MALAYSIA – BANKS

GUIDANCE ON COMPLYING WITH REGULATORY REQUIREMENTS APPLICABLE TO FINANCIAL SERVICES INSTITUTIONS USING CLOUD COMPUTING

Last updated: November 2014

1. WHAT DOES THIS MICROSOFT GUIDANCE CONTAIN?

This guidance document provides a guide to complying with the regulatory process and requirements applicable to financial services institutions using cloud computing. In this guidance financial services institutions means conventional banks (although the documents listed also cover Islamic banks) as opposed to Takaful operators, insurers, development financial services institutions and capital market intermediaries where certain other guidelines apply ("**FSIs**"). Microsoft has prepared a guidance document for insurance companies which is available on request.

Sections 2 to 6 of this guidance sets out some high level information about the applicable legal frameworks governing banks' and insurance companies' use of cloud computing services and the regulatory process that applies.

Section 7 sets out questions in relation to outsourcing to a cloud services solution based on the laws, regulations and guidance that are relevant to the use of cloud services. Although there is no requirement to complete a checklist like this one, we have received feedback from FSIs that a checklist approach like this is very helpful. The checklist can be used:

(i) as a checklist for ensuring regulatory compliance with the requirements set out in the laws, regulations and guidelines (listed in Section 2); and

(ii) as a tool to aid discussions with the regulator(s) (listed in Section 3), should they wish to discuss your organization's overall approach to compliance with their requirements.

Appendix One also contains a list of key contractual requirements based on the laws, regulations and guidance that are relevant to an FSI's use of cloud services.

Note that this document is not intended as legal or regulatory advice and does not constitute any warranty or contractual commitment. Instead, it is intended to streamline the regulatory process for you. You should seek independent legal advice on your technology outsourcing project and your legal and regulatory obligations. Please note that the scope of this document specifically does not include potentially applicable state laws, rules and regulations.

2. WHAT REGULATIONS AND GUIDANCE ARE RELEVANT?

BNM has developed several relevant documents which FSIs should bear in mind. There are effectively different "layers" of rules that apply depending on whether the use of Office 365 constitutes an "outsourcing" and, if so, whether it is significant enough to constitute a "material outsourcing". It is prudent to assume that the use of Office 365 would as a minimum constitute an "outsourcing". Whether it would then constitute a "material outsourcing" would be determined on a case-by-case basis, based on an analysis of whether the disruption of the Microsoft Cloud Services would have the potential to significantly impact the FSI's business operations, reputation or profitability. Note that we have included all relevant regulations regardless of whether or not the outsourcing is deemed to be "material" or not for the sake of completeness.

Finally, *even if* it does not constitute an "outsourcing" or "material outsourcing", more other general technology guidelines apply, specifically: IT Guidelines, E-Banking Guidelines, Business Continuity Management Guidelines and Guidelines on Data Management and Management Information System as listed below.

The relevant documents are as follows:

- BNM's Circular on Outsourcing of Banking Operations. Unfortunately this is not a publicly available document although Microsoft has had sight of various BNM letters which comprise this Circular.
- BNM's Guidelines on the Provision of Electronic Banking (e-banking) Services by FSIs.
- BNM's Guidelines on Data Management and MIS Framework for FSIs.
- BNM's Guidance on Business Continuity Management (**"BNM's BCM Guidelines"**)
- BNM's Guidelines on Management of IT environment.

- In addition, the Financial Services Act 2013 (**"FSA"**) contains some relevant provisions.

Note that relevant documents are not available on the BNM website but we have included a hyperlink where they are.

3. **WHO IS/ARE THE RELEVANT REGULATOR(S)?**

The Bank Negara Malaysia (**"BNM"**)

4. **IS REGULATORY APPROVAL REQUIRED IN MALAYSIA?**

Yes.

The prior consent of BNM is only required if the FSI wishes to undertake an outsourcing using an overseas provider.

However, all outsourcings must be notified to BNM.

5. **IS/ARE THERE (A) SPECIFIC FORM OR QUESTIONNAIRE(S) TO BE COMPLETED?**

No.

