BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Merchant Acquiring Services

Applicable to:

Registered merchant acquirers

Issued on: 15 September 2021

BNM/RH/PD 028-119

TABLE OF CONTENTS

PART A OVERVIEW

1. Introduction

1.1 Merchant acquiring services enable merchants to accept payment instruments for the sale of goods or services to their customers. Acquirers provide the link between the users of payment instruments to the merchants to enable the purchase of goods or services. When users pay for the goods or services using payment instruments, acquirers ensure that funds for such payment are settled in a timely manner to the merchants.

1.2 In tandem with the rapid changes in the electronic payment (e-payment) landscape, merchant acquiring services have experienced significant growth and considerable change in their business arrangements and set-up. Merchants have extended their acceptance of payment instruments from only payment cards to other types of instruments such as electronic money (e-money). Merchant acquiring services are no longer confined to the use of traditional Point-of-Sale (POS) terminals but now extend to the use of new payment methods such as Quick Response (QR) code and online banking. The acquiring arrangements have also expanded to accept more electronic commerce (e-commerce) merchants and involvement of third parties such as payment facilitators to facilitate expansion. Merchant acquiring services have also adapted to constant evolution of technological advancements to cater for needs of users and enhance efficiency. All of the above changes have increased the complexity and the number of players along the payment chain before payment reaches the merchants.

1.3 Due to the increasingly important role played by acquirers in the payment landscape, it is important to specify the minimum expectations and regulatory requirements for merchant acquiring services to promote confidence in the use of e-payment by both merchants and users of payment instruments. The regulatory requirements serve to ensure proper risk management in merchant acquiring services, which includes the management of settlement risk, financial risk, fraud risk and technology and cyber risk.

1.4 The objectives of this policy document are as follows –

(a) to ensure the safety and reliability of merchant acquiring services provided by acquirers; and

(b) to preserve public confidence in using or accepting payment instruments for the payment of goods and services.

2. Applicability

2.1 This policy document is applicable to acquirers registered pursuant to sections 17(1) and 18 of the Financial Services Act 2013 (FSA) that fulfils the following criteria –

(a) enters into a contract with merchant(s), which results in a transfer of funds to the merchant(s) by –

(i) conducting or being responsible for fund settlement; or

(ii) issuing fund settlement instructions;

(b) facilitates the merchant's acceptance of payment instruments; and

(c) is a direct participant of payment instrument network(s) to provide merchant acquiring services.

2.2 The requirements under paragraph 9 of this policy document are only applicable to non-bank acquirers.

3. Legal Provisions

3.1 The requirements in this policy document are specified pursuant to sections 18(2), 33(1), 49, 123(1) and 143 of the FSA.

3.2 The guidance in this policy document is issued pursuant to section 266 of the FSA.

4. Effective Date

4.1 This policy document comes into effect on 15 March 2022.

4.2 However, for non-bank acquirers, the following will apply –

(a) paragraphs 17.1 to 21.3 come into effect on 15 September 2022; and

(b) paragraphs 9.1 to 9.3 come into effect on 15 September 2023.

5. Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA unless otherwise defined in this policy document.

5.2 For the purposes of this policy document –

"S" denotes a standard, an obligation, a 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;

"acquirer" refers to any person who is registered[1] pursuant to sections 17(1) and 18 of the FSA to provide merchant acquiring services and fulfils the criteria under paragraph 2.1;

"critical system" refers to any application system that supports the provision of critical services, where failure of the system has the potential to significantly impair the acquirer's provision of services to customers or counterparties, business operations, financial position, reputation or compliance with applicable laws and regulatory requirements;

"customer and counterparty information" as used in Part D of this policy document, refers to any information relating to the affairs or, in particular, the account, of any customer or counterparty of an acquirer in whatever form;

[1] For avoidance of doubt, an e-money issuer that also conducts its own merchant acquiring services (i.e. acquires merchants directly) for its own e-money scheme is also considered as an acquirer.

"cyber risk" refers to threats or vulnerabilities emanating from the connectivity of internal technology infrastructure to external networks or the Internet;

"digital service" refers to the provision of payment services delivered to customers via electronic channels and devices including Internet and mobile devices, self-service and point-of-sale terminals;

"direct participant" refers to a principal member of a payment instrument network(s) for purposes of providing merchant acquiring services;

"direct settlement method" refers to a method whereby settlement is done directly from a payment instrument network or an identified settlement bank[2] to the merchant, based on the payment instruction by the acquirer. Such settlement funds cannot be claimed by the acquirer or creditors of the acquirer, including upon the acquirer's liquidation;

"e-commerce merchant" refers to merchant that sells or offers goods and/or services electronically over the Internet or any other channels not involving face-to-face interaction (e.g. mail or telephone order);

"foreign-issued payment instrument" refers to a payment instrument issued by an issuer not locally incorporated in Malaysia but may be accepted at local merchants;

"issuer of e-money" refers to a person approved under section 11 of the FSA or Islamic Financial Services Act 2013 (IFSA) to issue e-money;

"key responsible persons" or **"KRP"** refer to persons that are accountable or responsible for the management and oversight of merchant acquiring services. These comprise the directors and Chief Executive Officer (CEO);

[2] A licensed bank, licensed Islamic bank or prescribed institution appointed or identified to conduct direct settlement to merchants.

"large acquirers" refer to acquirers with an actual or projected amount of average monthly transaction value (MTV) of more than RM10,000,000 (where for the purpose of calculation of average MTV, the actual amount is calculated based on a 12-month moving average, while the projected amount is calculated based on an estimation of the average monthly amount for the next 12-month period);

"licensed Islamic bank" means an Islamic bank licensed under the IFSA;

"merchant" refers to a person or an entity that has a contractual agreement with an acquirer to accept payment instruments for the sale or offer of goods or services. This includes the merchants acquired by a payment facilitator on behalf of an acquirer;

"non-bank acquirer" refers to any person who is not a licensed bank, licensed Islamic bank or prescribed institution that is registered pursuant to sections 17(1) and 18 of the FSA to provide merchant acquiring services and fulfils the criteria under paragraph 2.1;

"outsourcing arrangement" refers to an arrangement in which a service provider performs an activity on behalf of the acquirer on a continuing basis[3], where the activity would otherwise be undertaken by the acquirer and does not include activities set out in **Appendix 9**;

"payment facilitator" refers to an entity that is appointed by an acquirer to perform merchant acquiring services on behalf of the acquirer. For avoidance of doubt, a payment facilitator can be either: (1) an existing acquirer for any payment instrument network or (2) a third party acquirer;

"payment gateway service provider" refers to an entity that provides the information technology (IT) system and infrastructure for purposes of processing or supporting payment or settlement transactions;

[3] For avoidance of doubt, an arrangement which is time-bound does not preclude that activity from being considered as being performed on a continuing basis.

"payment instrument network" refers to a payment system that enables payment to be made using a payment instrument under its brand and provides clearing and/or settlement services for its members namely issuers and/or acquirers;

"physical merchant" refers to merchant that sells or offers goods or services physically over the counter (i.e. brick-and-mortar/face-to-face business);

"point-of-sale (POS) terminal" refers to an electronic device located in or at a merchant's premise that enables a customer to effect a transaction for the purchase of goods or services using a payment instrument;

"prescribed institution" means a development financial institution prescribed under the Development Financial Institutions Act 2002;

"production data centre" refers to any facility which hosts active critical production application systems irrespective of location;

"senior management" refers to the CEO and senior officers;

"service provider" refers to an entity, including an affiliate, providing services to an acquirer under an outsourcing arrangement. This may include third party service provider as used in Part D of this policy document;

"small acquirers" refer to acquirers with an actual or projected amount of average MTV of less than RM10,000,000 (where for the purpose of calculation of average MTV, the actual amount is calculated based on a 12-month moving average, while the projected amount is calculated based on an estimation of the average monthly amount for the next 12-month period);

"SME" refers to small and medium enterprises as defined in the Notification on Definition of Small and Medium Enterprises (SMEs)[4] issued by Bank Negara Malaysia (the Bank) and as may be updated from time to time;

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

"third party acquirer" refers to an entity that is appointed by an acquirer to perform merchant acquiring services on behalf of the acquirer, but does not fulfil the criteria in paragraph 2.1; and

"third party service provider" as used in Part D of this policy document refers to an internal group affiliate or external entity providing technology-related functions or services that involve the transmission, processing, storage or handling of confidential information pertaining to the acquirer or its customers. This includes cloud computing software, platform and infrastructure service providers.

6. Related Legal Instruments and Policy Documents

6.1 This policy document must be read together with other relevant legal instruments and policy documents that have been issued by the Bank, in particular –

(a) the policy document on the Risk-Based Authentication for Online Payment Card Transaction;
(b) the policy document on the Payment Card Reform Framework;
(c) the policy document on the Management of Customer Information and Permitted Disclosures; and
(d) the policy document on Interoperable Credit Transfer Framework.

[4] Issued on 27 December 2017.

7. Policy Documents Superseded

7.1 This policy document supersedes the requirements listed below –

(a) Paragraph 33 – Specific requirements for acquirers in policy document on Credit Card issued on 2 July 2019;

(b) Paragraph 34 – Specific requirements for acquirers in policy document on Credit Card-i issued on 2 July 2019;

(c) Paragraph 23 – Specific requirements for acquirers in policy document on Debit Card issued on 2 December 2016;

(d) Paragraph 25 – Specific requirements for acquirers in policy document on Debit Card-i issued on 2 December 2016;

(e) Paragraph 30 – Specific requirements for acquirers in policy document on Charge Card issued on 2 December 2016; and

(f) Paragraph 32 – Specific requirements for acquirers in policy document on Charge Card-i issued on 2 December 2016.

PART B GOVERNANCE

8. Effective Governance and Oversight

S 8.1 Acquirers shall establish adequate governance arrangements which are effective and transparent to ensure the continued integrity of its merchant acquiring services which include, among others, the following –

(a) a board of directors (board) and senior management that consists of people with calibre, credibility and integrity;

(b) clearly defined and documented organisational arrangements, such as ownership and management structure; and

(c) segregation of duties and internal control arrangements to reduce the chances of mismanagement and fraud.

Board roles and responsibilities

S 8.2 The board shall have a board charter that sets out the mandate, responsibilities and procedures of the board and its committees (if any), including the matters reserved for the board's decision.

