Merchant Acquiring Services
Exposure Draft

Applicable to:
Registered merchant acquirers

Issued on: 17 July 2020
This exposure draft sets out Bank Negara Malaysia (the Bank)’s proposed requirements and expectations on merchant acquirers registered pursuant to section 18(1) of the Financial Services Act 2013 which fulfil the criteria as set out under paragraph 2.1 of this exposure draft.

The Bank invites written comments on the proposals in this exposure draft, including suggestions for particular issues, areas for clarification and any alternative proposals that the Bank should consider. To facilitate the Bank’s assessment, please support each comment with a clear rationale, accompanying evidence or illustration, as appropriate. In addition to providing general feedback, respondents are requested to respond to the specific questions set out in this exposure draft.

Responses must be submitted by **1 September 2020** to:

Pengarah
Jabatan Pemantauan Pembayaran
Bank Negara Malaysia
Jalan Dato’ Onn
50480 Kuala Lumpur
Email: pdpolicy@bnm.gov.my

Electronic submission is encouraged. Feedback received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

In the course of providing your feedback, you may direct any queries to the following officers at 03-26988044 ext. number -

1. Suriana Jumali (ext. 8161 or e-mail suriana@bnm.gov.my) ;or
2. Ummairah Nadhirah (ext. 8594 or e-mail ummairah@bnm.gov.my)
| Appendix 7 | CONTROL MEASURES ON INTERNET APPLICATION .................................................. 70 |
| Appendix 8 | CONTROL MEASURES ON MOBILE APPLICATION AND DEVICES .................................... 71 |
| Appendix 9 | CONTROL MEASURES ON QR CODE ........................................................................... 72 |
| Appendix 10 | CONTROL MEASURES ON CYBERSECURITY ................................................................. 73 |
PART A  OVERVIEW

1. Introduction

1.1 In tandem with the rapid changes in the 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 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 online merchants such as master merchants, Small and Medium Enterprise (SME) merchants and appointed third party acquirers/ payment facilitators to facilitate expansion and such arrangements involve constantly evolving technological advancements. All of the above increase the complexity and the number of players along the payment chain before payment reaches the ultimate merchants.

1.2 Based on the above, it is timely for the Bank to provide greater clarity and specify the regulatory requirements for merchant acquiring services. This is important to ensure proper risk management in merchant acquiring services, such as the management of settlement risk, financial risk, technology and cyber risk, fraud risk and Money Laundering/ Terrorism Financing (ML/TF) risk, in order to secure payment transactions and increase confidence in the use of e-payments.

1.3 The objectives of this policy document are as follows –

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

(b) to preserve users’ and merchants’ confidence in using or accepting payment instruments for the payment of goods and services.
2. Applicability

2.1 This policy document is applicable to registered merchant acquirers pursuant to section 18(1) of the Financial Services Act 2013 (FSA) which fulfil the following criteria (acquirer):

(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 Notwithstanding paragraph 2.1, paragraph 11 is applicable only for non-bank merchant acquirer.

Question 1:

i) Please provide your views on the criteria specified in paragraph 2.1 and the impact to your institution, if any.

ii) The criteria would cause third party acquirers/ payment facilitators to be scoped out from the requirements in this policy document. Therefore, current third party acquirers/ payment facilitators will not be within the purview of FSA, although still allowed to conduct their business. Please provide your views on this impact.

3. Legal provisions

3.1 The requirements in this policy document are specified pursuant to sections 18(2), 33(1), 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 the issuance of the final policy document.

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 purpose 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 actions;

- **“G”** denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendation that are encouraged to be adopted;

- **“acquirer”** means any person who has been registered by the Bank pursuant to section 18(1) 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 merchant acquirer’s provision of services to customers or counterparties, business operations, financial position, reputation or compliance with applicable laws and regulatory requirements;
“contracted merchant” refers to merchants that are acquired by a third party acquirer/ payment facilitator and/ or merchants that sell their goods and services via a master merchant’s marketplace;

“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” means a principal member of a payment instrument network(s) that provides merchant acquiring services. The principal member may appoint a payment facilitator to perform merchant acquiring services;

“e-commerce merchants” refer to merchants that sell goods or services electronically over the Internet or any other channels not involving face-to-face interaction (e.g. online merchants, mail or telephone order);

“foreign-issued payment instrument” means a payment instrument issued by an issuer not locally incorporated in Malaysia but may be used at local merchants;

“large acquirers” refer to non-bank acquirers with an average monthly transaction value (MTV) of more than RM10,000,000 annually;

“licensed bank” or “licensed Islamic bank” means any banking institution licensed under the FSA or Islamic Financial Services Act 2013 (IFSA) or a prescribed institution under the Development Financial Institution Act (DFIA);

“master merchant” refers to a merchant that operates a marketplace whereby such merchant enters into a contract with other merchants (i.e. contracted merchants) to offer their goods and services on its marketplace;