Unlike in certain jurisdictions, such as Singapore, there are no specific forms or questionnaires that an FSI must complete when considering cloud computing solutions.

6. **DOES THE REGULATOR MANDATE SPECIFIC CONTRACTUAL REQUIREMENTS THAT MUST BE ADOPTED?**

Yes.

BNM does specifically mandate contractual requirements that must be agreed by FSIs with their service providers. These are not set out in one list in any one place unfortunately but scattered across the different documents referred to above. Microsoft has included these points in the document which follows in relation to the relevant issues and Appendix One contains a comprehensive list and details of where in the Microsoft contractual documents these points are covered.

7. CHECKLIST

Key:

In blue text, Microsoft has included template responses that would demonstrate how your proposed use of Microsoft's services would address the point raised in the checklist. Some points are specific to your own internal operations and processes and you will need to complete these answers as well.

In *red italics*, Microsoft has provided guidance to assist you with the points in the checklist.

Ref.	Question/requirement	Template response and guidance
A. GENERAL		
1.	Who is the Service Provider? Please provide company profile/background.	*In case requested, details of the Microsoft corporate entity providing the services are provided below.* The Service Provider is Microsoft Operations Pte Ltd, the regional licensing entity for Microsoft Corporation, a global provider of information technology devices and services, which is publicly-listed in the USA (NASDAQ: MSFT). Microsoft's full company profile is available here: https://www.microsoft.com/en-us/news/inside_ms.aspx.
2.	List all proposed activities and operations to be outsourced to the Service Provider. Confirm that the outsourcing will not include the following operational functions: (i) Those which involve direct and physical contact with the borrowers e.g. actual collection of debts, provision	*Paragraph 2 of the BNM's letter dated 14 April 2000 on Outsourcing of Banking Operations which provides that FSIs are not allowed to outsource the listed operational functions.* We can confirm that the outsourced services will not involve the listed operational functions and, in particular, we will not be outsourcing any core activities or any inherent banking functions such as services associated with placement of deposits and withdrawals. The arrangement will involve the outsourcing of certain IT functions through the use of Microsoft's "Office 365" service, which is described in more detail here: Microsoft Office 365. Amongst other things, the Office 365

Ref.	Question/requirement	Template response and guidance
	of after-sale services to customers and fraud investigations; (ii) Critical functional of banking institutions e.g. loan approval and administration, trading and investment, provision of fee-based services; and (iii) Internal audit functions.	service includes: • Microsoft Office applications hosted in the "cloud"; • Hosted email; • Web conferencing, presence and instant messaging; • Data and application hosting; • Spam and malware protection; and • IT support services.
3.	Will the outsourcing impair your image, integrity and credibility?	*Paragraph 1(ii) of the BNM's Circular on Outsourcing of Banking Operations.* We see absolutely no reason why this outsourcing to Microsoft would have any impairment on our image, integrity or credibility. As outlined in detail in section C below, we have undertaken robust due diligence in relation to our selected service provider and are very confident that, in Microsoft, we have selected a reputable and capable provider.
4.	Is the cost lower for you to outsource such functions rather than to develop the necessary infrastructure and expertise?	*Paragraph 1(iii) of the BNM's Circular on Outsourcing of Banking Operations. You will need to answer this question based on your own cost analysis and internal capability.*