S 8.3 The board shall have the overall responsibility in ensuring the sustainable growth, financial soundness and reliability of the acquirer's merchant acquiring services which include –

(a) determining, reviewing and approving strategies, business plans and significant policies, including its risk appetite and monitoring management's performance in implementing them;

(b) setting corporate values and clear lines of responsibility and accountability that are communicated throughout the organisation;

(c) ensuring adequate assessment is conducted on key responsible persons (KRP);

(d) ensuring selection of competent senior management;

(e) ensuring that the operations of the business are conducted prudently, and within the framework of relevant laws and policies;

(f) ensuring that comprehensive risk management policies, processes and infrastructure, and effective operationalisation of the risk controls to manage the various types of risks, are in place and effective; and

(g) establishing an effective compliance and internal audit functions.

S 8.4 The board shall ensure that an effective oversight and risk management mechanism is in place, which includes the following –

(a) an effective oversight and governance structure to manage the day-to-day operations of the acquirer;

(b) risk management and control framework on the following areas –

(i) technology risk management and cyber resilience;

(ii) mitigation of fund settlement risk to merchants;

(iii) mitigation of fraud or illegal activities;

(iv) merchant recruitment and monitoring;

(v) outsourcing arrangement with service providers; and

(c) appropriate and timely reporting or escalation of issues that may impact the safety, security or operational reliability of the merchant acquiring operations.

S 8.5 The board shall ensure that the risk management and control framework is periodically reviewed for continued effectiveness. This includes ensuring an audit by an independent party is conducted with reasonable frequency to detect weaknesses and enable corrective measures to be taken in a timely manner.

S 8.6 The board and its committees (if any) shall be of a size that promotes effective deliberation and encourages the active participation of all directors. The board shall meet sufficiently whereby the number and frequency of board meetings shall commensurate with the size and complexity of the acquirer’s operations, to review the acquirer’s performance, including the status of its compliance with regulatory requirements and to deal with any issues pertaining to the operations of merchant acquiring services.

S 8.7 The board shall ensure that clear and accurate minutes of board meetings are maintained to record the decisions of the board, including the key deliberations, rationale for each decision made, and any significant concerns or dissenting views.

S 8.8 With regard to the management of technology and cybersecurity risks, the board shall –

(a) establish and approve the technology risk appetite which is aligned with the acquirer's risk appetite statement. In doing so, the board shall approve the corresponding risk tolerances for technology-related events and ensure key performance indicators are in place to monitor the acquirer's technology risk against its approved risk tolerance. The board shall ensure the senior management of the acquirer provides regular updates on the status of these indicators, key technology risks and critical technology operations to facilitate strategic decision-making; and

(b) ensure and oversee the adequacy of the acquirer's IT and cybersecurity strategic plans covering a period of no less than three (3) years. These plans shall address the acquirer's requirements on infrastructure, control measures to mitigate IT and cyber risk as well as financial and non-financial resources, which are commensurate with the complexity of the acquirer's operations and changes in the risk profile as well as the business environment. These plans shall be periodically reviewed, at least once every three (3) years.

G 8.9 Given the rapidly evolving cyber threat landscape, the board should allocate sufficient time to discuss cyber risks and related issues, including the strategic and reputational risks associated with a cyber-incident. This should be supported by input from external experts as appropriate. The board should also ensure its continuous engagement in cybersecurity preparedness, education and training.

S 8.10 The board shall be responsible for ensuring the effectiveness of the audit function including technology audit. The board shall review and ensure the appropriate audit scope, procedures and frequency of audits. The board shall also ensure effective

oversight over the prompt closure of corrective actions to address any issues or control gaps.

Senior Management

S 8.11 The senior management of acquirers shall be responsible for ensuring the following –

(a) effective policies and procedures are established and implemented for, among others, the following areas –

(i) risk management and appropriate controls to manage and monitor risks, including those under paragraph 8.4(b);

(ii) due diligence and oversight to manage outsourced arrangements supporting the merchant acquiring operations;

(iii) sufficient and timely reporting or escalation of issues to the board;

(b) overseeing the formulation and effective implementation of any business or strategic plan, including the strategic technology plan and associated technology policies and procedures; and

(c) a robust assessment is conducted to approve any deviation from policies and procedures, including technology-related policies. Material deviations shall be reported to the board.

S 8.12 The senior management shall consist of individuals with the appropriate skill set and experience to adequately support the merchant acquiring services. This includes individuals from technology functions to provide guidance on the acquirers' technology plans and operations.

S 8.13 The senior management shall ensure adequate allocation of resources as well as appropriately skilled and competent staff to support all critical functions of the merchant acquiring services, including to ensure maintenance of robust technology systems and management of technology risk.

G 8.14 For large acquirers, the senior management should embed appropriate oversight arrangements within the technology function to support the enterprise-wide

oversight of technology risk. These arrangements should provide for designated staff responsible for the identification, assessment and mitigation of technology risks who do not engage in day-to-day technology operations.

PART C OPERATIONAL REQUIREMENTS

9. Minimum Capital Funds Requirements for Non-Bank Acquirers

S 9.1 Small non-bank acquirers are required to maintain, at all times, minimum capital funds of RM300,000.

S 9.2 Large non-bank acquirers are required to maintain, at all times, minimum capital funds of RM1,000,000.

S 9.3 Non-bank acquirers shall maintain the required minimum capital funds in accordance with the computation specified in **Appendix 1**.

10. Settlement Risk Management

S 10.1 Acquirers shall be responsible to process the payment of funds to its merchants in a proper and timely manner to manage settlement risk. For the purpose of this paragraph, settlement risk is described as the risk of acquirers' inability to honour the obligation to transfer funds arising from a transaction as a result of clearing, at an agreed-upon time to the merchants.

S 10.2 Acquirers shall ensure timely and complete funds settlement to merchants as per the terms agreed in the contractual agreement with merchants.

S 10.3 Acquirers shall ensure that the settlement period commensurate with the merchants' business models and needs.

G 10.4 Acquirers should ensure that the settlement period is no longer than two (2) and five (5) working days from the date of funds received from the payment instrument

network, for physical merchants and e-commerce merchants, respectively. Notwithstanding this, acquirers should strive for a shorter settlement period and if a merchant requests for a shorter settlement period, the acquirer should assess the feasibility of accommodating such requests accordingly.

S 10.5 Acquirers shall deposit the funds received for settlement to merchants in a dedicated deposit account (i.e. designated account) with licensed banks, licensed Islamic banks or prescribed institutions, separately from their own funds. The funds in the dedicated deposit account shall only be used for settlement purposes to the merchants and/or chargebacks to issuers of payment instruments less the Merchant Discount Rate (MDR) charged or any other applicable charges to the merchant.

S 10.6 In the event settlement by acquirers to SME merchants takes more than two (2) working days from the date of funds received from the payment instrument network, the acquirer shall ensure the funds are safeguarded as follows –

(a) place the settlement funds in a trust account with a licensed bank, licensed Islamic bank or prescribed institution in accordance with the Trustee Act 1949; or

(b) adopt direct settlement method to merchants; or

(c) secure a bank guarantee from a licensed bank, licensed Islamic bank or prescribed institution on such settlement funds or outstanding amount for settlement.

S 10.7 Acquirers shall be liable to provide the funds settlement to merchants in the event the issuer, including foreign issuers of payment instruments, or any other parties involved in the handling of such funds, fail to fulfil its settlement obligations.

11. Merchant Management

Merchant recruitment

S 11.1 Acquirers shall establish prudent underwriting criteria and procedures to ensure proper due-diligence for on-boarding of a merchant. The assessment criteria shall include the following –

(a) relevant background information on the merchant (e.g. financial history such as bankruptcy/insolvency check, nature of business, etc.);

(b) legitimacy of the merchant's business, with no involvement in or association with any fraudulent or illegal activities including business activities intended to deceive consumers such as "scratch and win" and "get-rich-quick" schemes; and

(c) the merchant has not been blacklisted by any authorities or other acquirers for any suspected fraudulent or illegal activities.

S 11.2 Acquirers shall verify the merchants' identity using reliable documents, information or any other measures that acquirers deem appropriate, taking into consideration the nature and size of the business of the respective merchants, before establishing any acquiring relationship with the merchants.

G 11.3 For purposes of paragraph 11.2 –

(a) the verification method may include site visits, website/channel checking or company screening; and

(b) documents and information to be used for verification may include the business name, address, website/channel, contact, proof of existence (e.g. business registration number, identification number, etc.), owner details, business nature and products/services offered.

S 11.4 Merchants shall not be on-boarded via a merchant recruitment agent[5] unless approved by the acquirer. Acquirers shall retain the responsibility to ensure proper

[5] The merchant recruitment agent's roles are limited to the referral of merchants, collection of merchants' information and documents for application purposes and submission to acquirers for approval. The activities do not involve processing of funds or facilitating the transactions.

due-diligence on merchants is conducted by the merchant recruitment agent and ensure that the merchants on-boarded do not conduct fraudulent or illegal activities. Acquirers shall also ensure that controls as per paragraphs 11.1 and 11.2 are put in place by the merchant recruitment agent.

Merchant monitoring

S 11.5 Acquirers shall conduct effective monitoring on their merchants' activities to ensure that the merchants are not involved in any fraudulent or illegal activities.

S 11.6 Acquirers shall maintain a "watch list" of merchants that are suspected to be collusive or involved in fraudulent or illegal activities, and the activities of these merchants shall be closely monitored and investigated.

S 11.7 Acquirers shall monitor chargebacks and its trend, including the merchants' capacity to repay these chargebacks and act accordingly (e.g. close monitoring, termination of merchant, if necessary) to mitigate any risks associated with engaging such merchants.

S 11.8 Acquirers shall terminate immediately any acquiring relationship with a merchant that has been charged or convicted of a criminal offence relating to fraudulent or illegal activity.

G 11.9 Acquirers shall conduct periodic assessment, which may include mystery shopping or audit on their merchants, to ensure that the merchants adhere to payment instruments' acceptance and authorisation procedures.

Information security requirements for merchants

S 11.10 Acquirers shall ensure that merchants maintain and demonstrate compliance with the applicable regulations on data security and data protection as well as establish controls[6] that are effective in protecting customer data and information. This

[6] Controls include process and procedures as well as IT security controls that are commonly accepted as effective by industry practice.

includes any third party service providers engaged by the merchants for accessing, storing, transmitting and processing customer data.

