BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Outsourcing

Applicable to−

1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed insurers
5. Licensed takaful operators
6. Prescribed development financial institutions

Issued on: 28 December 2018 BNM/RH/PD 028-93

TABLE OF CONTENTS

PART A OVERVIEW

1 Introduction

1.1 The Malaysian financial landscape has transformed significantly over the last decade, underpinned by a more integrated and globalised environment, rapid technological advances and diverse financing needs. With growing competition and the need to gain greater flexibility to manage business changes, outsourcing is increasingly used as a means of improving operational efficiency, reducing costs and achieving strategic objectives. The ability to leverage expertise within financial groups and harness potential group synergies has also led to financial institutions outsourcing a broader range of internal processes and business functions to their affiliates.

1.2 Increasing digitalisation and advancement in financial technologies have further spurred financial institutions to continuously adapt their business models and processes through outsourcing in order to have access to, and reap the benefits of, these technologies. This has led to growing interest in recent years to use cloud service providers to improve business agility in responding to customer needs and to achieve economies of scale.

1.3 Outsourcing arrangements, if not effectively managed, can increase risk to the financial institution and threaten its safety and soundness. A key concern to regulators is the over-reliance on service providers for activities that are critical to the ongoing operations and safety of financial institutions. Globally, as regulators move towards the implementation of recovery and resolution planning, extensive outsourcing - especially within a complex group structure - poses challenges to the ability of the financial institution to maintain operational continuity of critical functions during recovery and resolution phases.

1.4 The growing number of data-related incidences of breaches in recent years also underscores the importance of instituting strong data security protocols for data of financial institutions that reside in the data centres of service providers. These breaches can undermine the responsibility of financial institutions in safeguarding the confidentiality of customer information, and have had adverse effects on the reputation of financial institutions as custodians of public funds. This, if not managed properly, could ultimately impact public confidence in the financial system.

1.5 The Bank expects that financial institutions will not outsource any activity that would result in the delegation of management oversight and responsibilities, changes the obligations of the financial institution towards its customers, creates undue risks, or impairs the effectiveness and robustness of the financial institution’s internal controls.

1.6 This policy document sets out the scope of arrangements relevant to the outsourcing policy, and the requirements and expectations on financial institutions to maintain appropriate internal governance and outsourcing risk

frameworks, including those relevant to the protection of data confidentiality. The requirements also serve to ensure the Bank's continued ability to carry out effective supervisory oversight over financial institutions in relation to their outsourced activities.

2 Applicability

2.1 This policy document is applicable to financial institutions as defined in paragraph 5.2.

2.2 For a financial institution operating as a foreign branch in Malaysia, the requirements in this policy document shall apply in respect of the Malaysian operations of such a branch with the following modifications:
(a) any reference to the board in this policy document shall refer to the governing body/committee of the foreign branch; and
(b) any reference to senior management in this policy document shall refer to the officers performing a senior management function of the branch.

2.3 The requirements in paragraph 12.1 shall not apply to an outsourcing arrangement entered into by the branches of locally incorporated financial institutions located outside Malaysia in respect of such branch operations.

3 Legal provisions

3.1 This policy document is issued pursuant to−
(a) sections 47(1), 143(1) and 266 of the Financial Services Act 2013 (FSA);
(b) sections 57(1), 155(1) and 277 of the Islamic Financial Services Act 2013 (IFSA); and
(c) sections 41(1), 116(1) and 126 of the Development Financial Institutions Act 2002 (DFIA).

4 Effective date

4.1 This policy document comes into effect on 1 January 2019, save for the transitional arrangements as set out in Part D.

5 Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, IFSA or DFIA, as the case may be, unless otherwise defined in this policy document.

5.2 For the purposes of this policy document−

"S" denotes a standard, an obligation, requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action;

"G" denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted;

"activity" refers to a business or operational function, process or system;

"affiliate", in relation to an entity, refers to any corporation that controls, is controlled by, or is under common control with, a financial institution;

"board" means the board of directors of a financial institution, including a committee of the board where responsibilities of the board as set out in this policy document have been delegated to such a committee;

"customer" refers to any person who uses, has used or may be intending to use[1], any financial service or product including–

(i) a representative of the customer (such as the parents of a minor and authorised representative[2]); and

(ii) a person who has entered or intends to enter into arrangements with a financial institution (such as a guarantor or third party security provider) on account of or for the benefit of a customer;