Ref.	Question/requirement	Template response and guidance
B. OUTSOURCING POLICY AND RISK MANAGEMENT		
5.	Has Board approval been sought and documented prior to signing the outsourcing contract?	*Paragraph 4(ii) of the BNM's Circular on Outsourcing of Banking Operations. BNM expects that you will have sought Board approval in relation to the outsourcing so you will need to confirm this here.* Yes.
6.	Is senior management confident that there are effective oversight, review and reporting arrangements in place to ensure that service level agreements regarding standards on data quality, integrity and accessibility are observed at all times?	*Paragraph 4.12 of the BNM's Guidelines on Data Management and MIS Framework for Development Financial Institutions ("**DFI Guidelines**"). You may want to add to the following any specific details of communications with and involvement of senior management.* Yes. Essential to us is that, despite the outsourcing, we retain control over our own business operations, including control of who can access data and how they can use it. At a contractual level, we have dealt with this via our contract with Microsoft, which provides us with legal mechanisms to manage the relationship including appropriate allocation of responsibilities, oversight and remedies and the relevant regulatory requirements. At a practical level, we have selected the Office 365 product since it provides us with transparency in relation to data location, authentication and advanced encryption controls. We (not Microsoft) will continue to own and retain all rights to our data and our data will not be used for any purpose other than to provide us with the Office 365 services. In choosing Microsoft, we also took into account the fact that the European Union's data protection authorities have found that Microsoft's enterprise cloud contracts meet the high standards of EU privacy law. Microsoft is the first – and so far the only – company to receive this approval.
7.	Do you have in place proper reporting and monitoring procedures over the	*Paragraph 4(vi) of the BNM's Circular on Outsourcing of Banking Operations.*

Ref.	Question/requirement	Template response and guidance
	integrity and quality of work conducted by the Service Provider?	Yes. Microsoft's Service Level Agreement (**"SLA"**) applies to the Office 365 product. Our IT administrators also have access to the Office 365 Service Health Dashboard, which provides real-time and continuous monitoring of the Office 365 service. The Service Health Dashboard provides our IT administrators with information about the current availability of each service or tool (and history of availability status) details about service disruption or outage, scheduled maintenance times. The information is provided via an RSS feed. Amongst other things, it provides a contractual 99.9% uptime guarantee for the Office 365 product and covers performance monitoring and reporting requirements which enable us to monitor Microsoft's performance on a continuous basis against service levels. As part of the support we receive from Microsoft, we also have access to a technical account manager who is responsible for understanding our challenges and providing expertise, accelerated support and strategic advice tailored to our organization. This includes both continuous hands-on assistance and immediate escalation of urgent issues to speed resolution and keep mission-critical systems functioning. We are confident that such arrangements provide us with the appropriate mechanisms for managing performance and problems. We also have extensive audit rights as detailed in section E below.
C. SERVICE PROVIDER SELECTION CRITERIA & DUE DILIGENCE		
8.	Is the selection process of the Service Provider and its sub-contractors, if any, formally defined and documented?	*Various Malaysian regulations contain obligations in relation to due diligence and having a formal selection process, specifically: (i) Paragraph 4(i) of the BNM's Circular on Outsourcing of Banking Operations provides for the need for banking institution to perform due diligence review over the capabilities and expertise of the outsourcing vendor prior to selection; (ii) Paragraph 15(a), Part II of the BNM's Guidelines on Management of IT Environment states that due diligence should be adequately carried out to review and assess outsourcing viabilities, capabilities, reliabilities, expertise and track records before being approved by the board of directors;*

Ref.	Question/requirement	Template response and guidance
		and (iii) Paragraph 13 of the BNM's Guidelines on the Provision of Electronic Banking (e-banking) Services by FSIs provides for a need of a comprehensive and ongoing due diligence and oversight process for managing the FSI's outsourcing relationship and other third-party dependencies supporting e-banking. Yes. The selection process was formally defined and documented. It covered the service provider's: • financial soundness; • reputation; • managerial skills • technical capabilities; and • operational capability and capacity in relation to the services to be performed. [Please see the attached documentation for further information.]
9.	Did your selection criteria consider the following? (a) Capabilities, expertise, track records, experience, technical competence and adequacy of human resource capabilities of the Service Provider to	*This is covered in several places: paragraph 4(i) of the BNM's Circular on Outsourcing of Banking Operations; paragraph 15(a), Part II of the BNM's Guidelines on Management of IT Environment; paragraph 1(d), Part IV of the BNM's Guidelines on Management of IT Environment; paragraph 1(d), Part IV of the BNM's Guidelines on Management of IT Environment; and paragraph 15(b), Part II of the BNM's Guidelines on Management of IT Environment.* Yes. We followed a rigorous review and selection process. Set out below are the specific areas we considered and