S 11.11 The acquirers' agreements with merchants shall include provisions to ensure the merchants and merchants' third party service providers maintain compliance with applicable security requirements and established security standards.

S 11.12 Acquirers shall educate[7] and raise awareness among their merchants on the importance of protection of customer data and the legal consequences[8] of failing to adequately protect such data.

12. Fraud Risk Management

S 12.1 Acquirers shall put in place an effective mechanism, which includes the process and procedures to mitigate fraud risk, which includes fraud prevention, detection and monitoring.

S 12.2 Acquirers shall ensure the following –

(a) real time fraud detection and monitoring, effective early detection of unusual transactions and mechanism to halt or delay fraudulent or suspicious transactions;

(b) necessary processes and procedures are in place to enable authentication by customers based on the risk profile of customers and transactions, to effectively mitigate and manage the potential risk identified;

(c) the fraud risk management measures shall be reviewed periodically to ensure proactive actions are taken to address any inadequacies in such measures;

(d) fraud incidents and their assessment shall be reported to the board and senior management in a timely manner if the impact is significant; and

[7] By providing appropriate level of awareness through various measures such as training, constant reminders or engagement sessions.
[8] Such as non-compliance with the Personal Data Protection Act 2010.

(e) reporting to the Bank shall be made in a timely manner if the impact is significant and in accordance with the fraud reporting requirement as issued by the Bank.

13. Business Continuity Management

S 13.1 Acquirers shall ensure that they have adequate resources and capacity in terms of hardware, software and other operating capabilities[9] to deliver consistently reliable and secure services.

S 13.2 Acquirers shall ensure that measures are in place to support operational reliability, which include –

(a) strong internal controls to minimise operational risk such as system security risk;

(b) comprehensive and well-documented operational and technical procedures; and

(c) systems with a robust disaster recovery plan, including a highly reliable backup system.

S 13.3 Acquirers shall undertake a structured risk assessment process to –

(a) identify potential threats that could cause material business disruptions, resulting in the inability to fulfil business obligations; and

(b) assess the likelihood of the identified threats occurring and determine the impact on the acquirer (e.g. business impact analysis).

S 13.4 Acquirers shall develop an effective business continuity plan (BCP) and disaster recovery plan (DRP) for at least all critical business functions and other functions, where applicable.

G 13.5 For purposes of paragraph 13.3, acquirers are expected to carry out a business impact analysis (BIA) on an annual basis, which forms the foundation of

[9] This may refer to any other skills or processes involved in the operations (e.g. adequate manpower and skill set to operate the systems).

developing the BCP and as and when there are material changes to the acquirers' business activities.

G 13.6 Acquirers should determine the maximum tolerable downtime (MTD) and recovery time objectives (RTO) for each critical business function. The goal is to develop a BCP that details out the procedures and the minimum level of resources required to recover the critical business functions within the recovery timeframe and maintain services at an acceptable level.

S 13.7 To ensure comprehensiveness of its business continuity management, acquirers shall ensure its outsourced service provider also has an effective BCP and DRP and implements other relevant safeguards to ensure the continuity of the material outsourced activities, with the objective to minimise the acquirers' business disruptions.

S 13.8 Acquirers shall test the BCP and DRP regularly to ensure the functionality and effectiveness of the recovery strategies and procedures, preparedness of staff and other recovery resources.

14. Outsourcing

S 14.1 Acquirers shall remain responsible and accountable for the services outsourced to any service provider[10] (e.g. payment facilitators, merchant recruitment agents, payment gateway service providers, IT service providers) under an outsourcing arrangement[11].

S 14.2 Prior to entering into any outsourcing arrangement, acquirers shall, at minimum, ensure the following –

(a) availability of sufficient expertise within the acquirer to oversee and manage the outsourcing relationship;

[10] Including affiliates of the acquirer, regardless of jurisdiction.

[11] For avoidance of doubt, an arrangement will be deemed as an outsourcing arrangement as long as the activities fulfil the "outsourcing arrangement" definition specified under paragraph 5.2 of this policy document.

(b) the scope and nature of services and operations to be outsourced would not compromise the controls and risk management of the merchant acquiring services. Acquirers shall ensure the following –

(i) the outsourcing of such processes does not take away the critical decision making function of the acquirers;

(ii) the outsourcing of such processes does not threaten strategic arrangements, flexibility needed by acquirers on important areas and control of the acquirers;

(iii) the outsourcing of such processes would not impair the reputation, integrity and credibility of the acquirers; and

(iv) processes are in place for the acquirers to retain the ability to comply with the regulatory and supervisory requirements on the outsourced functions.

S 14.3 Acquirers shall perform appropriate due diligence of the service provider before the outsourcing arrangements are formalised, which includes the following areas –

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

(b) risk management and internal control capabilities, including physical and IT security controls as well as business continuity management[13];

(c) measures and procedures to ensure data protection and confidentiality;

(d) reliance of service providers on sub-contractors; and

(e) ability of the service provider to comply with relevant laws, regulations and requirements in this policy document.

G 14.4 Acquirers should also assess the extent of concentration risk to which the acquirer is exposed with respect to a single service provider and the mitigation measures to address this concentration, except when the service provider is an affiliate and is supervised by a financial regulatory authority.

[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.

[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.

S 14.5 Approval from the board to outsource identified functions shall be obtained and documented, substantiated by outcomes of the due diligence process conducted on the service provider.

S 14.6 Acquirers shall ensure that the outsourcing arrangement is governed by a written agreement, which shall be comprehensive, legally enforceable and shall include the minimum requirements specified in **Appendix 2**.

S 14.7 In addition to the requirements in **Appendix 2**, for an outsourcing arrangement with a payment facilitator, acquirers shall ensure that the agreement between the payment facilitator and merchant –

(a) clearly reflects that the payment facilitator is entering into the agreement with the merchant on behalf of and/or as agent of the acquirer;

(b) contains relevant information of the transactions relevant to the acquirer, including information on the merchants and any other information that may have significant implications to the acquirer; and

(c) contains the acquirer's contact details which the merchant may use to directly submit queries and concerns, if any, related to the transactions.

S 14.8 Acquirers shall 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, acquirers shall ensure the following –

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

(c) 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;

(d) the service provider maintains compliance with applicable security requirements and established security standards[14] at all times; and

(e) the service provider undertakes to safeguard customer information of the acquirer at all times and reports any customer information breach to the acquirer within an agreed timeframe.

S 14.9 In addition to the requirements in paragraph (b) of **Appendix 2**, where applicable, the acquirer shall ensure that the service provider provides a written undertaking to the acquirer to comply with all relevant laws and regulatory requirements on secrecy and data protection.

S 14.10 Acquirers shall ensure their service provider complies with the relevant regulatory requirements specified in this policy document[15] and as may be specified by the Bank from time to time.

S 14.11 The requirement in paragraph 14.10 is also applicable when a service provider engages a sub-contractor to undertake the activities that were outsourced by the acquirer, whereby the acquirer shall implement proper controls to ensure that the sub-contractor complies with the relevant requirements based on standards issued by the Bank to acquirers from time to time.

S 14.12 Acquirers shall have a contingency plan or arrangements to secure business continuity with the service provider in the event the arrangement with the service provider is abruptly terminated. This is to mitigate any significant discontinuity in the work that is supposed to be conducted by the service provider. The contingency plan shall be reviewed from time to time to ensure that the plan is current and ready for implementation in the event of abrupt termination of the service provider.

[14] Any relevant local or international standards commonly applied by the relevant industry.

[15] This includes specific requirements for system development and acquisition, data centre operations, network resilience, technology security and cybersecurity, wherever applicable.

S 14.13 Notwithstanding that the operational activities are outsourced, reporting by the service provider to the acquirer and monitoring mechanisms on the service provider shall be put in place by the acquirer to ensure that the integrity and quality of work conducted by the service provider is maintained. Regular reviews shall also be conducted by the acquirer to monitor the performance of the service provider.

S 14.14 Periodic independent reviews either via internal and/or external audits, shall be conducted on the outsourced operations, with the same scope of review if the said operations are conducted in-house.

S 14.15 Acquirers shall ensure that any weaknesses highlighted during the audit pursuant to paragraph 14.14 are well-documented and promptly rectified by the service provider especially where such weaknesses may affect the integrity of the internal controls of the acquirers.

G 14.16 For outsourcing arrangements where the service provider is located or the services are performed outside Malaysia, the acquirer should have appropriate controls and safeguards in place to manage any additional risk, with regard to various conditions, including legal and regulatory requirements as well as social and political conditions.

S 14.17 Acquirers shall ensure that the outsourcing arrangements undertaken outside Malaysia are conducted in a manner which does not affect –

(a) the acquirer's ability to effectively monitor the service provider and execute its BCP;

(b) the acquirer'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.

S 14.18 For outsourcing involving cloud services, acquirers may rely on third party certification and reports made available by the cloud service provider for purposes of conducting audits and inspections on the cloud service provider and sub-contractors. However, such reliance by the acquirer shall be 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.

15. Arrangement with Parties Involved in Payment and Settlement Process

S 15.1 Acquirers are responsible for ensuring that the parties that they enter into a contract with, who may also expose merchants to payment and/or settlement risk, are able to manage such risks appropriately. Such parties include payment facilitators.

S 15.2 In addition to the requirements in paragraph 14, acquirers are required to ensure such parties in paragraph 15.1 have adequate operational and risk management policies and procedures in place, which include the following –

(a) the parties conduct sound assessment and due-diligence on their merchants to ensure that the merchants are conducting a legitimate business and not involved in fraudulent or illegal activities;

(b) the parties have safeguard measures to ensure timely and complete funds settlement to the merchants (e.g. placing funds in a designated account with licensed banks, licensed Islamic banks or prescribed institutions only for settlement purposes and are transparent in their settlement terms and period to their merchants);

(c) the parties as well as their merchants are able to ensure confidentiality, security and integrity of customer data at all times;

(d) the parties are able to ensure the safety, reliability and availability of their system and network infrastructure; and

(e) the parties have appropriate dispute resolution mechanisms for the merchants.

S 15.3 Acquirers shall be held responsible for fulfilling the settlement obligation to the merchants of a payment facilitator, in the event that the payment facilitator fails to fulfil its settlement obligations to the merchants.

S 15.4 Notwithstanding paragraph 14.11, acquirers shall ensure that a payment facilitator does not appoint another payment facilitator for purposes of acquiring a merchant.