"customer information" refers to any information relating to the affairs or, in particular, the account, of any particular customer of a financial institution in whatever form including in the form of a record, book, register, correspondence, other document or material;

"financial institution" refers to a licensed person and a prescribed development financial institution;

"foreign branch" refers to the Malaysian operations of a licensed person that is established as a branch in Malaysia;

"material outsourcing arrangement" refers to an outsourcing arrangement which−

(i) in the event of a service failure or security breach, has the potential to significantly impact the financial institution's provision of financial services to customers, business operations, financial position, reputation, or compliance with applicable laws and regulatory requirements; or

[1] A potential customer who has provided his/her information to the financial institution for purposes of using the institution's financial services or products, including a person who subsequently withdraws his/her application or whose application has been rejected by the institution.

[2] Any person authorised by a customer to act on his/her behalf. For instance, trustee, someone with power of attorney, legal guardian, or insurance agent authorised by a customer.

(ii) involves customer information and in the event of unauthorised access, disclosure or modification, or loss or theft of the information, has a material impact on the customer or financial institution.

In assessing whether an outsourcing arrangement is material, a financial institution shall have regard to the factors set out in Appendix 4[3];

"outsourcing arrangement" refers to an arrangement in which a service provider performs an activity on behalf of a financial institution on a continuing basis[4], where the activity would otherwise be undertaken by the financial institution and does not include activities set out in Appendix 3[5];

"outsourcing risk" refers to risk emanating from outsourcing arrangements that could result in a disruption to business operations, financial loss or reputational damage to a financial institution[6];

"senior management" refers to the Chief Executive Officer and senior officers;

"service provider" refers to an entity, including an affiliate, providing services to a financial institution under an outsourcing arrangement; and

"sub-contractor" refers to any entity, including an affiliate, which performs the whole or a part of the outsourced activity for the primary service provider.

6 Related legal instruments and policy documents

6.1 This policy document must be read together with other relevant legal instruments, policy document and guidelines that have been issued by the Bank, in particular those listed in Appendix 1.

7 Policy documents and circulars superseded

7.1 This policy document supersedes the guidelines and circulars listed in Appendix 2.

---

3 For the avoidance of doubt, any arrangement involving internal control functions (i.e. risk management, internal audit and compliance) shall be considered as a material outsourcing arrangement.

4 For the avoidance of doubt, an agreement which is time-bound does not preclude the activity from being considered as being performed on a continuing basis.

5 Appendix 3 provides a non-exhaustive list of arrangements that are outside the scope of this policy document.

6 This includes strategic risk, reputational risk, compliance risk, operational risk, exit strategy risk, counterparty risk, country risk, contractual risk, information security risk and concentration risk.

PART B POLICY REQUIREMENTS

8 Responsibilities of the board and senior management

S 8.1 Financial institutions shall have strong oversight and control over outsourcing arrangements, as would have been the case if they were performed in-house.

S 8.2 The board and senior management shall be accountable for ensuring effective oversight and governance of outsourcing arrangements, supported by a robust outsourcing risk management framework[7] to manage outsourcing risks and ensure compliance with relevant laws, regulations and prudential requirements that relate to outsourced activities. In particular, the board and senior management must have regard to the financial institution's ability to fulfil its obligations to customers, including the ability of customers to obtain redress, and ensure consistency with its recovery and resolution planning.

S 8.3 In fulfilling its responsibilities, the board must–

(a) establish a clear risk appetite governing outsourcing arrangements;

(b) approve the outsourcing risk management framework which, among others, addresses the financial institution's basis and approach for identifying material outsourcing arrangements. The framework must cover all outsourcing arrangements, regardless of whether they involve third parties or affiliates;

(c) establish a sound internal governance structure that provides effective oversight and control over outsourcing arrangements, consistent with the financial institution's overall business strategy and risk appetite, and does not result in the delegation of the board and management oversight and decision making responsibilities;

(d) retain sufficient management capacity and skilled resources within the institution to oversee the outsourced activity, including where the outsourced activity is undertaken by an affiliate of the financial institution; and

(e) ensure effective management of outsourcing risk, having regard to the assessments made by senior management on the state of compliance to the outsourcing risk management framework.