“merchant” means a person or an entity that accepts payment instruments for the
sale of goods or services;

“merchant acquiring services” refer to a business of an operator of a payment system that enters into a contract with a merchant for the purpose of accepting payment instruments for payment of goods or services;

“non-bank acquirer” means any person who is not a licensed person that has been registered by the Bank pursuant to section 18(1) of the FSA to provide merchant acquiring services and fulfils the criteria under paragraph 2.1;

“operator” means any person, acting alone or under an arrangement with another person, responsible for the rules, procedures and operations of a payment system;

“outsourcing arrangement” refers to an arrangement in which a service provider performs an activity on behalf of the acquirer on a continuing basis, where the activity would otherwise be undertaken by the acquirer;

“third party acquirer/payment facilitator” refers to a non-direct participant of payment instrument network(s) that is appointed by an acquirer (i.e. a direct participant of payment instrument network(s)) to perform merchant acquiring services;

“payment gateway service provider” refers to an entity that provides the IT system and infrastructure for purposes of processing payment or settlement transactions;

“payment instruments” refer to payment instruments accepted at merchants for making payment of goods and services (e.g. credit card, credit card-i, debit card, debit card-i, charge card, charge card-i, e-money, channel/system that facilitates transfer of funds from current or saving account);

1 For the 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” means 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 (e.g. Visa, Mastercard, UnionPay International, e-money scheme²);

“payment system” means any system or arrangement for the transfer, clearing or settlement of funds or securities;

“physical merchants” refer to merchants that sell goods or services physically over the counter (i.e. brick-and-mortar/face-to-face business);

“point-of-sale (POS) terminal” means 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;

“small acquirers” refer to non-bank acquirers with an average MTV of less than RM10,000,000 annually; and

“SME” means small and medium enterprises as defined in the Notification on Definition of Small and Medium Enterprises (SMEs) issued by the Bank.

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 Payment Card Reform Framework issued on 23 December 2014; and

(b) the policy document on the Management of Customer Information and Permitted Disclosures issued on 17 October 2017.

² It is also an issuer of payment instrument under its own brand name.
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 management that consists of people with calibre, credibility, integrity, and fulfil the fit and proper criteria as stipulated in paragraph 9;

(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.

S 8.2 The Board has the overall responsibility in ensuring the financial soundness and stability of the acquirer. The major responsibilities of the Board are given in Appendix 1.

S 8.3 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 third parties; and

(c) appropriate and timely reporting or escalation of issues that may impact the operations or security of the merchant acquiring operations.
8.4 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.

8.5 With regard to technology risk management and cybersecurity, 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 years. These plans must 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 must be periodically reviewed, at least once every three years.

8.6 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.

8.7 The Board is 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.

8.8 The senior management of acquirers is 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 8.3(b);

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

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

(b) oversee 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 must be reported to the Board.

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

8.10 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 a robust technology systems and management of technology risk.

8.11 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.

### 9. Fit and proper criteria

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| S  | 9.1 Any person to be appointed as a Key Responsible Person (KRP)\(^3\) of an acquirer must have been assessed by the Board to have met all the fit and proper criteria based on, at minimum, the factors set out in paragraphs 9.2 to 9.4, relating to –  
|   | (a) probity, personal integrity and reputation; 
|   | (b) competency and capability; and 
|   | (c) financial integrity.  
| G  | 9.2 Probity, personal integrity and reputation are values that can be demonstrated through personal qualities such as honesty, integrity, diligence, independence of mind and fairness. These qualities are demonstrated over time and demand a disciplined and on-going commitment to high ethical standards.  
| G  | 9.3 Competency and capability are demonstrated by a person who possesses the relevant knowledge, experience and ability to understand the technical requirements of the business, the inherent risks and the management process required to perform his role in a key function in the relevant capacity effectively.  
| G  | 9.4 Financial integrity is demonstrated by a person who manages his own financial affairs properly and prudently.  
| S  | 9.5 The Board shall ensure the following in determining the fitness and propriety of the KRP –  

---

\(^3\) Key responsible person (KRP) in this policy document refers to a person that is directly accountable or responsible for the management or oversight of an acquirer. This may include the directors, Chief Executive Officer (CEO) and management.
(a) the Board shall consider the minimum factors as given in Appendix 2 in assessing a KRP’s level of probity, integrity, reputation, competency, capability and financial integrity;
(b) an effective policies and procedures are in place to conduct assessment on the fitness and propriety of KRP and in making decisions on their appointments;
(c) the policies and procedures are periodically reviewed to ensure relevance and appropriateness; and
(d) where the KRP no longer demonstrates the ability to fulfil fit and proper criteria, immediate steps must be taken to reduce the risk associated with the KRP who continues to hold the position and remove the KRP from such position as soon as practicable.

9.6 The acquirer shall inform the Bank in writing of any removal of KRP arising from the actions taken under paragraph 9.5(d).

