An incident at service provider occurred that impacted delivery service.*
KRI breaches	A	*Some arrangements with KRI breaches on due diligence.*
B. Key Highlights		*Third party risk profile remains stable. Breaches are within risk thresholds.*
C. Emerging Risks/Changes in Regulatory or Internal Rules		*No major developments.*
D. New High Risk Arrangements		*Onboarding of several high risk arrangements.*

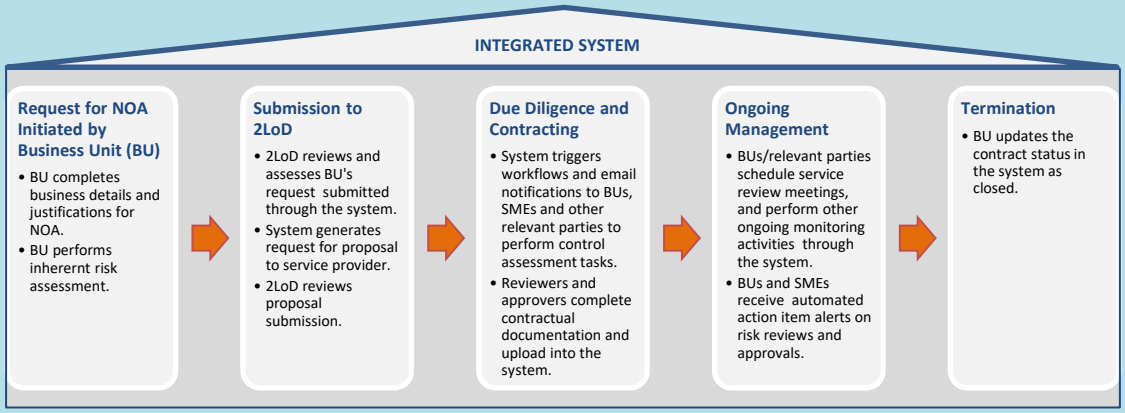
Narrations in the Description column are for illustration purpose only.

3.33 ***System implementation*** - Banks are at different phases of system implementation for managing NOAs. Some rely largely on spreadsheets and manual processes, or are still in the process of automating workflows. Others were more advanced in the use of systems and tools to capture the different third party risk management processes, such as risk assessment, due diligence, and monitoring of control tasks and performance metrics. ***Case Example 8*** describes the implementation of a system at a bank meant to manage the full life cycle of NOAs, including automation of workflows. Banks should consider exploring the use of technology to reduce human errors, enhance efficiency and improve effectiveness of third party risk management.

CASE EXAMPLE 8

Bank implements a system with capabilities to manage various requirements over the life cycle of NOAs, from onboarding, ongoing monitoring to termination.

Integrated modules in the system that enable automated workflows for review and approval of requests for new NOAs, and action item alerts for ongoing monitoring.



Due diligence and ongoing monitoring of NOAs and third party risk

Banks implement risk assessment methodologies for risk rating NOAs that adequately consider higher risk factors, such as sharing of confidential information or providing support to critical functions.

Banks set out clear requirements on due diligence and independent oversight for onboarding of new NOAs and reviews of existing ones, that are commensurate with risks involved. Due diligence considers all relevant stakeholders of the NOAs, including partners and service providers.

Banks implement structured control processes for the ongoing monitoring of NOAs, over the life cycle of the relationships. High risk arrangements necessitate more stringent ongoing monitoring.

Banks deploy adequate risk monitoring tools and mechanisms to manage third party risk. These tools and mechanisms include the setting of a third party risk taxonomy and implementation of appropriate KRIs to facilitate a holistic view on the third party risk of the bank.

4 Conclusion

4.1 The thematic inspections show that banks have room to raise risk management standards in managing third party risk. Banks are generally familiar with outsourcing risk, but some are only beginning to pay attention to risks posed by other service providers such as ecosystem partnerships and business alliances. MAS expects banks to have robust processes to manage their third party arrangements, especially if their business strategy promotes or necessitates the active use of such arrangements. This is important in bolstering their operational resilience.

4.2 The inspected banks have taken, or are taking, remedial actions to improve their frameworks and processes. Banks that are not part of the thematic inspections should benchmark their practices against this paper and take steps to address gaps, if any, in a risk-appropriate manner. As the operational risk that banks are exposed to continues to evolve, they should continually evaluate the effectiveness of their ability to manage this risk.

4.3 Non-bank FIs should also take reference from the paper and implement the recommended practices in a risk-proportionate manner.

Monetary Authority of Singapore