S 8.4 In respect of paragraph 8.3(d), the board must have in place adequate processes to ensure that–

(a) the outsourcing arrangement does not create situations of conflict between the financial institution and the service provider;

(b) the financial institution retains the continuous ability to comply with regulatory and supervisory requirements, in particular where the institution is dependent on the service provider to meet this objective; and

[7] Where a financial institution is responsible for oversight over its subsidiaries, the board and senior management must ensure that the group-wide outsourcing risk management framework adequately addresses outsourcing risk across entities within the group.

(c) where the outsourced activity is undertaken by an affiliate, the financial institution retains effective control[8] of the outsourcing arrangement.

S 8.5 The board must also approve an outsourcing plan, detailing the financial institution's planned outsourcing arrangements for the following financial year, before the plan is submitted to the Bank under paragraph 13.1. In assessing the plan, the board must have in place mechanisms to obtain assurance from senior management that the requirements set out in this policy document are duly met.

S 8.6 Senior management shall bear primary responsibility over the day-to-day management of outsourcing risk. In fulfilling its responsibilities, senior management must–

(a) develop the outsourcing risk management framework which amongst others, clearly articulates the accountability of the board and senior management and the process involved in approving and managing outsourcing arrangements. The framework, including the basis and approach for identifying material arrangements, must be reviewed periodically and kept up to date to ensure that it is appropriate in light of material changes to the scope, nature and complexity of the financial institution's operations, and in line with the financial institution's outsourcing strategy and risk appetite;

(b) manage outsourcing risks on an institution-wide basis;

(c) continuously monitor all outsourcing arrangements. This includes−

(i) ensuring timely escalation to the board of material developments on outsourcing arrangements, outsourcing risk issues and incidents of non-compliance by the service provider;

(ii) ensuring outsourcing arrangements continue to remain within the outsourcing strategy and risk appetite;

(iii) conducting an independent review[9] on a periodic basis to ensure compliance with the outsourcing framework and taking prompt remedial actions to address any gaps identified;

(iv) ensuring internal audit covers outsourcing risk as part of the risk-based audit plan; and

(v) where relevant, ensuring outsourcing arrangements do not compromise the financial institution's ability to comply with Shariah requirements;

(d) conduct assessments on the effectiveness of management of outsourcing risk on a periodic basis, covering at a minimum−

(i) a review of the performance of the service provider[10] and whether the service provider complies with the terms of the outsourcing agreement;

---

8 In the case of leveraging group systems, a financial institution retains control over decisions with respect to system parameters and inputs.

9 For the avoidance of doubt, the review must be performed by a function independent of the function that undertakes the outsourcing arrangement, which includes the institution's internal or external auditors or relevant agents, who have the requisite skills and experience to perform such reviews.

10 This includes an assessment of the continued ability of the service provider to perform the activity to the level expected in accordance with the outsourcing agreement.

(ii) the adequacy of internal control processes, including data security practices of the service provider;
(iii) whether prompt corrective actions taken by the service provider in the event of a breach of the outsourcing agreement are effective;
(iv) whether the terms of the outsourcing agreement remain appropriate and are in line with the financial institution's outsourcing risk appetite; and
(v) the financial institution's ability to preserve continuity of the outsourced activities under periods of stress[11];

(e) ensure prompt notification to the Bank of developments concerning outsourcing arrangements that result, or could result, in a material impact on the financial institution; and

(f) maintain a complete register of all outsourcing arrangements. The register must, at a minimum, include the information set out in Appendix 5 and be made readily available to the Bank upon request.

S 8.7 In respect of paragraph 8.6(a), senior management must determine whether an outsourcing arrangement is considered a material outsourcing arrangement, and whether the arrangement is appropriate to be outsourced, based on the framework approved by the board and having regard to the factors as set out in Appendix 4.

9 Outsourcing process and management of risks

G 9.1 Effective management of outsourcing risk requires financial institutions to have an in-depth and holistic understanding of risks arising from outsourcing arrangements. This entails an understanding of the relationship between the financial institution and the service provider, and impact of the outsourcing arrangement to the operations of the financial institution.

Assessment of service provider

G 9.2 Conducting a comprehensive and robust due diligence process is necessary for a financial institution to make an informed selection of service providers in relation to the risks associated with the outsourcing arrangement.

S 9.3 A financial institution must conduct appropriate due diligence of a service provider at the point of considering all new arrangements, and renewing or renegotiating existing arrangements. The scope and depth of the due diligence process must be commensurate with the materiality of the outsourced activity. The due diligence process must cover, at a minimum−

(a) capacity, capability, financial strength and business reputation[12];

[11] For the avoidance of doubt, this refers to stress incidents that could occur at the institution or the service provider.