S 15.5 Acquirers shall periodically monitor the transactions or activities of the parties mentioned in paragraph 15.1 (e.g. through transaction monitoring, site visits at the business premises or audit assessment) to ensure that appropriate controls and risk mitigation measures are put in place by such parties in managing the payment and/or settlement risk and any issues or weaknesses detected are promptly rectified.

16. Appropriate Treatment for Merchants

S 16.1 Acquirers shall establish appropriate rules and procedures on liability management and chargeback, which shall be clearly specified in the merchant agreements. Acquirers shall ensure that merchants are not held liable for any fraud losses or chargeback if the transactions acceptance procedures as stipulated in the merchant agreement have been adhered to by the merchants.

S 16.2 In the event funds are withheld from the merchants, the acquirers are responsible for ensuring that the withholding of such funds due to their merchants (e.g. for suspected fraudulent transactions or to facilitate chargeback requests from the issuer) is done in a fair manner and not detrimental to the merchants. This shall include but is not limited to the following –

(a) provide clarity in the circumstances for withholding of funds due to the merchants (e.g. fraudulent transactions);

(b) provide clarity and identify the definite period for withholding of funds due to the merchants (e.g. within chargeback period of one hundred and twenty (120) days);

(c) processes involved in releasing of withheld funds are done in an expedient manner and within the identified timeframe;

(d) maintenance of withheld funds is made in a separate account, which shall not be used for acquirers' own operations; and

(e) provide clear communication and regular updates on the status of the withheld funds to the merchants.

S 16.3 Acquirers shall establish clear and robust dispute resolution procedures to ensure effective and timely resolution of dispute cases between acquirers and their merchants.

S 16.4 Acquirers shall acknowledge receipt of the dispute within two (2) working days from the date such dispute is lodged and provide a written decision to merchants within thirty (30) working days. Acquirers shall inform the merchants if a longer time is required to address the dispute and provide appropriate rationale.

PART D INFORMATION TECHNOLOGY (IT) REQUIREMENTS

17. Technology Risk Management

S 17.1 Acquirers shall establish the Technology Risk Management Framework (TRMF), which is a framework to safeguard the acquirers' information infrastructure, systems and data as an integral part of the acquirers' risk management framework.

G 17.2 The TRMF should include the following –

(a) clear definition of technology risk;

(b) clear responsibilities assigned for the management of technology risk at different levels and across functions, with appropriate governance and reporting arrangements;

(c) the identification of technology risks to which the acquirers are exposed, including risks from the adoption of new or emerging technology;

(d) risk classification of all information assets/systems based on their criticality;

(e) risk measurement and assessment approaches and methodologies;

(f) risk controls and mitigations; and

(g) continuous monitoring to timely detect and address any material risks.

G 17.3 Acquirers should establish an independent enterprise-wide technology risk management function which should be responsible for —

(a) implementing the TRMF and Cyber Resilience Framework (CRF) as provided under paragraph 19;

(b) advising on critical technology projects and ensuring critical issues that may have an impact on the acquirers' risk tolerance are adequately deliberated or escalated in a timely manner; and

(c) providing independent views to the board and senior management on third party assessment[16], where necessary.

G 17.4 Acquirers should designate a Chief Information Security Officer (CISO), by whatever name called, to be responsible for the technology risk management function of the acquirers. The acquirers should ensure that the CISO has sufficient authority, independence and resources[17]. The CISO should —

(a) be independent from day-to-day technology operations;

(b) keep apprised of current and emerging technology risks which could potentially affect the acquirers' risk profile; and

(c) be appropriately certified.

G 17.5 The CISO should be responsible for ensuring the acquirers' information assets and technologies are adequately protected, which include —

(a) formulating appropriate policies for the effective implementation of TRMF and CRF;

(b) enforcing compliance with these policies, frameworks and other technology-related regulatory requirements; and

[16] Relevant third party assessment may include the Data Centre Risk Assessment (DCRA), Network Resilience and Risk Assessment (NRA) and independent assurance for introduction of new or enhanced digital services.

[17] Acquirers' CISO may take guidance from the expertise of a group-level CISO, in or outside of Malaysia, and may also hold other roles and responsibilities. Such designated CISO should be accountable for and serve as the point of contact with the Bank on the acquirers' technology-related matters, including managing entity-specific risks, supporting prompt incident response and reporting to the acquirers' board.

(c) advising senior management on technology risk and security matters, including developments in the acquirers' technology security risk profile in relation to its businesses and operations.

18. Technology Operations Management

Technology Project Management

S 18.1 Acquirers shall establish appropriate governance requirements commensurate with the risk and complexity[18] of technology projects undertaken. This shall include establishing project oversight roles and responsibilities, authority and reporting structures, and risk assessment throughout the project life cycle.

G 18.2 The risk assessment should identify and address the key risks arising from the implementation of technology projects. These include the risks that could threaten successful project implementation and the risks that a project failure will lead to a broader impact on the acquirers' operational capabilities. At a minimum, due regard should be given to the following areas –

(a) the adequacy and competency of resources including those of the vendor to effectively implement the project. This should also take into consideration the number, size and duration of significant technology projects undertaken concurrently by the acquirers;

(b) the complexity of systems to be implemented such as the use of unproven or unfamiliar technology and the corresponding risks of integrating the new technology into existing systems, managing multiple vendor-proprietary technologies, large-scale data migration or cleansing efforts and extensive system customisation;

(c) the adequacy and configuration of security controls throughout the project life cycle to mitigate cybersecurity breaches or exposure of confidential data;

(d) the comprehensiveness of the user requirement specifications to mitigate risks

[18] For example, large-scale integration projects or those involving IT systems should be subject to more stringent project governance requirements such as more frequent reporting to the board and senior management, more experienced project managers and sponsors, more frequent milestone reviews and independent quality assurance at major project approval stages.

from extensive changes in project scope or deficiencies in meeting business needs;

(e) the robustness of system and user testing strategies to reduce risks of undiscovered system faults and functionality errors;

(f) the appropriateness of system deployment and fallback strategies to mitigate risks from prolonged system stability issues; and

(g) the adequacy of disaster recovery operational readiness following the implementation of new or enhanced systems.

G 18.3 The board and senior management should receive and review timely reports on the management of these risks on an ongoing basis throughout the implementation of significant projects.

System Development and Acquisition

G 18.4 Acquirers should establish an Enterprise Architecture Framework (EAF) that provides a holistic view of technology throughout the acquirers. The EAF is an overall technical design and high-level plan that describes the acquirers' technology infrastructure, systems' inter-connectivity and security controls. The EAF facilitates the conceptual design and maintenance of the network infrastructure, related technology controls and policies and serves as a foundation on which acquirers plan and structure system development and acquisition strategies to meet business goals.

S 18.5 Acquirers shall establish clear risk management policies and practices for the key phases of the system development life cycle (SDLC) encompassing system design, development, testing, deployment, change management, maintenance and decommissioning. Such policies and practices shall also embed security and relevant enterprise architecture considerations into the SDLC to ensure confidentiality, integrity and availability of data[19]. The policies and practices shall be reviewed at least once every three (3) years to ensure that they remain relevant to the acquirers' environment.

[19] The security considerations shall include ensuring appropriate segregation of duties throughout the SDLC.

G 18.6 Acquirers are encouraged to deploy automated tools for software development, testing, software deployment, change management, code scanning and software version control to support more secure systems development.

G 18.7 Acquirers should consider the need for diversity[20] in technology to enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.

S 18.8 Acquirers shall establish a sound methodology for rigorous system testing prior to deployment. The testing shall ensure that the system meets user requirements and performs robustly. Where sensitive test data is used, acquirers shall ensure proper authorisation procedures and adequate measures to prevent their unauthorised disclosure are in place.

G 18.9 The scope of system testing referred to in paragraph 18.8 should include unit testing, integration testing, user acceptance testing, application security testing, stress and regression testing, and exception and negative testing, where applicable.

S 18.10 Acquirers shall ensure any changes to the source code of critical systems are subject to adequate source code reviews to ensure the code is secure and was developed in line with recognised coding practices prior to introducing any system changes.

S 18.11 In relation to IT systems that are developed and maintained by vendors, acquirers shall ensure the source code continues to be readily accessible and secured from unauthorised access.

S 18.12 Acquirers shall physically segregate the production environment from the development and testing environment for critical systems. Where acquirers are

[20] Diversity in technology may include the use of different technology architecture designs and applications, technology platforms and network infrastructure.

relying on a cloud environment, the acquirers shall ensure that these environments are not running on the same virtual host.

S 18.13 Acquirers shall establish appropriate procedures to independently review and approve system changes. The acquirers shall also establish and test contingency plans in the event of unsuccessful implementation of material changes to minimise any business disruption.

S 18.14 Where acquirers' IT systems are managed by third party service providers, the acquirers shall ensure, including through contractual obligations, that the third party service providers provide sufficient notice to the acquirers before any changes are undertaken that may impact the IT systems.

G 18.15 When decommissioning systems, acquirers should ensure minimal adverse impact on merchants and business operations. This includes establishing and testing contingency plans in the event of unsuccessful system decommissioning.

Cryptography

G 18.16 Acquirers should promote the adoption of strong cryptographic controls for protection of important data and information which include –

(a) the adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;

(b) the adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction;

(c) the periodic review, at least every three (3) years, of existing cryptographic standards and algorithms in IT systems, external linked or customer-facing applications to prevent exploitation of weakened algorithms or protocols; and

(d) the development and testing of compromise-recovery plans in the event of a cryptographic key compromise. This should set out the escalation process,

procedures for keys regeneration, interim measures, changes to business-as-usual protocols and containment strategies or options to minimise the impact of a compromise.

G 18.17 Acquirers should conduct due diligence and evaluate the cryptographic controls associated with the technology used in order to protect the confidentiality, integrity, authentication, authorisation and non-repudiation of information. Where acquirers do not generate their own encryption keys, the acquirers should undertake appropriate measures to ensure robust controls and processes are in place to manage encryption keys. Where this involves a reliance on third party assessment[21], the acquirers should consider whether such reliance is consistent with the acquirers' risk appetite and tolerance. Acquirers should also give due regard to the system resources required to support the cryptographic controls and the risk of reduced network traffic visibility of data that has been encrypted.