Ref.	Question/requirement	Template response and guidance
	perform the specified activity to be outsourced. (b) Service Provider's understanding of your organizations strategic and business objectives in relation to the specific activity outsourced. (c) Financial strength and resources of the Service Provider (based on recent audited financial statements and other relevant information), including the consideration of the extent of the Service Provider's liabilities and financial ability (i.e., professional indemnity insurance coverage) to compensate your organization for errors, negligence and other operational failures. (d) Security and internal controls, standards, policies and	why we decided on Microsoft: **(a) Capabilities, experience and track record.** Microsoft is an industry leader in cloud computing. Office 365 was built based on ISO/IEC 27001 standards and was the first major business productivity public cloud service to have implemented the rigorous set of global standards covering physical, logical, process and management controls. 40% of the world's top brands use Office 365. We consulted various case studies relating to Office 365, which are available on the Microsoft website and also considered the fact that Microsoft has amongst its customers some of the world's largest organizations and FSIs. **(b) Service Provider's understanding of our objectives.** We have conducted detailed discussions with Microsoft and are confident that they understand our business and objectives. As set out above and below, their extensive experience and reputation in helping other financial institutions also helps us to be confident in this decision. **(c) Financial strength and resources.** Microsoft Corporation is publicly-listed in the United States and is amongst the world's largest companies by market capitalization. Microsoft's audited financial statements indicate that it has been profitable for each of the past three years. Its market capitalization is in the region of USD 280 billion. Accordingly, we have no concerns regarding its financial strength and ability to compensate us for failures. **(d) Security and internal controls.** Microsoft is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centers of even the most sophisticated organizations. We have confidence in the security of the solution and the systems and controls offered by Microsoft. In addition to the ISO/IEC 27001 certification, Office 365 is designed for security with BitLocker Advanced Encryption Standard ("**AES**") encryption of email at rest and security sockets layer ("**SSL**")/transport layer security ("**TLS**") encryption of data in transit. The Microsoft service is subject to the SSAE16 SOC1 Type II audit, an independent, third party audit. In particular, all personnel with

Ref.	Question/requirement	Template response and guidance
	procedures.	access to customer data are subject to background screening, security training and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. User access to data is also limited by user role. For example, system administrators are not provided with database administrative access. Microsoft offers contractually-guaranteed 99.9% uptime, hosted out of world class data centers with physical redundancy at disk, NIC, power supply and server levels, constant content replication, robust backup, restoration and failover capabilities, real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service, with 24/7 on-call engineering teams. Microsoft data center locations are made public on the Microsoft Trust Center
D. SERVICE AGREEMENT ***See also Appendix One to this document which includes a comprehensive list of the different provisions in the various regulations in Malaysia which require FSIs to insert specific contractual provisions into their agreements with outsourcing vendors. The appendix then maps these against the clauses of Microsoft's agreement where these are covered.***		
10.	Has a service agreement ("**SA**") for each of the items, activities, operations, transactions or areas to be outsourced to the Service Provider been established?	*Paragraph 4(iv) of the BNM's Guidelines on Outsourcing of Banking Operations.* Yes. The written contract we have with Microsoft is in the form of an SLA which is available at: **http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37** and a Business and Services Agreement which is available upon request.