[12] This includes an assessment that the service provider is a going concern and has strong governance structures to manage the outsourced activity throughout the duration of the arrangement.

(b) risk management and internal control capabilities, including physical and IT security controls, and business continuity management[13];
(c) the location of the outsourced activity (e.g. city and country), including primary and back-up sites;
(d) access rights of the financial institution and the Bank to the service provider;
(e) measures and processes to ensure data protection and confidentiality;
(f) reliance on sub-contractors, if any, in particular where the sub-contracting adds further complexity to the operational chains of the outsourcing arrangement;
(g) undue risks [14] resulting from similar business arrangements, if any, between the service provider and the financial institution;
(h) the extent of concentration risk to which the financial institution is exposed with respect to a single service provider and the mitigation measures to address this concentration. This does not apply to a service provider that is an affiliate and is supervised by a financial regulatory authority; and
(i) ability of the service provider to comply with relevant laws, regulations and requirements in this policy document.

S 9.4 In performing due diligence on an affiliate, the institution must make an objective assessment of the affiliate's ability to perform the outsourced activity guided by the considerations applied in paragraph 9.3. The depth of such a due diligence process may be different if the service provider is an affiliate that is supervised by a financial regulatory authority.

S 9.5 A financial institution must ensure that the outcomes of the due diligence process are well-documented and escalated to the board, where relevant, in line with the outsourcing risk management framework of the financial institution.

Outsourcing agreement

S 9.6 An outsourcing arrangement must be governed by a written agreement that is legally enforceable. The outsourcing agreement must, at a minimum, provide for the following−
(a) duration of the arrangement with date of commencement and expiry or renewal date;
(b) responsibilities of the service provider, with well-defined and measurable risk and performance standards in relation to the outsourced activity. Commercial terms tied to the performance of the service provider must not create incentives for the service provider to take on excessive risks that would affect the financial institution;
(c) controls to ensure the security of any information shared with the service provider at all times, covering at a minimum−

[13] Including the ability of the service provider to respond to service disruptions or problems resulting from natural disasters, or physical or cyber-attacks, within an appropriate timeframe.
[14] For instance, concentration risk to a systemic service provider in the industry or where the service provider's fee structure or relationship with the financial institution may create potential conflict of interest issues.

(i) responsibilities of the service provider with respect to information security;
(ii) scope of information subject to security requirements;
(iii) provisions to compensate the financial institution for any losses and corresponding liability obligations arising from a security breach attributable to the service provider;
(iv) notification requirements in the event of a security breach; and
(v) applicable jurisdictional laws;

(d) use of information shared with the service provider is limited to the extent necessary to perform the obligations under the outsourcing agreement;
(e) continuous and complete access by the financial institution to its data held by the service provider in the event of a dispute with the service provider, or termination of the arrangement;
(f) ability of the financial institution and its external auditor[15] to conduct audits and on-site inspections on the service provider and its sub-contractors, and to obtain any report or finding made in relation to the outsourced activity;
(g) notification to the financial institution of adverse developments that could materially affect the service provider's ability to meet its contractual obligations;
(h) measures that the service provider would take to ensure continuity of the outsourced activity in the event of an operational disruption or failure on the part of the service provider;
(i) regular testing of the service provider's business continuity plans (BCP), including specific testing that may be required to support the financial institution's own BCP testing, and a summary of the test results to be provided to the financial institution with respect to the outsourced activity;
(j) the dispute resolution process in the event of default or non-performance of obligations, including remedies and indemnities where relevant;
(k) circumstances that may lead to termination of the arrangement, the contractual parties' termination rights and a minimum period to execute the termination provisions, including providing sufficient time for an orderly transfer of the outsourced activity to the financial institution or another party;
(l) terms governing the ability of the primary service provider to sub-contract to other parties. Sub-contracting should not dilute the ultimate accountability of the primary service provider to the financial institution over the outsourcing arrangement, and the institution must have clear visibility over all sub-contractors[16]. Therefore, the outsourcing agreement between the financial institution and primary service provider must stipulate the following:
(i) the accountability of the primary service provider over the performance and conduct of the sub-contractor in relation to the outsourcing arrangement;
(ii) the rights of the financial institution to terminate the outsourcing agreement in the event of excessive reliance on sub-contracting (e.g.