10. Shareholder suitability

10.1 An acquirer shall ensure that its shareholder⁴ fulfils the shareholder suitability requirements as set out in paragraphs 10.2 on an on-going basis and shall not act in a manner that would be detrimental to the safety and soundness of the acquirer.

10.2 For the purpose of paragraph 10.1, an acquirer shall ensure that its shareholder –
(a) does not act or, in the case of a corporate shareholder, conduct its business or operations in a manner that would cast doubt on its honesty and integrity as a shareholder of the acquirer;
(b) has a good reputation and refrain from acting in a manner that tarnishes or could tarnish its reputation or the reputation of the acquirer. Examples of circumstances that may cause a shareholder to breach this requirement are given in Appendix 3; and

⁴ Refers to a person that holds an aggregate interest of 5% or more in the shares of a registered person.
(c) has adequate control of its financial risks and maintain a sound financial position on a continuous basis, so that it can serve as a source of financial strength for the acquirer in the event that capital support is required. Examples of circumstances that may cause a shareholder to breach this requirement is given in Appendix 3.

S 10.3 Where the Bank requires the submission of all relevant documents or information, including documents or information relating to the shareholder’s associated or related corporations and their ultimate beneficial owners, for the purpose of facilitating the Bank’s on-going assessment of shareholder suitability, the acquirer shall submit such documents or information to the Bank as accorded under section 143(3) of the FSA.
PART C OPERATIONAL REQUIREMENTS

11. Specific requirements for non-bank acquirers

Capital requirements

S 11.1 Non-bank acquirers with an average MTV of less than RM10,000,000 annually (i.e. small acquirers) are required to maintain, at all times, minimum shareholders’ funds of RM300,000.

S 11.2 Non-bank acquirers with an average MTV of more than RM10,000,000 annually (i.e. large acquirers) are required to maintain, at all times, minimum shareholders’ funds of RM1,000,000.

Question 2:
Please provide feedback on the following:
(i) The Bank is considering to provide a one-year grace period for an existing non-bank acquirer to fulfil the capital requirement. What is the expected timeline for your institution to be able to meet the above requirement?
(ii) Potential challenges in meeting the minimum shareholders’ funds requirement, particularly for small acquirers.

12. Settlement risk management

S 12.1 Acquirers shall ensure timely and complete funds settlement to merchants.

S 12.2 Acquirers shall ensure that the settlement period commensurate with the merchant’s business models and needs.

G 12.3 Acquirers should ensure that the settlement period is no longer than two (2) and five (5) working days from the transaction date, for physical merchants and e-commerce merchants respectively. Notwithstanding this, if a merchant requests for a shorter settlement period, acquirer shall assess accordingly.
12.4 Acquirers shall deposit the funds received for settlement to merchants in a dedicated deposit account (designated account) with licensed banks or licensed Islamic banks, separate 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 card issuers less the Merchant Discount Rate (MDR) charged or any other applicable charges to the merchant.

12.5 In the event settlement to SME merchants by acquirers takes more than two (2) working days upon receiving the funds from the payment instrument network/issuer or upon delivery of products/services, whichever is later, the acquirer shall safeguard the funds as follows –

(a) secure a bank guarantee from a licensed bank or licensed Islamic bank on such settlement funds or outstanding amount for settlement; or

(b) place the settlement funds in a trust account with a licensed bank or licensed Islamic bank in accordance with the Trustee Act 1949.

Illustration of calculation is given in Appendix 4.

12.6 Acquirers shall be liable for providing 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, fails to fulfil its settlement obligations.

Question 3:
For purposes of paragraph 12.5, please identify the potential challenges in meeting the requirement on safeguarding of funds for settlements beyond T+2. Please propose alternative measures, if any.
13. Merchant management

Merchant recruitment

S 13.1 Acquirers shall establish prudent underwriting criteria and procedures for on-boarding a merchant. The assessment criteria shall include the following –

(a) financial strength and relevant background details (e.g. the merchant has not been declared a bankrupt or insolvent);

(b) legitimacy of 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 13.2 Acquirers are required to verify merchants’ identity using reliable documents, information or any other measures, before establishing any acquiring relationship with the merchants.

G 13.3 For purposes of paragraph 13.2 –

(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, ID), owner details, business nature and products/ services offered.

5 Includes master merchant.
S 13.4 If a merchant recruitment agent\(^6\) is engaged, acquirers shall ensure that proper controls as required in paragraphs 13.1 and 13.2 are put in place by the merchant recruitment agent. Merchants shall not be on-boarded via the merchant recruitment agents unless approved by the acquirers and acquirers shall retain the responsibility for ensuring the merchants on-boarded do not conduct fraudulent or illegal activities.

**Merchant monitoring**

S 13.5 Acquirers shall conduct effective monitoring on their merchants’ activities to ensure that the merchants are not involved in any fraudulent or illegal activities.