G 18.18 Acquirers should ensure cryptographic controls are based on the effective implementation of suitable cryptographic protocols. The protocols should include secret and public cryptographic key protocols, both of which should reflect a high degree of protection to the applicable secret or private cryptographic keys. The selection of such protocols should be based on recognised international standards and tested accordingly. Commensurate with the level of risk, secret cryptographic key and private-cryptographic key storage and encryption/decryption computation should be undertaken in a protected environment, supported by a hardware security module (HSM) or trusted execution environment (TEE).

G 18.19 Acquirers should store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated with customers should be issued by recognised certificate authorities. The acquirers should ensure that the implementation of authentication and signature protocols using such certificates are subject to strong protection to ensure that the

[21] For example, where the acquirers are not able to perform its own validation on embedded cryptographic controls due to the proprietary nature of the software or confidentiality constraints.

use of private cryptographic keys corresponding to the user certificates is legally binding and irrefutable. The initial issuance and subsequent renewal of such certificates should be consistent with industry best practices and applicable legal/regulatory specifications.

Data Centre Infrastructure

S 18.20 Acquirers shall ensure proper management of data centres and specify the resilience and availability objectives[22] of their data centres which are aligned with their business needs.

G 18.21 The network infrastructure should be designed to be resilient, secure and scalable. Potential data centre failures or disruptions should not significantly degrade the delivery of its financial services or impede its internal operations.

G 18.22 Acquirers should ensure production data centres are concurrently maintainable. This includes ensuring that production data centres have redundant capacity components and distribution paths serving the computer equipment.

G 18.23 In addition to paragraph 18.22, large acquirers are also encouraged to ensure recovery data centres are concurrently maintainable.

G 18.24 Acquirers should host IT systems in a dedicated space intended for production data centre usage. The dedicated space is to be physically secured from unauthorised access and is not located in a disaster-prone area. Acquirers should ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centres, including hardware components, electrical utility, thermal management and data centre infrastructure.

S 18.25 Acquirers shall establish proportionate controls, ensure adequate maintenance, and holistic and continuous monitoring of the critical components of the production

[22] Availability objectives refer to the level of availability of the data centre which is expected to be specified as an internal policy.

data centres aligned with the acquirer's risk appetite.

G 18.26 Acquirers are encouraged to appoint a technically competent external third party service provider to carry out a production data centre risk assessment and set proportionate controls aligned with the acquirers' risk appetite. The assessment should consider all major risks associated with the production data centre and to be conducted periodically or whenever there is a material change in the data centre infrastructure. The assessment should at a minimum, include a consideration of whether paragraphs 18.22 to 18.25 have been adopted. For data centres managed by third party service providers, acquirers may rely on independent third party assurance reports provided such reliance is consistent with the acquirers' risk appetite and tolerance, and the independent assurance has considered similar risks and meets the expectations in this paragraph for conducting the assessment. The designated board-level committee should deliberate the outcome of the assessment.

Data Centre Operations

S 18.27 Acquirers shall ensure their capacity needs are well-planned and managed with due regard to business growth plans. This includes ensuring adequate system storage, central processing unit (CPU) power, memory and network bandwidth.

G 18.28 Acquirers should involve both the technology stakeholders and the relevant business stakeholders within the acquirers in their development and implementation of capacity management plans.

S 18.29 Acquirers shall establish appropriate monitoring mechanisms to track capacity utilisation and performance of key processes and services[23]. These monitoring mechanisms shall be capable of providing timely and actionable alerts to administrators.

[23] For example, batch runs and backup processes for the acquirers' application systems and infrastructure.

S 18.30 Acquirers shall segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity[24]. In the case where vendors' or programmers' access to the production environment is necessary, these activities shall be properly authorised and monitored.

S 18.31 Acquirers shall establish adequate control procedures for their data centre operations. These control procedures shall include procedures for batch processing management to ensure timely and accurate batch processes, implementing changes in the production system, error handling, as well as, management of other exceptional conditions.

G 18.32 Acquirers are encouraged to undertake an independent risk assessment of their end-to-end backup storage and delivery management to ensure that existing controls are adequate in protecting sensitive data at all times.

S 18.33 Acquirers shall maintain a sufficient number of backup copies of critical data, the updated version of the operating system software, production programmes, system utilities, all master and transaction files and event logs for recovery purposes. Backup media shall be stored in an environmentally secure and access-controlled backup site.

G 18.34 In regard to paragraph 18.32 and 18.33, acquirers should also adopt the controls as specified in **Appendix 3** or their equivalent to secure the storage and transportation of sensitive data in removable media.

G 18.35 Where there is a reasonable expectation for immediate delivery of service, acquirers should ensure that the relevant critical systems are designed for high availability.

[24] For example, system development activities shall be segregated from data centre operations.

Network Resilience

G 18.36 Acquirers are encouraged to design a reliable, scalable and secure enterprise network that is able to support their business activities, including future growth plans.

G 18.37 Acquirers should ensure the network services for their critical systems are reliable and have no SPOF in order to protect the critical systems against potential network faults and cyber threats.

G 18.38 Acquirers should establish real-time network bandwidth monitoring processes and corresponding network service resilience metrics to flag any over utilisation of bandwidth and system disruptions due to bandwidth congestion and network faults. This includes traffic analysis to detect trends and anomalies.

S 18.39 Acquirers shall ensure network services supporting IT systems are designed and implemented to ensure the confidentiality, integrity and availability of data.

G 18.40 Acquirers should establish and maintain a network design blueprint identifying all of their internal and external network interfaces and connectivity. The blueprint should highlight both physical and logical connectivity between network components and network segmentations.

S 18.41 Acquirers shall ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three (3) years.

S 18.42 Acquirers shall implement appropriate safeguards to minimise the risk of a system compromise in one entity affecting other entities within the group. Safeguards implemented may include establishing logical network segmentation for the acquirers from other entities within the group.

G 18.43 Acquirers are encouraged to appoint a technically competent external third party service provider to carry out regular network risk assessment and set

proportionate controls aligned with its risk appetite. The assessment should be conducted periodically or whenever there is a material change in the network design. The assessment should consider all major risks and determine the current level of resilience.

Third Party Service Provider Management

S 18.44 In addition to the requirements in paragraph 14 on outsourcing arrangements, the acquirer shall fulfil the requirements under paragraphs 18.45 to 18.51 specifically for IT related third party service providers.

S 18.45 The board and senior management of the acquirers shall exercise effective oversight and address associated risks when engaging third party service providers for critical technology functions and systems. Engagement of third party service providers, including engagements for independent assessment, does not in any way reduce or eliminate the principal accountabilities and responsibilities of acquirers for the security and reliability of technology functions and systems.

S 18.46 Acquirers shall conduct proper due diligence on the third party service provider's competency, system infrastructure and financial viability as relevant prior to engaging its services. In addition, an assessment shall be made of the third party service providers' capabilities in managing the following specific risks –

(a) data leakage such as unauthorised disclosure of customer and counterparty information;
(b) service disruption including capacity performance;
(c) processing errors;
(d) physical security breaches;
(e) cyber threats;
(f) over-reliance on key personnel;
(g) mishandling of confidential information pertaining to the acquirers or its customers in the course of transmission, processing or storage of such information; and
(h) concentration risk.

S 18.47 At a minimum, the outsourcing agreements with the acquirers' third party service providers shall contain arrangements for disaster recovery and backup capability, where applicable, and IT system availability.

S 18.48 Acquirers shall ensure their ability to regularly review the outsourcing agreements with their third party service providers to take into account the latest security and technological developments in relation to the services provided.

S 18.49 Acquirers shall ensure data residing in third party service providers are recoverable in a timely manner. The acquirers shall ensure clearly defined arrangements with the third party service providers are in place to facilitate the acquirers' immediate notification and timely updates to the Bank and other relevant regulatory bodies in the event of a cyber-incident.

S 18.50 Acquirers shall ensure the storage of their data is at least logically segregated from the other clients of the third party service providers. There shall be proper controls over and periodic review of the access provided to authorised users.

S 18.51 Acquirers shall ensure IT system hosted by third party service providers have adequate recovery and resumption capability and provisions to facilitate an orderly exit in the event of failure or unsatisfactory performance by the third party service providers.

Cloud Services

S 18.52 Acquirers shall fully understand the inherent risk of adopting cloud services. In this regard, acquirers are required to conduct a comprehensive risk assessment prior to cloud adoption which considers the inherent architecture of cloud services that leverage on the sharing of resources and services across multiple tenants over the Internet. The assessment shall specifically address risks associated with the following –

(a) sophistication of the deployment model;

(b) migration of existing systems to cloud infrastructure;

(c) location of cloud infrastructure;

(d) multi-tenancy or data co-mingling;

(e) vendor lock-in and application portability or interoperability;

(f) ability to customise security configurations of the cloud infrastructure to ensure a high level of data and technology system protection;

(g) exposure to cyber-attacks via cloud service providers;

(h) termination of a cloud service provider including the ability to secure the acquirers' data following the termination;

(i) demarcation of responsibilities, limitations and liability of the cloud service providers; and

(j) ability to meet regulatory requirements and international standards on cloud computing on a continuing basis.

S 18.53 The risk assessment as outlined in paragraph 18.52 shall be documented and made available for the Bank's review as and when requested by the Bank.

S 18.54 Acquirers shall demonstrate that specific risks associated with the use of cloud services for IT systems have been adequately considered and addressed. The risk assessment shall address the risks outlined in paragraph 18.52, as well as, the following areas –

(a) the adequacy of the over-arching cloud adoption strategy of the acquirers including –

(i) board oversight over cloud strategy and cloud operational management;

(ii) senior management roles and responsibilities on cloud management;

(iii) conduct of day-to-day operational management functions;

(iv) management and oversight by the acquirers of cloud service providers;

(v) quality of risk management and internal control functions; and

(vi) strength of in-house competency and experience.

(b) the availability of independent, internationally recognised certifications of the cloud service providers, at a minimum, in the following areas –

(i) information security management framework, including cryptographic modules such as used for encryption and decryption of user data; and

(ii) cloud-specific security controls for protection of customer and counterparty or proprietary information including payment transaction data in use, in storage and in transit;

(c) the degree to which the selected cloud configuration adequately addresses the following attributes –

(i) geographical redundancy;

(ii) high availability;

(iii) scalability;

(iv) portability;

(v) interoperability; and

(vi) strong recovery and resumption capability including appropriate alternate Internet path to protect against potential Internet faults.