Ref.	Question/requirement	Template response and guidance
11.	Does the SA cover the following? (a) Nature and scope of the service provided (i.e., scope of the relationship, frequency, content, agreed roles, responsibilities and duties of Service Provider and location of service to be provided) (b) Protection of confidentiality and security of your organization and your clients' information (i.e. roles and responsibility, liability for losses in the event of breach of security/confidentiality; and requirement for immediate notification if there is a breach) (c) Business resumption and contingency arrangements (d) Reporting requirements (i.e., type, content and frequency of reporting; whether the	*Relevant obligations can be found in different places including: (i) paragraph 4(iv) of the BNM's Circular on Outsourcing of Banking Operations; (ii) paragraph 1(c), Part V of the BNM's Guidelines on Management of IT Environment; (iii) paragraph 4(ix) of the BNM's Circular on Outsourcing of Banking Operations; (iv) paragraph 4(vii) of the BNM's Circular on Outsourcing of Banking Operations; (v) paragraph 4(v) of the BNM's Circular on Outsourcing of Banking Operations; (vi) paragraph 4(iv) of the BNM's Circular on Outsourcing of Banking Operations; (vii) paragraphs 13.3(c) and (d) of the BNM's Guidelines on the Provision of Electronic Banking (e-banking) Services by FSIs; (viii) paragraph 110 of the BNM's BCM Guidelines; and (ix) paragraph 111 of the BNM's BCM Guidelines.* Yes. Taking each of the points in turn: **(a) Nature and scope of services etc:** The contract includes this. See section 2 for an overview of the services which are being provided. **(b) Protection of confidentiality and security:** Microsoft as an outsourcing partner is an industry leader in cloud security and implements policies and controls on par with or better than on-premises data centers of even the most sophisticated organizations. Office 365 was built based on ISO/IEC 27001 standards, a rigorous set of global standards covering physical, logical, process and management controls. This makes us confident that there are very robust security controls in place to protect the transmission and storage of information/data within Microsoft's infrastructure. The following security features are also relevant to protecting the transmission and storage of information/data within the Microsoft infrastructure: **1.** The Microsoft Office 365 security features consist of three parts: (a) built-in security features; (b) security controls; and (c) scalable security. These include 24-hour monitored physical hardware, isolated customer data, automated operations and lock-box processes, secure networks and encrypted data.

Ref.	Question/requirement	Template response and guidance
	performance is met; and reporting of incidents or events that may affect the service; testing and review of work done by the Service Provider; progress of work conducted) (e) Default termination. (f) Service Provider is subject to all applicable regulations and guidelines including BNM's BCM Guidelines. (g) Requirements for ensuring the continuity of the outsourced business function in the event of a major disruption affecting the Service Provider's services (including recovery time objectives ("**RTO**") and provisions for legal liability if the RTO is not achieved).	**2.** Microsoft implements the Microsoft Security Development Lifecycle (**"SDL"**) which is a comprehensive security process that informs every stage of design, development and deployment of Microsoft software and services, including Office 365. Through design requirements, analysis of attack surface and threat modeling, the SDL helps Microsoft predict, identify and mitigate vulnerabilities and threats from before a service is launched through its entire production lifecycle. **3.** Networks within the Office 365 data centers are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Client connections to Office 365 use SSL (as defined above) for securing Outlook, Outlook Web App, Exchange ActiveSync, POP3, and IMAP. Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft data center. These connections are encrypted using industry-standard TLS (as defined above)/SSL. The use of TLS/SSL establishes a highly secure client-to-server connection to help provide data confidentiality and integrity between the desktop and the data center. Customers can configure TLS between Office 365 and external servers for both inbound and outbound email. This feature is enabled by default. Microsoft also implements traffic throttling to prevent denial-of-service attacks. **4.** From a people and process standpoint, preventing breach involves auditing all operator/administrator access and actions, zero standing permission for administrators in the service, "Just-In-Time (JIT) access and elevation" (that is, elevation is granted on an as-needed and only-at-the-time-of-need basis) of engineer privileges to troubleshoot the service, and segregation of the employee email environment from the production access environment. Employees who have not passed background checks are automatically rejected from high privilege access, and checking employee backgrounds is a highly scrutinized, manual-approval process. Data is also encrypted. Further details are included in section F below.