S 13.6 Acquirers shall maintain a “watch list” of merchants that are suspected to be collusive or involved in fraudulent or illegal activities, if any, and the activities of these merchants shall be closely monitored and investigated.

S 13.7 Acquirers shall monitor the chargebacks trend, including their 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 13.8 Acquirers shall terminate immediately any acquiring relationship with a merchant that is confirmed\(^7\) to be involved in fraudulent or illegal activity.

S 13.9 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.

---

\(^6\) The merchant recruitment agent’s roles are limited to the referral of merchants, collection of merchants’ information and document for application purposes and submission to acquirers for approval. The activities do not involve in processing or facilitating the transactions.

\(^7\) Refers to merchant that has been charged or convicted in court or after acquirer’s own investigation or assessment is completed substantiated by adequate and appropriate evidence (i.e. not a mere allegation).
**Information security requirements for merchants**

S 13.10 Acquirers shall ensure that merchants maintain and demonstrate compliance with the highest level of information security requirement. This includes any third party service providers engaged by the merchants for accessing, storing, transmitting and processing customer’s data.

S 13.11 Acquirers’ agreement with merchant shall include provisions to ensure merchants and merchants’ third party service providers maintain compliance with applicable security requirements and established security standards⁸.

S 13.12 Acquirers shall educate⁹ their merchants on the importance of the contractual obligation on securing customer’s data and the consequences of failing to adequately protect such data.

## 14. Fraud risk management

S 14.1 Acquirers shall put in place an effective fraud prevention mechanism to reduce the chances of fraud occurrence. This shall include having the necessary processes and procedures to enable authentication by customers based on the risk profile of transactions and customers.

S 14.2 Acquirers shall deploy effective fraud detection and monitoring mechanism that is –

(a) conducted on real time basis; and

(b) effective in facilitating early detection of unusual transactions and in halting or delaying fraudulent or suspicious transactions.

S 14.3 The fraud risk management measures must be reviewed periodically to ensure proactive actions are taken to address any inadequacies in such measures.

---

⁸ Such as Payment Card Industry Data Security Standard (PCI DSS).

⁹ By providing appropriate level of awareness through various measures such as training, constant reminders or engagement sessions.
14.4 Fraud incidents and their assessment shall be reported to the senior management and the Board in a timely manner if the impact is significant.

14.5 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 prescribed by the Bank.

15. **Business Continuity Management**

15.1 Acquirers shall ensure that they have the resources and capacity in terms of hardware, software and other operating capabilities\(^{10}\) to deliver consistently reliable and secure services.

15.2 Acquirers shall ensure that the following measures are in place to support operational reliability, which include –

(a) strong internal controls for system and personnel administration;

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

(c) systems with sufficient capacity to support business requirements; and

(d) systems with a robust business continuity and disaster recovery plan, including a highly reliable backup system.

16. **Outsourcing**

16.1 Acquirers shall remain responsible and accountable for the services outsourced to any outsourced parties\(^{11}\) (e.g. third party acquirers/ payment facilitators, merchant recruitment agents, payment gateway service providers, IT service providers) under an outsourcing arrangement.

---

\(^{10}\) This may refer to any other skills or processes involved in the operations (e.g. adequate manpower and skill set to operate the systems).

\(^{11}\) Including affiliates of the acquirer, regardless of jurisdiction.
16.2 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; and

(b) 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 flexibility 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 acquirer to retain the continuous ability to comply with the regulatory and supervisory requirements on the outsourced functions.

16.3 Acquirers shall perform appropriate due diligence review of the integrity, competency, financial viability as well as risk management and internal controls of the outsourced parties before the outsourcing arrangements are formalised.

16.4 Approval from the Board to outsource their functions shall be obtained and documented.

16.5 Acquirers shall establish outsourcing agreement when engaging an outsourced party, which must be comprehensive and includes the following –

(a) clearly defined roles, responsibilities and obligations of the outsourced party;

(b) provisions to ensure that the outsourced party maintains and demonstrates compliance with the highest level of information security requirement, including –
(i) for the outsourced party to be bound by confidentiality provisions stipulated under the contract even after the engagement has ended; and
(ii) for the outsourced party to maintain compliance with applicable security requirements and established security standards\(^{12}\) at all times;
(c) clear provisions on access rights for the Bank and any party appointed by the acquirers to examine any activity of and/or related to the acquirers. This shall include access to any record, file or data of the acquirers, including management information and the minutes of all consultative and decision-making processes as well as rights to enter the premises of the outsourced party to conduct examination or investigation;
(d) dispute resolution process in the event of default or non-performance of obligations, including remedies and indemnities where relevant;
(e) requirements for the outsourced party to provide sufficient prior notice to the acquirer of any sub-contracting which is substantial; and
(f) conditions under which the outsourcing arrangement may be terminated.