G 18.55 Acquirers should consider the need for a third party pre-implementation review on cloud implementation that also covers the areas set out in paragraph 18.54.

S 18.56 Acquirers shall implement appropriate safeguards on customer and counterparty information and proprietary data when using cloud services to protect against unauthorised disclosure and access. This shall include retaining ownership, control and management of all data pertaining to customer and counterparty information, proprietary data and services hosted on the cloud, including the relevant cryptographic keys management.

Access Control

S 18.57 Acquirers shall implement an appropriate access control policy for the identification, authentication and authorisation of users (internal and external users such as third party service providers). This shall address both logical and physical technology access controls, which are commensurate with the level of risk of unauthorised access to its technology systems.

G 18.58 In observing paragraph 18.57, acquirers should consider the following in accessing the control policy –

(a) adopt a "deny all" access control policy for users by default unless explicitly authorised;

(b) employ "least privilege" access rights or on a "need-to-have" basis where only the minimum sufficient permissions are granted to legitimate users to perform their roles;

(c) employ time-bound access rights which restrict access to a specific period including access rights granted to third party service providers;

(d) employ segregation of incompatible functions to ensure that no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features. This may include a combination of functions such as –

(i) system development and technology operations;

(ii) security administration and system administration; and

(iii) network operation and network security;

(e) employ dual control functions which require two or more persons to execute an activity;

(f) adopt stronger authentication for critical activities including for remote access;

(g) limit and control the use of the same user ID for multiple concurrent sessions;

(h) limit and control the sharing of user ID and passwords across multiple users; and

(i) control the use of generic user ID naming conventions in favour of more personally identifiable IDs.

S 18.59 Acquirers shall employ robust authentication processes to ensure the authenticity of identities in use. Authentication mechanisms shall commensurate with the criticality of the functions and adopt at least one or more of these three (3) basic authentication factors, namely, something the user knows (e.g. password, PIN), something the user possesses (e.g. smart card, security device) and something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).

G 18.60 Authentication methods that depend on more than one factor typically are more difficult to compromise than a single factor system. In view of this, acquirers are encouraged to properly design and implement (especially in high-risk or 'single sign-on' systems) multi-factor authentication (MFA) that is more reliable and provide stronger fraud deterrents.

S 18.61 Acquirers shall periodically review and adapt their password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords. There shall be appropriate controls in place to check the strength of the passwords created.

G 18.62 Acquirers are encouraged to adopt dedicated user domains for selected critical functions, separate from the broader enterprise-wide user authentication system.

S 18.63 Acquirers shall establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix shall be periodically reviewed and updated.

S 18.64 Acquirers shall ensure the following —

(a) access controls to enterprise-wide systems are effectively managed and monitored; and

(b) user activities in IT systems are logged for audit and investigations. Activity logs shall be maintained for at least three (3) years and regularly reviewed in a timely manner.

G 18.65 In fulfilling the requirement under paragraph 18.64, large acquirers are encouraged to –

(a) deploy an identity access management system to effectively manage and monitor user access to enterprise-wide systems; and

(b) deploy automated audit tools to flag any anomalies.

Patch and End-of-Life System Management

S 18.66 Acquirers shall ensure that the IT systems are not running on outdated systems with known security vulnerabilities or end-of-life (EOL) technology systems. In this regard, the acquirers shall clearly assign responsibilities to identified functions –

(a) to continuously monitor and implement latest patch releases in a timely manner; and

(b) identify critical technology systems that are approaching EOL for further remedial action.

G 18.67 Acquirers should establish a patch and EOL management framework which addresses among others the following requirements –

(a) identification and risk assessment of all technology assets for potential vulnerabilities arising from undeployed patches or EOL systems;

(b) conduct of compatibility testing for critical patches;

(c) specification of turnaround time for deploying patches according to the severity of the patches; and

(d) adherence to the workflow for end-to-end patch deployment processes including approval, monitoring and tracking of activities.

Security of Digital Services

S 18.68 Acquirers shall implement robust technology security controls in providing digital services which assure the following –

(a) confidentiality and integrity of customer and counterparty information and transactions;

(b) reliability of services delivered via channels and devices with minimum disruption to services;

(c) proper authentication of users or devices and authorisation of transactions;

(d) sufficient audit trail and monitoring of anomalous transactions;

(e) ability to identify and revert to the recovery point prior to incident or service disruption; and

(f) strong physical control and logical control measures.

G 18.69 Acquirers should implement controls to authenticate and monitor all financial transactions. These controls, at a minimum, should be effective in mitigating man-in-the-middle attacks, transaction fraud, phishing and compromise of application systems and information. Acquirers should deploy MFA technology and channels that are more secure than unencrypted short messaging service (SMS).

S 18.70 Acquirers shall ensure sufficient and relevant digital service logs are retained for investigations and forensic purposes for at least three (3) years.

G 18.71 Acquirers should ensure that the use of more advanced technology to authenticate and deliver digital services such as biometrics, tokenisation and contactless communication[25] comply with internationally recognised standards where available. The technology should be resilient against cyber threats[26] including malware, phishing or data leakage.

G 18.72 Acquirers should undertake a comprehensive risk assessment of the advanced technologies and the algorithms deployed in its digital services. Algorithms should be regularly reviewed and validated to ensure they remain appropriate and accurate. Where third party software is used, acquirers may rely on relevant independent reports provided that such reliance is consistent with the acquirers' risk appetite and tolerance, and the nature of digital services provided by the acquirers which leverage on the technologies and algorithms.

[25] Such as QR code, Bar Code, Near Field Communication (NFC), Radio Frequency Identification (RFID).

[26] For example, in respect of QR payments, acquirers shall implement safeguards within its respective mobile applications to detect and mitigate risks relating to QR code that may contain malware or links to phishing websites.

G 18.73 Acquirers should ensure authentication processes using biometric technology are secure, highly resistant to spoofing and have a minimal false acceptance rate to ensure confidentiality, integrity and non-repudiation of transactions.

G 18.74 Acquirers should perform continuous surveillance to assess the vulnerability of the operating system and the relevant technology platform used for its digital delivery channels to security breaches and implement appropriate corresponding safeguards. At a minimum, acquirers should implement sufficient logical and physical safeguards for the following channels/devices –

(a) payment acceptance device;
(b) QR code;
(c) Internet application; and
(d) mobile application and devices.

In view of the evolving threat landscape, these safeguards should be continuously reviewed and updated to protect against fraud and to secure the confidentiality and integrity of customer and counterparty information and transactions.

G 18.75 With respect to paragraph 18.74, acquirers should adopt the controls specified in the following Appendices for the respective digital delivery channel –

(a) **Appendix 4**: Control Measures on Payment Acceptance Device;
(b) **Appendix 5**: Control Measures on Internet Application;
(c) **Appendix 6**: Control Measures on Mobile Application and Devices; and
(d) **Appendix 7**: Control Measures on Quick Response Code.

19. Cybersecurity Management

Cyber Risk Management

G 19.1 Acquirers should ensure that there is an enterprise-wide focus on effective cyber risk management to reflect the collective responsibility of business and technology lines for managing cyber risks.

S 19.2 Acquirers shall develop a Cyber Resilience Framework (CRF), which articulates the acquirers' governance for managing cyber risks, its cyber resilience objectives and

its risk tolerance, with due regard to the evolving cyber threat environment. Objectives of the CRF includes ensuring operational resilience against extreme but plausible cyber-attacks.

G 19.3 The CRF should be able to support the effective identification, protection, detection, response, and recovery (IPDRR) of systems and data hosted on-premise or by third party service providers from internal and external cyber-attacks. The CRF should consist of, at a minimum, the following elements –

(a) development of an institutional understanding of the overall cyber risk context in relation to the acquirers' businesses and operations, their exposure to cyber risks and current cybersecurity posture;

(b) identification, classification and prioritisation of critical systems, information, assets and interconnectivity (with internal and external parties) to obtain a complete and accurate view of the acquirers' information assets, critical systems, interdependencies and cyber risk profile;

(c) identification of cybersecurity threats and countermeasures including measures to contain reputational damage that can undermine confidence in the acquirers;

(d) layered (defense-in-depth) security controls to protect data, infrastructure and assets against evolving threats;

(e) timely detection of cybersecurity incidents through continuous surveillance and monitoring;

(f) detailed incident handling policies and procedures and a crisis response management playbook to support the swift recovery from cyber-incidents and contain any damage resulting from a cybersecurity breach; and

(g) policies and procedures for timely and secure information sharing and collaboration with other acquirers and participants in financial market infrastructure to strengthen cyber resilience.

G 19.4 In addition to the elements provided in paragraph 19.3 above, large acquirers are encouraged to —

(a) implement a centralised automated tracking system to manage their technology asset inventory; and

(b) establish a dedicated in-house cyber risk management function to manage cyber risks or emerging cyber threats. The cyber risk management function should be responsible for the following –

(i) perform detailed analysis on cyber threats, provide risk assessment on potential cyber-attacks and ensure timely review and escalation of all high-risk cyber threats to the board and senior management; and

(ii) proactively identify potential vulnerabilities including those arising from infrastructure hosted with third party service providers through the simulation of sophisticated "Red Team" attacks on their current security controls.

Cybersecurity Operations

G 19.5 Acquirers should establish clear responsibilities for cybersecurity operations which should include implementing appropriate mitigating measures in the acquirers' conduct of business that correspond to the following phases of the cyber-attack lifecycle –

(a) reconnaissance;

(b) weaponisation;

(c) delivery;

(d) exploitation;

(e) installation;

(f) command and control; and

(g) exfiltration.

G 19.6 Where relevant, acquirers should adopt the control measures on cybersecurity as specified in **Appendix 8** to enhance its resilience to cyber-attacks.

G 19.7 Acquirers are encouraged to deploy effective tools to support the continuous and proactive monitoring and timely detection of anomalous activities in its technology

infrastructure. The scope of monitoring should cover all critical systems including the supporting infrastructure.

S 19.8 Acquirers shall ensure that their cybersecurity operations continuously prevent and detect any potential compromise of their security controls or weakening of their security posture. For large acquirers, this shall include performing a quarterly vulnerability assessment of external and internal network components that support all critical systems.