15 Including an agent appointed by the financial institution.
16 In this respect, the primary service provider must provide sufficient notice to the financial institution before entering into an agreement with the sub-contractor.

where the sub-contracting materially increases the risks to the financial institution); and

(iii) the requirement for the sub-contractor and its staff to be bound by confidentiality provisions even after the arrangement has ceased[17]; and

(m) corresponding obligations for staff of the service provider, who are involved in the delivery of services to the financial institution's customers, to comply with similar conduct standards imposed by the Bank on the financial institution.

S 9.7 The outsourcing agreement must also contain provisions which–

(a) enable the Bank to have direct, timely and unrestricted access to the systems and any information or documents relating to the outsourced activity;

(b) enable the Bank to conduct on-site supervision of the service provider where the Bank deems necessary;

(c) enable the Bank to appoint an independent party to perform a review of the relevant systems, information or documents of the service provider relating to the outsourced activity, where the Bank deems necessary; and

(d) allow the financial institution the right to modify or terminate the arrangement when the Bank issues a direction to the financial institution to that effect under the FSA, IFSA or DFIA, as the case may be.

Protection of data confidentiality

G 9.8 Misuse, unauthorised or inadvertent disclosure of confidential information is a serious risk event for financial institutions. It is therefore imperative that the financial institution satisfies itself that the level of security controls, governance, policies, and procedures at the service provider are robust to protect the security and confidentiality of information shared under the outsourcing arrangement.

S 9.9 A financial institution must ensure that appropriate controls are in place and are effective in safeguarding the security, confidentiality and integrity of any information shared with the service provider. In meeting this requirement, the financial institution must ensure that−

(a) information disclosed to the service provider is limited to the extent necessary to provide the contracted service, and only on a need-to-know basis;

(b) information shared with the service provider is used only to the extent necessary to perform the obligations under the outsourcing agreement;

(c) all locations (e.g. city and country) where information is processed or stored, including back-up locations, are made known to the financial institution;

(d) where the service provider is located, or performs the outsourced activity, outside Malaysia, the service provider is subject to data protection standards that are comparable to Malaysia;

[17] See paragraph 9.9(f).

(e) where the service provider provides services to multiple clients, the financial institution's information must be segregated [18] from the information of other clients of the service provider;
(f) the service provider is bound by confidentiality provisions stipulated under the outsourcing agreement even after the arrangement has ceased; and
(g) information shared with the service provider is destroyed, rendered unusable, or returned to the financial institution in a timely and secure manner once the outsourcing arrangement ceases or is terminated.

Business continuity planning

G 9.10 A financial institution is responsible for ensuring that its BCP consider any operational disruptions at, or failure of, the service provider.

S 9.11 A financial institution must ensure that its BCP provide for all outsourcing arrangements. The depth and comprehensiveness of the BCP must be commensurate with the materiality of the outsourcing arrangements. At a minimum, the financial institution must ensure that the BCP include probable, adverse scenarios[19] with specific action plans. The practicality of such plans must, among others, take into consideration−
(a) the estimated cost involved to resume the outsourced activity;
(b) the possible need for an alternative service provider, including considerations of the limited number of service providers in the market; and
(c) the degree of difficulty, cost and time required to reintegrate the outsourced activity in-house.

S 9.12 In the event of a disruption, material outsourced activities must be resumed without undue delay and with minimal impact and disruptions to both business operations and the financial institution's customers.

S 9.13 A financial institution must, at all times, ensure that it has ready access to all its records and information at the service provider with respect to the outsourced activity which would be necessary for it to operate and meet its legal and regulatory obligations. This includes scenarios where network connectivity is not available, the service provider becomes insolvent or a dispute resolution process is ongoing.

S 9.14 A financial institution must periodically test its own BCP and proactively seek assurance on the state of BCP preparedness of the service provider and where relevant, alternative service providers. The intensity and regularity of the BCP testing and assessments of BCP preparedness must be commensurate with the materiality of the outsourcing arrangement. In assessing this preparedness, the financial institution must, at a minimum−
(a) ensure that the back-up arrangements are available and ready to be operated when necessary;

[18] Either logically or physically.
[19] For instance, failure, liquidation or operational disruption of the service provider, non-performance by the service provider, unexpected termination of the outsourcing arrangement, or material deterioration in the performance of the service provider.

(b) ensure that the service provider periodically tests its BCP and provides any test reports, including any identified deficiencies, that may affect the provision of the outsourced service and measures to address such deficiencies as soon as practicable; and
(c) for material outsourcing arrangements, participate in joint testing with the service provider to enable an end-to-end BCP test for these arrangements by the financial institution.