16.6 In addition to the requirements in paragraph 16.5(b), the acquirer shall ensure that the outsourced parties provide a written undertaking to the acquirers to comply with the secrecy provision pursuant to section 133 of the FSA, the Policy Document on Management of Customers Information and Permitted Disclosures issued by the Bank, and any other relevant policy documents as may be specified by the Bank.

16.7 Acquirers shall ensure their outsourced party complies with all relevant regulatory requirements specified in this policy document\(^{13}\) and as may be specified by the Bank from time to time.

---
\(^{12}\) Such as PCI DSS.
\(^{13}\) This includes specific requirements for system development and acquisition, data centre operations, network resilience, technology security and cybersecurity, wherever applicable.

Issued on: 17 July 2020
16.8 The requirement in paragraph 16.7 is also applicable when an outsourced party engages a subcontractor to undertake the activities that were outsourced by the acquirer, whereby the acquirer shall implement proper controls to ensure that the subcontractor complies with the relevant requirements based on standards issued by the Bank to acquirers from time to time.

16.9 The acquirer shall have a contingency plan or arrangements to secure business continuity with the outsourced party in the event the arrangement with the outsourced party is suddenly terminated. This is to mitigate any significant discontinuity in the work that is supposed to be conducted by the outsourced party. The contingency plan shall be –

(a) reviewed from time to time to ensure that the plan is current and ready for implementation in the event of sudden termination of the outsourced party; and

(b) approved by the Board of the acquirers.

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

16.11 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.

16.12 Acquirers shall ensure that any weaknesses highlighted during the audit are well-documented and promptly rectified by the outsourced parties especially where such weaknesses may affect the integrity of the internal controls of the acquirers.
16.13 For outsourcing arrangement where the outsourced party is located or the services are performed outside Malaysia, the acquirer should have in place appropriate control and safeguards to manage any additional risk, with regard to various conditions, including legal and regulatory requirements as well as social and political conditions.

17. **Arrangement with parties involved in payment and settlement process**

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

17.2 In addition to requirements in paragraph 16 for third party acquirers/payment facilitators and paragraph 13 for master merchants, acquirers are required to ensure such parties in paragraph 17.1 have adequate operational and risk management policies and procedures in place, which include the following –

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

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

(c) the parties’ contracted merchants are able to ensure confidentiality, security and integrity of 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 their contracted merchants.
17.3 Acquirers shall be held responsible for fulfilling the settlement obligation to the contracted merchants of a third party acquirer/ payment facilitator, in the event that the third party acquirer/ payment facilitator fails to fulfil its settlement obligations to the contracted merchants.

17.4 Notwithstanding paragraph 16.8, acquirers shall ensure that a third party acquirer/ payment facilitator does not appoint another third party acquirer/ payment facilitator for purposes of acquiring a merchant.

17.5 Acquirers shall periodically monitor the transactions or activities of the parties mentioned in paragraph 17.1 (e.g. through transaction monitoring, site visit 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/ settlement risk and any issues or weaknesses detected are promptly rectified.

**Question 4:**
Please highlight any challenges in fulfilling the requirements specified in paragraph 17.

**18. Appropriate treatment for merchants**

18.1 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.

18.2 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 fair and not detrimental to the merchants by taking into consideration the merchants' interests. 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 eighty (180) 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 18.3 Acquirers shall establish clear and robust dispute resolution procedures to ensure effective and timely resolution of dispute cases between acquires and their merchants.

S 18.4 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 fourteen (14) working days. Merchants shall be informed if a longer time is required to address the dispute by providing appropriate rationale.
PART D  IT SECURITY CONTROLS

19. Technology Risk Management

S 19.1 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 19.2 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 19.3 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 21;
(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\(^\text{14}\), where necessary.

---

\(^{14}\) 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.
19.4 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. 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.

19.5 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
(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.
20. Technology Operations Management

Technology Project Management

S 20.1 Acquirers shall establish appropriate governance requirements commensurate with the risk and complexity\(^{16}\) 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 20.2 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 from extensive changes in project scope or deficiencies in meeting business needs;

\(^{16}\) 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.
(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 20.3 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 20.4 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 20.5 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. The policies and practices shall be reviewed at least once every three years to ensure that they remain relevant to the acquirers’ environment.

17 The security considerations shall include ensuring appropriate segregation of duties throughout the SDLC.
20.6 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.

20.7 Acquirers should consider the need for diversity\textsuperscript{18} in technology to enhance resilience by ensuring critical systems infrastructure are not excessively exposed to similar technology risks.

20.8 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.

20.9 The scope of system testing referred to in paragraph 20.8 should include unit testing, integration testing, user acceptance testing, application security testing, stress and regression testing, and exception and negative testing, where applicable.

20.10 Acquirers shall ensure any changes to the source code of IT 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.

20.11 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.

20.12 Acquirers shall physically segregate the production environment from the development and testing environment for critical systems. Where acquirers are relying on a cloud environment, the acquirers shall ensure that these environments

\textsuperscript{18} Diversity in technology may include the use of different technology architecture designs and applications, technology platforms and network infrastructure.
are not running on the same virtual host.