S 19.9 Acquirers shall conduct annual penetration tests on their internal and external network infrastructure as well as IT systems including web, mobile and all external-facing applications. The penetration testing shall reflect extreme but plausible cyber-attack scenarios based on emerging and evolving threat scenarios. Acquirers shall engage suitably accredited penetration testers and third party service providers to perform this function.

G 19.10 In addition to the requirement in paragraph 19.9 above, large acquirers are encouraged to undertake independent compromise assessment on the technology infrastructure of their critical systems at least annually and ensure the results of such assessment are escalated to the board and senior management in a timely manner.

S 19.11 Acquirers shall establish standard operating procedures (SOP) for vulnerability assessment and penetration testing (VAPT) activities. The SOP shall outline the relevant control measures including ensuring the external penetration testers are accompanied on-premises at all times, validating the event logs and ensuring data purging.

S 19.12 Acquirers shall ensure the outcome of the penetration testing exercise is properly documented and escalated in a timely manner to senior management to identify and monitor the implementation of relevant remedial actions.

Distributed Denial of Service (DDoS)

G 19.13 Acquirers should ensure their technology systems and infrastructure, including IT systems outsourced to or hosted by third party service providers, are adequately protected against all types of DDoS attacks (including volumetric, protocol and application layer attacks) through the following measures –

(a) subscribing to DDoS mitigation services, which include automatic "clean pipe" services to filter and divert any potential malicious traffic away from the network bandwidth;

(b) regularly assessing the capability of the service third party service provider to expand network bandwidth on-demand including upstream third party service provider capability, adequacy of the third party service provider's incident response plan and its responsiveness to an attack; and

(c) implementing mechanisms to mitigate against Domain Name Server (DNS) based layer attacks.

Data Loss Prevention (DLP)

G 19.14 Acquirers should establish a clear DLP strategy and processes in order to ensure that proprietary and customer and counterparty information is identified, classified and secured. At a minimum, acquirers should –

(a) ensure that data owners are accountable and responsible for identifying and appropriately classifying data;

(b) undertake a data discovery process prior to the development of a data classification scheme and data inventory; and

(c) ensure that data accessible by third parties is clearly identified and policies should be implemented to safeguard and control third party access. This includes having in place adequate contractual agreements to protect the interests of the acquirers and their customers.

G 19.15 Acquirers should design internal control procedures and implement appropriate technology in all applications and access points to enforce DLP policies and trigger any policy violations. The technology deployed should cover the following –

(a) data in-use – data being processed by IT resources;

(b) data in-motion – data being transmitted on the network; and

(c) data at-rest – data stored in storage mediums such as servers, backup media and databases.

G 19.16 Acquirers should implement appropriate policies for the removal of data on technology equipment, mobile devices or storage media to prevent unauthorised access to data.

Security Operations Centre (SOC)

S 19.17 Acquirers shall ensure their SOC, whether managed in-house or by third party service providers, has adequate capabilities for proactive monitoring of its technology security posture. This shall enable the acquirers to detect anomalous user or network activities, flag potential breaches and establish the appropriate response supported by skilled resources based on the level of complexity of the alerts. The outcome of the SOC activities shall also inform the acquirers' reviews of its cybersecurity posture and strategy.

G 19.18 The SOC should be able to perform the following functions –

(a) log collection and the implementation of an event correlation engine with parameter-driven use cases such as Security Information and Event Management (SIEM);

(b) incident coordination and response;

(c) vulnerability management;

(d) threat hunting;

(e) remediation functions including the ability to perform forensic artifact handling, malware and implant analysis; and

(f) provision of situational awareness to detect adversaries and threats including threat intelligence analysis and operations, and monitoring indicators of compromise (IOC). This includes advanced behavioural analysis to detect signature-less and file-less malware and to identify anomalies that may pose security threats including at endpoints and network layers.

G 19.19 Acquirers should ensure that the SOC provides a regular threat assessment report, which should include, at a minimum, the following –

(a) trends and statistics of cyber events and incidents categorised by type of attacks, target and source IP addresses, location of data centres and criticality of applications; and

(b) intelligence on emerging and potential threats including tactics, techniques and procedures (TTP).

For large acquirers, such reports should be provided on a monthly basis.

G 19.20 Acquirers are encouraged to subscribe to reputable threat intelligence services to identify emerging cyber threats, uncover new cyber-attack techniques and support the implementation of countermeasures.

S 19.21 Acquirers shall ensure the following –

(a) the SOC is located in a physically secure environment with proper access controls; and

(b) the SOC operates on a 24x7 basis with disaster recovery capability to ensure continuous availability.

Cyber Response and Recovery

S 19.22 Acquirers shall establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the organisation's overall crisis management plan, escalation processes, business continuity and disaster recovery planning. This includes developing a clear communication plan for engaging shareholders, regulatory authorities, customers and employees in the event of a cyber-incident.

G 19.23 Acquirers should establish and implement a comprehensive Cyber Incident Response Plan (CIRP). The CIRP shall address the following –

(a) Preparedness: Establish a clear governance process, reporting structure and roles and responsibilities of the Cyber Emergency Response Team (CERT) as well as invocation and escalation procedures in the event of an incident;

(b) Detection and analysis: Ensure effective and expedient processes for identifying points of compromise, assessing the extent of damage and preserving sufficient evidence for forensics purposes;

(c) Containment, eradication and recovery: Identify and implement remedial actions to prevent or minimise damage to the acquirers, remove the known threats and resume business activities; and

(d) Post-incident activity: Conduct post-incident review incorporating lessons learned and develop long-term risk mitigations.

G 19.24 Acquirers should conduct an annual cyber drill exercise to test the effectiveness of their CIRP, based on various current and emerging threat scenarios (e.g. social engineering), with the involvement of key stakeholders including members of the board, senior management and relevant third party service providers. The test scenarios should include scenarios designed to test –

(a) the effectiveness of escalation, communication and decision-making processes that correspond to different impact levels of a cyber-incident; and

(b) the readiness and effectiveness of CERT and relevant third party service providers in supporting the recovery process.

S 19.25 Acquirers shall immediately notify the Bank of any cyber-incidents affecting the institution. Upon completion of the investigation, the acquirers are also required to submit a report on the incident to the Bank.

G 19.26 Acquirers are strongly encouraged to collaborate and cooperate closely with relevant stakeholders and competent authorities in combating cyber threats and sharing threat intelligence and mitigation measures.

20. Technology Audit

S 20.1 Acquirers shall ensure that the scope, frequency and intensity of technology audits are commensurate with the complexity, sophistication and criticality of technology systems and applications.

S 20.2 The audit function shall be adequately resourced with relevant technology audit competencies and sound knowledge of the acquirers' technology processes and operations.

G 20.3 Acquirers should ensure their technology audit staff are adequately conversant with the developing sophistication of the acquirers' technology systems and delivery channels.

G 20.4 In addition to paragraph 20.2, large acquirers are expected to establish a dedicated technology audit function that has specialised technology audit competencies to undertake technology audits.

S 20.5 Acquirers shall establish a technology audit plan that provides appropriate coverage of critical technology services, third party service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post-implementation reviews of new or material enhancements of technology services.

G 20.6 The audit function (in the case of paragraph 20.2) and the dedicated technology audit function (in the case of paragraph 20.4) may be enlisted to provide advice on compliance with and adequacy of control processes during the planning and development phases of new major products, systems or technology operations. In such cases, the technology auditors participating in this capacity should carefully consider whether such an advisory or consulting role would materially impair their independence or objectivity in performing post-implementation reviews of the products, systems and operations concerned.

21. Internal Awareness and Training

S 21.1 Acquirers shall provide adequate and regular technology and cybersecurity awareness education for all staff in undertaking their respective roles and measure the effectiveness of its education and awareness programmes. This cybersecurity awareness education shall be conducted at least annually by the acquirers and shall reflect the current cyber threat landscape.

G 21.2 Acquirers should provide adequate and continuous training for staff involved in technology operations, cybersecurity and risk management in order to ensure that the staff are competent to effectively perform their roles and responsibilities.

G 21.3 Acquirers should provide their board members with regular training and information on technology developments to enable the board to effectively discharge its oversight role.

PART E OTHER REQUIREMENTS

22. Other Compliance Requirements

S 22.1 Newly registered acquirers shall conduct a post-implementation review no later than six (6) months after the implementation of the acceptance of payment instruments. The review shall include the identification of issues, gaps, fraud incidents and implementation of action plans to resolve any shortcomings identified.

S 22.2 Acquirers shall notify the Bank in writing, to the Director of the department in charge of oversight/supervision of payment services on the following –

(a) any proposed changes to their merchant acquiring services model which are significant or changes the risk profile of the business model, which includes but is not limited to any changes in target market, mode of payment acceptance, as well as, payment and settlement flow, by providing the details within thirty (30) days prior to the effective date of the proposed changes; and

(b) any change in average MTV that would cause changes from recognition as a small to large acquirer or vice-versa, not more than sixty (60) days from such occurrence.

S 22.3 Acquirers shall submit the following to the Bank –

(a) its annual audited financial statements not later than three (3) months after its financial year end in writing to the Director of the department in charge of oversight/supervision of payment services;

(b) segmented financial reporting for merchant acquiring services only[27] on a quarterly basis;

(c) statistical report on the operation of its merchant acquiring services on a quarterly basis; and

(d) any other information as required by the Bank.

S 22.4 The information required in paragraphs 22.3(b) and (c) shall be submitted to STATsmart Integrated Submission Portal on the 20th day of the following month.

[27] Based on at least the acquirer's management account and covering the acquirer's merchant acquiring services only, if the acquirer also conducts other business activities.

Appendix 1 COMPUTATION OF MINIMUM CAPITAL FUNDS

Share capital *which includes:*

- Paid-up ordinary shares/common stock
- Paid-up irredeemable non-cumulative preference shares

plus **Reserves** *which includes:*

- Share premium
- General reserve fund

less **Intangible Assets**[28]

plus **Retained Profit** (or *less* **Accumulated Losses)**

plus **Audited Profit for the period** (or *less* **Unaudited Loss for the period)**

[28] Including goodwill, capitalised development costs, licenses and intellectual properties.