Ref.	Question/requirement	Template response and guidance
		(c) Business resumption and contingency arrangements: There are detailed business contingency provisions. See section G below for more details. **(d) Reporting requirements:** Our IT administrators have access to the **Office** 365 Service Health Dashboard, which provides real-time and continuous monitoring of the Office 365 service. The Service Health Dashboard provides our IT administrators with information about the current availability of each service or tool (and history of availability status) details about service disruption or outage, scheduled maintenance times. The information is provided via an RSS feed. Amongst other things, it provides a contractual 99.9% uptime guarantee for the Office 365 product and covers performance monitoring and reporting requirements which enable us to monitor Microsoft's performance on a continuous basis against service levels. As part of the support we receive from Microsoft, we also have access to a technical account manager who is responsible for understanding our challenges and providing expertise, accelerated support and strategic advice tailored to our organization. This includes both continuous hands-on assistance and immediate escalation of urgent issues to speed resolution and keep mission-critical systems functioning. We are confident that such arrangements provide us with the appropriate mechanisms for managing performance and problems. **(e) Default termination:** The Microsoft Business and Services Agreement (**"MBSA"**) contains usual termination provisions. The SLA is contained with the MBSA is terminable by us for convenience at any time by providing not less than 60 days' notice. Any sub-agreements to the MBSA are terminable by us for convenience at any time by providing not less than 30 days' notice. In addition, we have standard rights of termination for material breach. This gives us the flexibility and control we need to manage the relationship with Microsoft because it means that we can terminate the arrangements whether with or without cause. **(f) Regulations and guidelines on Business Continuity:** As set out in section F below, we have ensured that Microsoft is required to provide robust and comprehensive business continuity management and processes. **(g) Continuity in the event of disruption:** As set out in section F below, we have ensured that Microsoft is

Ref.	Question/requirement	Template response and guidance
		required to provide robust and comprehensive disaster recovery management and processes. Microsoft provides a contractual financially-backed 99.9% uptime guarantee for the Office 365 product and covers performance monitoring and reporting requirements which enable us to monitor Microsoft's performance on a continuous basis against service levels. Under the service credits mechanism in the SLA, we may be entitled to a service credit of up to 100% of the service charges. If a failure by Microsoft also constitutes a breach of contract to which the service credits regime does not apply, we would of course have ordinary contractual claims available to us too under the contract.
E. AUDIT		
12.	Has your organization made explicit provisions in the outsourcing contracts or obtained letters of undertaking from Service Providers to enable regulatory bodies and appointed personnel such as external and internal auditors to carry out inspection or examination of the Service Provider's books, internal controls, facilities, systems, processes and data relating to the services provided to your organization?	*There are various provisions under Malaysia law that require this. In particular see: (i) Section 148(1)(b) of the FSA; (ii) paragraph 4(viii) of the BNM's Circular on Outsourcing of Banking Operations; (iii) paragraph 13.3(f) of the BNM's Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions; (iv) Paragraph 15(c), Part II of the BNM's Guidelines on Management of IT Environment; (v) paragraph 113 of the BNM's BCM Guidelines; and (vi) paragraph 1(c), Part V of the BNM's Guidelines on Management of IT Environment.* Yes. We are confident that in our choice of Microsoft as Service Provider we have far more extensive audit rights than most if not all other Service Provider's offer. This was an important factor in our decision to choose this Service Provider. In particular, the following audit protections are made available by Microsoft: **1.** As part of Microsoft's certification requirements, they are required to undergo regular independent third party auditing (via the SSAE16 SOC1 Type II audit, a globally-recognized standard), and Microsoft shares with us the independent third party audit reports. Microsoft also agrees as part of the compliance program

Ref.	Question/requirement	Template response and guidance
		to customer right to monitor and supervise. We are confident that such arrangements provide us with the appropriate level of assessment of Microsoft's ability to meet our policy, procedural, security control and regulatory requirements. **2.** BNM is given a contractual right of audit/inspection over Microsoft's facilities, so that it can assess and examine systems, processes and security and regulatory compliance. *Microsoft also offers a Compliance Framework Program. If you take-up the Compliance Framework Program, you may add this additional information about its key features: the regulator audit/inspection right, access to Microsoft's security policy, the right to participate at events to discuss Microsoft's compliance program, the right to receive audit reports and updates on significant events, including security incidents, risk-threat evaluations and significant changes to the business resumption and contingency plans.*
F. CONFIDENTIALITY AND SECURITY		
13.	Have you obtained from the Service Provider a written undertaking to protect and maintain the confidentiality of your customer data in compliance with the secrecy provision pursuant to section 133 of the FSA?	*Section 133(1) of the FSA which provides that no person who has access to any document or information relating to the affairs or account of any customer of a FSI, including: (a) the FSI; or (b) any person who is or has been a director, officer or agent of the FSI, shall disclose to another person any document or information relating to the affairs or account of any customer of the FSI. Please also see paragraph 4(iii) of the BNM's Circular on Outsourcing of Banking Operations and paragraph 13.3(e) of the BNM's Guidelines on the Provision of Electronic Banking (e-banking) Services by FSIs.* Yes. Our contract with Microsoft contains robust confidentiality provisions to prevent disclosure of confidential information whether of our customers or of our own. Information will only be provided to Microsoft's sub-contractors on a need to know basis for the purposes of providing the services and subject to similar restrictions on confidentiality. If anything further is required we would work with Microsoft to provide whatever further clarity