20.13 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.

20.14 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.

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

**Cryptography**

20.16 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 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 20.17 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\textsuperscript{19}, 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 20.18 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 20.19 Acquirers should store public cryptographic keys in a certificate issued by a certificate authority as appropriate to the level of risk. Such certificates associated

\textsuperscript{19} 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.
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 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** 20.20 Acquirers shall ensure proper management of data centres and specify the resilience and availability objectives\(^{20}\) of their data centres which are aligned with their business needs.

**G** 20.21 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** 20.22 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** 20.23 In addition to paragraph 20.22, large acquirers are also encouraged to ensure recovery data centres are concurrently maintainable.

**G** 20.24 Acquirers should host IT systems in a dedicated space intended for production data centre usage. The dedicated space should be physically secured from unauthorised access and is not located in a disaster-prone area. Acquirers should also ensure there is no single point of failure (SPOF) in the design and connectivity for critical components of the production data centres, including hardware

---

\(^{20}\) Availability objectives refer to the level of availability of the data centre which is expected to be specified as an internal policy.
components, electrical utility, thermal management and data centre infrastructure.

S 20.25 Acquirers shall establish proportionate controls, ensure adequate maintenance, and holistic and continuous monitoring of the critical components of the production data centres aligned with the acquirer’s risk appetite.

G 20.26 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 should 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 20.22 to 20.24 have been adhered to. 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 20.27 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 20.28 Acquirers should involve both the technology stakeholders and the relevant business stakeholders within the acquirers in their development and implementation of capacity management plans.
20.29 Acquirers shall establish appropriate monitoring mechanisms to track capacity utilisation and performance of key processes and services\(^{21}\). These monitoring mechanisms should be capable of providing timely and actionable alerts to administrators.

20.30 Acquirers shall segregate incompatible activities in the data centre operations environment to prevent any unauthorised activity\(^{22}\). In the case where vendors’ or programmers’ access to the production environment is necessary, these activities shall be properly authorised and monitored.

20.31 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.

20.32 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.

20.33 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.

20.34 In regard to paragraph 20.32, acquirers should also adopt the controls as specified in Appendix 5 or their equivalent to secure the storage and transportation of sensitive data in removable media.

\(^{21}\) For example, batch runs and backup processes for the acquirers’ application systems and infrastructure.

\(^{22}\) For example, system development activities must be segregated from data centre operations.
20.35 Where there is a reasonable expectation for immediate delivery of service, acquirers should ensure that the relevant systems are designed for high availability.

**Network Resilience**

20.36 Acquirers should design a reliable, scalable and secure enterprise network that is able to support their business activities, including future growth plans.

20.37 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.

20.38 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.

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

20.40 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.

20.41 Acquirers shall ensure sufficient and relevant network device logs are retained for investigations and forensic purposes for at least three years.
20.42 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.

20.43 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**

20.44 In addition to the requirements in paragraph 16 on outsourcing requirements, the acquirer shall fulfil the requirements under paragraphs 20.45 to 20.51 specifically for IT related third party service provider.

20.45 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.

20.46 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 provider’s 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.

20.47 At a minimum, the outsourcing agreement shall contain arrangements for disaster recovery and backup capability, where applicable, and IT system availability.

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

20.49 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 provider 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.

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

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

**Cloud Services**

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

20.53 The risk assessment as outlined in paragraph 20.52 shall be documented and made available for the Bank’s review as and when requested by the Bank.

20.54 Acquirers are expected to 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 20.52, 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; and
(c) the degree to which the selected cloud configuration adequately addresses the following attributes –
   (i) geographical redundancy;
   (ii) high scalability;
   (iii) scalability
   (iv) interoperability; and
   (v) strong recovery and resumption capability including appropriate alternate Internet path to protect against potential Internet faults.
20.55 Acquirers should consider the need for a third party pre-implementation review on cloud implementation that also covers the areas set out in paragraph 20.54.

20.56 Acquirers must 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**

20.57 Acquirers must 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 must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorised access to its technology systems.
In observing paragraph 20.57, acquirers should consider the following in their access 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.
20.59 Acquirers must 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 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).

20.60 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.

20.61 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.

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

20.63 Acquirers shall establish a user access matrix to outline access rights, user roles or profiles, and the authorising and approving authorities. The access matrix must be periodically reviewed and updated.
20.64 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 years and regularly reviewed in a timely manner.

20.65 In fulfilling the requirement under paragraph 20.64, large acquirers are encouraged to —
   (a) deploy an identity and 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**

20.66 Acquirers shall ensure that 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.
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

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.

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

20.71 Acquirers should ensure that the use of more advanced technology to authenticate and deliver digital services such as biometrics, tokenisation and contactless communication\(^{23}\) comply with internationally recognised standards where available. The technology should be resilient against cyber threats\(^{24}\) including malware, phishing or data leakage.