Appendix 2 MINIMUM REQUIREMENTS ON THE OUTSOURCING AGREEMENT

The outsourcing agreement shall, at a minimum, provide for the following –

(a) clearly defined roles and responsibilities as well as obligations of the service provider;

(b) provisions to ensure that the service provider ensures security and confidentiality of information shared with the service provider at all times, including –
   (i) responsibilities of the service provider with respect to information security and confidentiality as well as scope of such information;
   (ii) for the service provider to be bound by confidentiality provisions stipulated under the contract even after the engagement has ended;
   (iii) for the service provider to maintain compliance with applicable security requirements and established security standards (e.g. Payment Card Industry Data Security Standard (PCI DSS)) at all times;
   (iv) provisions on corresponding liability obligations arising from a security breach attributable to the service provider; and
   (v) notification requirements in the event of a security breach;

(c) clear provisions on access rights for the Bank or any party appointed by the Bank to examine or conduct audit on the activity conducted by the service provider or its sub-contractor for the acquirer. This shall include access to any system, record, information or data related to the acquirer, as well as rights to enter the premises of the service provider or its sub-contractor to conduct such examination or investigation;

(d) continuous and complete access by the acquirer to its data held by the service provider in the event of a dispute with the service provider, or termination of the arrangement;

(e) ability of the acquirer and its external auditor 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;

(f) dispute resolution process in the event of default or non-performance of obligations, including remedies and indemnities where relevant;

(g) 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;

(h) conditions under which the outsourcing arrangement may be terminated, with sufficient time for an orderly transfer of the outsourced activity to the acquirer or another party;

(i) allow the acquirer the right to modify or terminate the arrangement when the Bank issues a direction to the acquirer to that effect under the FSA; and

(j) where relevant, terms governing the ability of the service provider to sub-contract to other parties, which will not dilute the accountability of the service provider.

The terms must include requirement for the sub-contractor to be bound by information confidentiality provisions even after the arrangement has ceased.

Appendix 3 STORAGE AND TRANSPORTATION OF SENSITIVE DATA IN REMOVABLE MEDIA

Acquirers should ensure adequate controls and measures are implemented for the storage and transportation of sensitive data in removable media, including –

1) Deploying the industry-tested and accepted encryption techniques;

2) Implementing authorised access control to sensitive data (e.g. password protection, user access matrix);

3) Prohibiting unauthorised copying and reading from the media;

4) Shall there be a need to transport the removable media to a different physical location, acquirers should —
   (a) strengthen the chain of custody process for media management which includes –
      (i) the media must not be under single custody at any point of time;
      (ii) the media must always be within sight of the designated custodians; and
      (iii) the media must be delivered to its target destination without unscheduled stops or detours;
   (b) use secure and official vehicle for transportation; and
   (c) use strong and tamper-proof containers for storing the media with high-security lock (e.g. dual key and combination lock);

5) Ensuring third party service providers comply with the requirements in paragraphs 1 to 4 of this **Appendix 3**, in the event third party services are required in undertaking the storage management or transportation process of sensitive data in removable media.

Appendix 4 CONTROL MEASURES ON PAYMENT ACCEPTANCE DEVICE

1) Acquirers should ensure all relevant risks associated to the use of merchant's payment acceptance device are mitigated, including but not limited to the following -

   (a) ensuring the payment acceptance devices are –
      (i) adequately hardened and securely configured using methods that ensure its integrity and authenticity;
      (ii) protected from tampering and cyber threats such as malware attacks, key logger, and etc;
      (iii) designed for the protection of PIN data;
      (iv) certified to be fully compliant with applicable security standards, e.g. PCI PIN Transaction Security (PCI PTS), Software-based PIN Entry on COTS (PCI SPoC), etc.; and
      (v) used solely as the payment acceptance device.
   (b) ensuring PIN entry process and cardholder verification method (CVM) applications are secured and protected against manipulation or sabotage;
   (c) providing guidance for merchants to ensure the PIN is entered in a way that it cannot be observed by an unauthorised party;
   (d) PIN data must be encrypted upon entry and remain encrypted when transmitted to protect against malicious activity and attacks;
   (e) ensuring data is protected at all times to prevent data leakage and no data is stored on the payment acceptance devices;
   (f) ensuring only dedicated merchant staff are allowed to perform system administration functions (e.g. performing correction) of the payment acceptance device; and
   (g) for PIN Entry on COTS –
      (i) ensuring PIN CVM applications run only on secured and supported versions of operating systems which have not been compromised, jailbroken or rooted i.e. the security patches are up-to-date; and
      (ii) use of automated monitoring and attestation system to detect potential compromise of payment acceptance devices and ensuring that all components in the payment acceptance devices are always in a secure state.

Appendix 5 CONTROL MEASURES ON INTERNET APPLICATION

1) Acquirers should ensure the adequacy of security controls implemented for Internet application, which include –

   (a) ensuring Internet application only runs on secured versions of web browsers that have continued developer support for security patches to fix any vulnerabilities; and

   (b) putting in place additional authentication protocols to enable customers to identify the acquirers' genuine websites.

Appendix 6 CONTROL MEASURES ON MOBILE APPLICATION AND DEVICES

1) Acquirers should ensure digital payment services involving sensitive customer and counterparty information offered via mobile devices are adequately secured. This includes the following –
   (a) ensuring mobile applications run only on the supported version of operating systems and enforce the application to only operate on a secure version of operating systems which have not been compromised, jailbroken or rooted (i.e. the security patches are up-to-date);
   (b) designing the mobile application to operate in a secure and tamper-proof environment within the mobile devices. The mobile application shall be prohibited from storing customer and counterparty information used for authentication with the application server such as PIN and passwords. Authentication and verification of unique key and PIN shall be centralised at the host;
   (c) undertaking proper due diligence processes to ensure the application distribution platforms used to distribute the mobile application are reputable;
   (d) ensuring proper controls are in place to access, maintain and upload the mobile application on application distribution platforms;
   (e) activation of the mobile application must be subject to authentication by the acquirers;
   (f) ensuring secure provisioning process of mobile application in the user's device is in place by binding the mobile application to the user's profile such as device ID and account number; and
   (g) monitoring the application distribution platforms to identify and address the distribution of fake applications in a timely manner.

2) In addition to the guidance above, acquirers should also ensure the following measures are applied specifically for applications running on mobile devices used by the acquirers, appointed parties or intermediaries for the purpose of processing customer and counterparty information -
   (a) mobile device to be adequately hardened and secured;
   (b) ensure the capability to automatically wipe data stored in the mobile devices in the event the device is reported stolen or missing; and
   (c) establish safeguards that ensure the security of customer and counterparty information (e.g. Primary Account Numbers (PAN), Card Verification Value Numbers (CVV), expiry dates and Personal Identification Numbers (PIN) of payment cards), including to mitigate risks of identity theft and fraud[29].

[29] This includes risks associated with malwares that enable keystroke logging, PIN harvesting and other malicious forms of customer and counterparty information downloading.

Appendix 7 CONTROL MEASURES ON QUICK RESPONSE CODE

1) Ensure QR code authenticity which among others include –
   (a) QR codes are securely generated by host server, unique for each merchant/user/transaction, where dynamic QR codes should have reasonable expiry time;
   (b) block QR code application from operating on unsecured (e.g. rooted or jail-broken) devices;
   (c) any fake QR code shall be rejected upfront and the merchant/user shall be automatically notified of the authenticity of the scanned QR code; and
   (d) bind the QR code to the respective user or merchant ID and transaction amount.

2) Ensure QR codes do not contain any confidential data and are not stored in endpoint devices.

3) Ensure all relevant risks associated with the use of static QR codes at participating merchants are mitigated, including but not limited to the following –
   (a) all information from the scanned QR codes shall be transmitted to payment instrument's host server for authentication;
   (b) educate merchants on fraud risk related to static QR codes and the preventive measures to effectively mitigate such risk (e.g. merchants shall regularly inspect the displayed static QR code to ensure it has not been tampered with); and
   (c) enforce masking of sensitive customer and counterparty information when displayed on mobile devices.

Appendix 8 CONTROL MEASURES ON CYBERSECURITY

1) Conduct periodic review on the configuration and rules settings for all security devices. Use automated tools to review and monitor changes to configuration and rules settings.

2) Update checklists on the latest security hardening of operating systems.

3) Update security standards and protocols for web services encryption regularly. Disable support of weak ciphers and protocol in web-facing applications.

4) Ensure technology networks including mobile and wireless networks are segregated into multiple zones according to threat profile. Each zone shall be adequately protected by various security devices including firewall and Intrusion Prevention System (IPS).

5) Ensure security controls for server-to-server external network connections include the following –

   (a) server-to-server authentication such as Public Key Infrastructure (PKI) certificate or user ID and password;
   (b) use of secure tunnels such as Transport Layer Security (TLS) and Virtual Private Network (VPN) IPSec; and
   (c) deploying staging servers with adequate perimeter defences and protection such as firewall, IPS and antivirus.

6) Ensure security controls for remote access to server include the following –

   (a) restrict access to only hardened and locked down end-point devices;
   (b) use secure tunnels such as TLS and VPN IPSec;
   (c) deploy “gateway” server with adequate perimeter defences and protection such as firewall, IPS and antivirus; and
   (d) close relevant ports immediately upon expiry of remote access.

7) Ensure overall network security controls are implemented including the following –

   (a) dedicated firewalls at all segments. All external-facing firewalls must be deployed on High Availability (HA) configuration and “fail-close” mode activated. Deploy different brand name/model for two firewalls located in sequence within the same network path;
   (b) IPS at all critical network segments with the capability to inspect and monitor encrypted network traffic;
   (c) web and email filtering systems such as web-proxy, spam filter and anti-spoofing controls;
   (d) end-point protection solution to detect and remove security threats including viruses and malicious software;
   (e) solution to mitigate advanced persistent threats including zero-day and signatureless malware; and

(f) capture the full network packets to rebuild relevant network sessions to aid forensics in the event of incidents.

8) Synchronise and protect the Network Time Protocol (NTP) server against tampering.

Appendix 9 EXAMPLES OF ARRANGEMENTS EXCLUDED FROM OUTSOURCING SCOPE

For the purpose of paragraph 14, arrangements which entail procurement of services[30], 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 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) agent banking;

(g) trustee arrangement;

(h) credit or market information services;

(i) repair, support and maintenance of tangible asset;

(j) purchase or subscription of commercially available software;

(k) maintenance and support of licensed software;

(l) marketing and advertising;

(m) telecommunication, postal and courier service;

(n) physical security, premise access and guarding services; and

(o) catering, cleaning and event services.

[30] Where an acquirer acquires services, goods or utilities, which are not expected to be performed by the acquirer.