10 Outsourcing outside Malaysia

G 10.1 Outsourcing arrangements where the service provider is located, or performs the outsourced activity, outside Malaysia exposes a financial institution to additional risks (e.g. country risk). A financial institution should have in place appropriate controls and safeguards to manage these additional risks, having regard to social and political conditions, government policies, and legal and regulatory developments.

S 10.2 In conducting the due diligence process, a financial institution must ensure that such assessment addresses the added dimensions of risks associated with outsourcing outside Malaysia, and the ability of the financial institution or service provider to implement appropriate responses to emerging risk events in a timely manner.

S 10.3 A financial institution must ensure that outsourcing arrangements undertaken outside Malaysia are conducted in a manner which does not affect−
(a) the financial institution's ability to effectively monitor the service provider and execute the institution's BCP;
(b) the financial institution's prompt recovery of data in the event of the service provider's failure, having regard to the laws of the particular jurisdiction; and
(c) the Bank's ability to exercise its regulatory or supervisory powers, in particular the Bank's timely and unrestricted access to systems, information or documents relating to the outsourced activity.

11 Outsourcing involving cloud services

G 11.1 Where the outsourcing arrangement involves a cloud service provider, a financial institution should take effective measures to address risks associated with data accessibility, confidentiality, integrity, sovereignty, recoverability and regulatory compliance. This is particularly important as cloud service providers often operate a geographically dispersed computing infrastructure with regional or global distribution of data processing and storage.

S 11.2 In using cloud services, the inherent risks involved are similar to that of other forms of outsourcing arrangements. A financial institution that subscribes to cloud services must comply with the requirements of this policy document, and other relevant requirements on cloud services as specified by the Bank.

S 11.3 In relation to a financial institution's ability to conduct audits and inspections on the cloud service provider and sub-contractors pursuant to paragraph 9.6(f), the financial institution may rely on third party certification and reports made available by the cloud service provider for the audit[20], provided such reliance is supported by an adequate understanding and review of the scope of the audit and methods employed by the third party, and access to the third party and service provider to clarify matters relating to the audit.

S 11.4 In relation to the testing of a cloud service provider's BCP pursuant to paragraph 9.6(i), a financial institution must be able to access information on the state of robustness of the controls instituted by such cloud service providers arising from the BCP testing.

[20] For the avoidance of doubt, such certifications or reports should not substitute the financial institution's right to conduct on-site inspections where necessary.

PART C REGULATORY PROCESS

12 Approval for outsourcing arrangements

S 12.1 A financial institution must obtain the Bank's written approval before−

(a) entering into a new material outsourcing arrangement; or

(b) making a significant modification to an existing material outsourcing arrangement.

S 12.2 In assessing an outsourcing application under paragraph 12.1, the Bank will have regard, among others, to the following factors:

(a) the state of controls, risk management and governance of the financial institution;

(b) the materiality of the outsourcing arrangement; and

(c) other relevant matters, including any cooperation arrangements between the Bank and relevant financial regulatory authorities.

S 12.3 An application for approval pursuant to paragraph 12.1 must comprise, at a minimum, of the following information:

(a) name and registered address of the service provider, including the sub-contractors, where applicable;

(b) date of commencement of the arrangement and expiry or renewal date;

(c) a brief description of the activity to be outsourced;

(d) the locations (e.g. city and country) where the outsourced activity is undertaken by the service provider and sub-contractors, including where information is processed or stored, and the primary and back-up locations;

(e) where the arrangement involves the use of cloud service providers, the cloud services, deployment model, nature of data to be held and locations (e.g. city and country) where such data is stored, including back-up locations;

(f) outcomes of the financial institution's due diligence process;

(g) total costs of the outsourcing arrangement, including upfront and ongoing expenses;

(h) overall impact of the outsourcing arrangement on employment and talent capacity within the financial institution; and

(i) evidence of the approval granted by the relevant approval authority as determined under the financial institution's internal governance framework.

S 12.4 Notwithstanding paragraph 12.1, a financial institution is not required to obtain the Bank's prior written approval−

(a) where the outsourced activity is to be performed by an affiliate which is a financial institution; or

(b) where the outsourced activity is to be performed by an affiliate which is not supervised by the Bank, the Bank determines that the management of outsourcing risk by the financial institution is effective and having regard to the following:

(i) the affiliate is subject to the supervision of a financial regulatory authority; and

(ii) effective home-host supervisory cooperation arrangements between the Bank and the relevant financial regulatory authorities are in place.