20.72 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.

20.73 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.

20.74 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;

---

\(^{23}\) Such as QR code, Bar Code, Near Field Communication (NFC), Radio Frequency Identification (RFID).

\(^{24}\) 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.
(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 20.75 In fulfilling paragraph 20.74, acquirers should adopt the controls specified in the following Appendices for the respective digital delivery channel:
(a) Appendix 6: Control Measures on Payment Acceptance Device;
(b) Appendix 7: Control Measures on Internet Application;
(c) Appendix 8: Control Measures on Mobile Application and Devices; and
(d) Appendix 9: Control Measures on QR Code.

21. **Cybersecurity Management**

*Cyber Risk Management*

G 21.1 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 21.2 Acquirers shall develop a Cyber Resilience Framework (CRF), which articulates the institution’s 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.
21.3 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.
21.4 In addition to the elements provided in paragraph 21.3 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 senior management and the Board; 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

21.5 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 21.6 Where relevant, acquirers should adopt the control measures on cybersecurity as specified in Appendix 10 to enhance its resilience to cyber-attacks.

G 21.7 Acquirers should 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 21.8 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 21.9 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 21.10 In addition to the requirement in paragraph 21.9 above, large acquirers should 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 senior management and the Board in a timely manner.
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.

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)**

Acquirers shall 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 provider to expand network bandwidth on-demand including upstream service provider capability, adequacy of the 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)

21.14 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.

21.15 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.

21.16 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 21.17 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 21.18 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.
21.19 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.

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

21.21 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.

**Question 5:**
Are you agreeable with the requirements under paragraphs 21.17 to 21.21? If no, please provide your feedback on the following:

(i) Potential challenges in meeting the above requirements; and
(ii) Alternative measures, if any.
Cyber Response and Recovery

21.22 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.

21.23 Acquirers should establish and implement a comprehensive Cyber Incident Response Plan (CIRP). The CIRP should 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.
21.24 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.

21.25 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.

21.26 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.

22. Technology Audit

22.1 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.

22.2 The audit function shall be adequately resourced with relevant technology audit competencies and sound knowledge of the acquirers’ technology processes and operations.
G 22.3 Acquirers should ensure their technology audit staff are adequately conversant with the developing sophistication of the acquirers’ technology systems and delivery channels.

G 22.4 In addition to paragraph 22.2, large acquirers should establish a dedicated technology audit function that has specialised technology audit competencies to undertake technology audits.

S 22.5 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 22.6 The audit function (in the case of paragraph 22.2) and the dedicated technology audit function (in the case of paragraph 22.4) 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.
23. Internal Awareness and Training

**S 23.1** 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 should reflect the current cyber threat landscape.

**G 23.2** 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 23.3** Acquirers should provide their Board members with regular training and information on technology developments to enable the Board to effectively discharge its oversight role.

**Question 6:**
Please provide your feedback on the requirements for IT security and controls requirements under Part D:
(iii) Adequacy of the requirements;
(iv) Potential challenges in meeting the above requirements and alternative measures, if any.
PART E OTHER REQUIREMENTS

24. Other compliance requirements

24.1 Acquirers shall ensure that there is no exclusivity in the use of payment terminals/devices to support only a specific payment network or instrument.

24.2 Newy 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.

24.3 Acquirers shall notify the Bank in writing to Director of Payments Oversight Department of 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.

24.4 Acquirers shall comply with the policy document on Payment Card Reform Framework and other relevant requirements issued by the Bank from time to time.
Appendix 1  BOARD ROLES AND RESPONSIBILITIES

1) The Board has the overall responsibility in ensuring the financial soundness and stability of the acquirer. The major responsibilities of the Board 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 KRP in determining fulfilment of the fit and proper criteria;

(d) Ensuring competent 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 internal audit function.
Appendix 2     FACTORS FOR CONSIDERATION IN FIT AND PROPER ASSESSMENT

1) In assessing a KRP’s level of probity, integrity and reputation, the following are the minimum factors that must be considered by the Board –
   (a) whether the KRP is or has been the subject of any proceedings of a disciplinary or criminal nature, or has been notified of any impending proceedings or of any investigations, which might lead to such proceedings;
   (b) whether the KRP has contravened any provision made by or under any written law designed to protect members of the public against financial loss due to dishonesty, incompetence or malpractice;
   (c) whether the KRP has contravened any of the requirements and standards of a regulatory body, professional body, government or its agencies;
   (d) whether the KRP has engaged in any business practices which are deceitful, oppressive or otherwise improper (whether unlawful or not), or which otherwise reflect discredit on his professional conduct;
   (e) whether the KRP has been dismissed, asked to resign or has been resigned from employment or from a position of trust, fiduciary appointment or similar position because of questions about his honesty and integrity; and
   (f) whether, in the past, the KRP has acted unfairly or dishonestly in his dealings with his customers, employer, auditors and regulatory authorities.

2) In assessing a KRP’s competency and capability, the Board must consider factors which include, but are not limited to the following –
   (a) whether the KRP has the appropriate qualification, training, skills, practical experience and commitment to effectively fulfil the role and responsibilities of the position and in case of directors, having regard to their commitments; and
   (b) whether the KRP has satisfactory past performance or expertise in the nature of the business being conducted.
3) In assessing the KRP’s financial integrity, the Board must consider all relevant factors which include, but are not limited to the following –

(a) whether the KRP has been and will be able to fulfil his financial obligations, whether in Malaysia or elsewhere, as and when they fall due; and

(b) whether the KRP has been the subject of a judgment debt which is unsatisfied, either in whole or in part, whether in Malaysia or elsewhere.
Appendix 3 EXAMPLES OF CIRCUMSTANCES THAT BREACH SHAREHOLDER SUITABILITY

1) Examples of circumstances that may breach requirements in paragraphs 10.2(b) are, if a shareholder —
   (a) is subject to a bankruptcy or winding up proceeding;
   (b) fails, or is likely to fail, to meet its financial obligations as and when they fall due;
   (c) is, or has been, the subject of any criminal proceedings or convicted of any offence involving dishonesty, fraud or other financial crimes. Also includes any investigation relating to any criminal or regulated financial activity, or has been notified of any impending investigations;
   (d) fails, or is likely to fail, to comply with relevant laws, requirements, conditions or standards issued by a regulatory, professional or government body in Malaysia or any other jurisdiction, or has been, is expected to be or is subject to disciplinary or enforcement action by such bodies;
   (e) engages, or is about to engage, in any business practice that is deceitful or reflects discredit on the shareholder’s professional conduct; and
   (f) in respect of an individual shareholder has been dismissed, asked to resign or has resigned from employment, a position of trust, fiduciary appointment or other similar appointments due to concerns about his honesty or integrity.

2) Examples of circumstances that may breach paragraph 10.2(c) are, if a shareholder—
   (a) fails, or is likely to fail, to meet its financial obligations as and when they fall due; and
   (b) in respect of a corporate shareholder —
      (i) has, or is likely to have, insufficient assets, capital or reserves to withstand any financial shocks; and
      (ii) pursues, or is likely to pursue, excessive risks or aggressive expansion plans which are not reasonably supported by adequate financial capacity.
Appendix 4  ILLUSTRATION ON FUNDS TO BE SET ASIDE FOR MERCHANT SETTLEMENT

Illustration (i): Customer buys and receives goods on Day 1 for RM500. As funds received from payment instrument network/issuer is on Day 3 (i.e. T) which is LATER than the delivery of goods on Day 1, the acquirer should settle to the SME merchants latest by Day 6 (i.e. 2 working days from T, the day of funds received). If the acquirer is unable to settle to SME merchants on Day 6, the acquirer shall safeguard the settlement funds of RM500 starting from **Day 6 and onwards** until settlement is made to SME merchants.

<table>
<thead>
<tr>
<th>Days after received funds</th>
<th>Activity</th>
<th>Days 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
<th>Day 6</th>
<th>Day 7</th>
<th>Day 8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Customer buys &amp; SME merchant delivers goods</td>
<td></td>
<td></td>
<td>Funds received from payment instrument network/issuer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Illustration (ii): Customer buys goods for RM500 on Day 1 but receives it on Day 4. As delivery of goods is on Day 4 (i.e. T) which is LATER than the receipt of funds from payment instrument network/issuer on Day 3, the acquirer should settle to SME merchants latest by Day 7 (i.e. 2 working days from T, the day of the delivery of goods). If the acquirer is unable to settle to SME merchants on Day 7, the acquirer shall safeguard the settlement funds starting from **Day 7 and onwards** until settlement is made to SME merchants.

<table>
<thead>
<tr>
<th>Days after delivery</th>
<th>Activity</th>
<th>Days 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
<th>Day 6</th>
<th>Day 7</th>
<th>Day 8</th>
<th>Day 9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Customer buys goods</td>
<td></td>
<td></td>
<td>Funds received from payment instrument network/issuer</td>
<td>SME Merchant delivers goods</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Days after delivery</th>
<th>Activity</th>
<th>Days 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
<th>Day 6</th>
<th>Day 7</th>
<th>Day 8</th>
<th>Day 9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix 5       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) Should 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 5, in the event third party services are required in undertaking the storage management or transportation process of sensitive data in removable media.
Appendix 6  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 7  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 8  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;

(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\(^{25}\); and

\(^{25}\) This includes risks associated with malwares that enable keystroke logging, PIN harvesting and other malicious forms of customer and counterparty information downloading.
Appendix 9  CONTROL MEASURES ON QR 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 jailbroken) devices; and
   (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 10 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.