S 12.5 In the event the Bank is of the view that an arrangement is considered material, the financial institution shall comply with paragraph 12.1.

S 12.6 An application under paragraph 12.1 must be submitted to Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan or Jabatan Penyeliaan Insurans dan Takaful, as the case may be.

13 Submission of outsourcing plan

S 13.1 A financial institution must submit an outsourcing plan approved by its board under paragraph 8.5 to the Bank within 3 months following the institution's financial year end, detailing the following:

(a) all planned outsourcing arrangements, both new and renewal of existing arrangements, for the following financial year;

(b) for each planned outsourcing arrangement−

(i) a brief description of the outsourced activity;

(ii) identification of material arrangements and main factors supporting the materiality assessment; and

(iii) the locations (e.g. city and country) where the outsourced service is undertaken, including where information is processed or stored, and back-up locations; and

(c) a description of the overall impact of the existing and planned outsourcing arrangements on employment and talent capacity within the financial institution, including any measures by the financial institution to manage the potential displacement of staff as a consequence of outsourcing arrangements, including up-skilling of staff.

For the avoidance of doubt, the yearly submission of the outsourcing plan does not constitute an approval by the Bank under paragraph 12.1.

S 13.2 A financial institution must ensure that the outsourcing plan has been holistically considered as part of its business plan.

S 13.3 The outsourcing plan in paragraph 13.1 must be submitted to Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan or Jabatan Penyeliaan Insurans dan Takaful, as the case may be.

PART D TRANSITIONAL ARRANGEMENTS

14 Transitional arrangements

S 14.1 For the purpose of paragraph 8.6(f), a financial institution must ensure that a complete register of all outsourcing arrangements is in place no later than 1 July 2019.

S 14.2 A financial institution must perform a gap analysis of all existing outsourcing arrangements against the requirements in this policy document. The financial institution must develop an action plan to address the gaps identified, including a timeline with key milestones. The gap analysis and action plan must be submitted to the Bank no later than 1 July 2019.

S 14.3 Notwithstanding paragraph 13.1, and unless otherwise approved by the Bank, a financial institution must submit an outsourcing plan for 2019 to the Bank by 1 July 2019.

S 14.4 The gap analysis, action plan, and outsourcing plan in paragraphs 14.2 and 14.3 must be submitted to Jabatan Penyeliaan Konglomerat Kewangan, Jabatan Penyeliaan Perbankan or Jabatan Penyeliaan Insurans dan Takaful, as the case may be.

S 14.5 Unless otherwise approved by the Bank, a financial institution must ensure that all existing outsourcing arrangements comply with the requirements in this policy document no later than 1 July 2022.

APPENDIX 1 RELATED LEGAL INSTRUMENTS, POLICY DOCUMENTS AND GUIDELINES

1. Credit Card
2. Credit Card-i
3. Guidelines on Data Management and MIS Framework
4. Guidelines on Data Management and MIS Framework for Development Financial Institutions
5. Debit Card
6. Debit Card-i
7. Fair Debt Collection Practices Circular
8. Circular on Fair Debt Collection Practices (Development Financial Institutions)
9. Guidelines on Business Continuity Management (Revised)
10. Guidelines on Management of IT Environment (GPIS 1)
11. Management of Customer Information and Permitted Disclosures
12. Operational Risk
13. Optimal Resource Sharing Arrangement
14. Exposure Draft on Risk Management in Technology (RMiT) and any relevant policy document issued thereafter
15. Shariah Governance Framework for Islamic Financial Institutions

APPENDIX 2 GUIDELINES AND POLICY DOCUMENTS SUPERSEDED

1. Guidelines on Outsourcing for Development Financial Institutions issued on 30 July 2009
2. Guidelines on Outsourcing for Takaful Operators issued on 12 April 2006
3. Guidelines on Outsourcing for Insurers issued on 24 December 2004
4. Guidelines on Outsourcing of Islamic Banking Operations issued on 23 June 2003
5. Guideline on Rationalisation of Operating Structure for Banking Institutions issued on 5 June 2000
6. Guidelines on Outsourcing of Banking Operations issued on 24 April 2000
7. Circular on Blanket Approval to Banking Institutions issued on 27 December 1995

APPENDIX 3 EXAMPLES OF ARRANGEMENTS EXCLUDED FROM SCOPE OF OUTSOURCING

1. For the purpose of this policy document, arrangements which entail procurement of services[21], leveraging common industry-wide infrastructure driven by regulatory requirements, and involvement of third parties due to legal requirements, are generally not considered as outsourcing arrangements. These include−

   (a) Services for the transfer, clearing and settlement of funds or securities provided by an operator of a designated payment system or an operator of an approved payment system under the FSA or the IFSA
   (b) Global financial messaging network services provided by an operator that is owned by its member financial institutions and is subject to the oversight of relevant regulators
   (c) Independent consultancy service (e.g. legal opinions, tax planning and valuation)
   (d) Independent audit assessment
   (e) Clearing and settlement arrangement between clearing houses and settlement institutions and their members
   (f) Co-insurance, reinsurance and retrocessions
   (g) Selling of insurance or takaful products by agent or broker
   (h) Correspondent banking service
   (i) Adjusting business
   (j) Trustee arrangement
   (k) Credit or market information services
   (l) Repair, support and maintenance of tangible asset (e.g. off-site ATM machine)
   (m) Purchase or subscription of commercially available software
   (n) Maintenance and support of licensed software
   (o) Telecommunication, postal and courier service
   (p) Physical security, premise access and guarding services
   (q) Catering, cleaning and event services

[21] Where a financial institution acquires services, goods or utilities which are not expected to be performed by the financial institution.

APPENDIX 4 MATERIAL OUTSOURCING ARRANGEMENTS

1. Without limiting the scope, in assessing whether an outsourcing arrangement is material, a financial institution shall have regard to the following factors:

   (a) significance of the activity to be outsourced e.g. in terms of contribution to income, cost as a percentage of total operating expenditure, or ability to achieve its strategic and business objectives;
   (b) financial, reputational and operational impact on the financial institution or significant business line;
   (c) impact on the financial institution's continuing ability to meet its obligations to its customers and counterparties in the event the service provider fails to provide the service or encounters a breach of confidentiality or security;
   (d) impact of the outsourcing on the financial institution's ability to maintain strong internal controls and meet its legal and regulatory requirements;
   (e) risk to security, confidentiality and integrity of its customer information;
   (f) interdependence of the activity to be outsourced with other activities of the financial institution;
   (g) aggregate exposure to a particular service provider in cases where the financial institution, including any affiliates, outsources multiple activities to the same service provider;
   (h) impact to the financial institution's business continuity and recovery and resolution plans, including the degree of difficulty, cost and time required to select an alternative service provider or to bring the outsourced activity in-house; and
   (i) complexity of the outsourcing arrangement and number of parties involved, in particular where the service is sub-contracted or where more than one service provider collaborates to deliver an end-to-end outsourcing solution.

2. For the avoidance of doubt, an assessment of the factors in paragraph 1 of this Appendix shall be made independent of mitigating controls by the financial institution to reduce the impact of a potential failure by a service provider in meeting the obligations under an outsourcing arrangement.

APPENDIX 5 REGISTER OF OUTSOURCING ARRANGEMENTS

1. The register must, at a minimum, include the following information for all outsourcing arrangements:

   (a) date of last update of the register;
   (b) a reference number for each outsourcing arrangement;
   (c) name, registered address, country of registration and corporate registration number of the service provider and sub-contractors;
   (d) clear identification of any service provider or sub-contractor that is an affiliate of the financial institution;
   (e) whether the service provider and sub-contractors are regulated by a financial regulatory authority;
   (f) a brief description of the outsourced activity;
   (g) whether the activity is considered material, the reasons and the date of last materiality assessment;
   (h) date of first commencement of arrangement, current date of appointment and expiry/renewal date;
   (i) the locations (e.g. city and country) where the outsourced activity is undertaken by the service provider and sub-contractors, including where information is processed or stored, and back-up locations;
   (j) where an arrangement involves the use of cloud service provider, the nature of data held and locations where such data is stored;
   (k) costs of arrangement, including pricing basis;
   (l) the governing law of the outsourcing agreement;
   (m) the date of the last and next scheduled audit, where relevant;
   (n) consideration of an alternative service provider[22];
   (o) where there are incidents involving data security breaches, a brief description of the incidents including the date of incidents and corrective actions taken by the service provider; and
   (p) date of the last and next scheduled joint business continuity plan testing.

[22] See paragraph 9.11(b).