Ref.	Question/requirement	Template response and guidance
		the regulator may require in this regard. It is also relevant to note that the European Union's data protection authorities have found that Microsoft's enterprise cloud contracts meet the high standards of EU privacy law. Microsoft is the first – and so far the only – company to receive this approval.
14.	Has senior management determined that there are adequate controls for identifying, reporting and responding to suspected security incidents and violations?	*Paragraph 6(b), Part II of the BNM's Guidelines on Management of IT Environment which provides that the senior management should ascertain that adequate internal controls, prevention measures and early detection of frauds, errors, omissions and other irregularities are in place.* Yes. Senior management is confident that there are adequate internal controls, prevention measures and processes for early detection of errors, omissions and security incidents. Our extensive due diligence and risk profiling at the outset and processes in place for monitoring, auditing and security protections assure us of this. We have set out details of this elsewhere in this document.
15.	Are the following security practices implemented by the Service Provider? (a) Access to security logs and audit trails. (b) Analysis of security logs for suspicious traffic and intrusion attempts. (c) Conducting security	*There are specific security practice requirements contained in Part III of the BNM's Guidelines on Management of IT Environment.* Yes. Taking each of the points in turn: **(a) Access to security logs and audit trails.** In the event that a security incident or violation is detected, Microsoft Customer Service and Support notifies Office 365 subscribers by updating the Service Health Dashboard that is available on the Office 365 portal. In addition, we have extensive audit rights as

Ref.	Question/requirement	Template response and guidance
	awareness education and programs. (d) Providing separate physical/logical environments for systems development, testing and production. (e) Encrypting critical or sensitive information which is stored or transmitted over communication networks.	described in Section E. **(b) Analysis of security logs for suspicious traffic and intrusion attempts.** Microsoft has robust automated processes which are constantly monitoring in this regard. **(c) Conducting security awareness education and programs.** All personnel with access to customer data are subject to background screening, security training and access approvals. In addition, the access levels are reviewed on a periodic basis to ensure that only users who have appropriate business justification have access to the systems. User access to data is also limited by user role. For example, system administrators are not provided with database administrative access. All appropriate Microsoft Staff take part in a Microsoft Online Services sponsored security-training program, and are recipients of periodic security awareness updates when applicable. Security education is an on-going process and is conducted regularly in order to minimize risks. **(d) Providing separate physical/logical environments for systems development, testing and production.** Microsoft has an operational change control procedure in place. The operational change control procedure includes an assessment process of possible change impact change testing in an approved non-production environment. **(e) Encrypting critical or sensitive information which is stored or transmitted over communication networks:** Networks within the Office 365 data centers are segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Edge router security allows the ability to detect intrusions and signs of vulnerability. Client connections to Office 365 use SSL for securing Outlook, Outlook Web App, Exchange ActiveSync, POP3, and IMAP. Customer access to services provided over the Internet originates from users' Internet-enabled locations and ends at a Microsoft data center. These connections are encrypted using industry-standard TLS/SSL. The use of TLS/SSL establishes a highly secure client-to-server connection to help provide data confidentiality and

Ref.	Question/requirement	Template response and guidance
		integrity between the desktop and the data center. Customers can configure TLS between Office 365 and external servers for both inbound and outbound email. This feature is enabled by default. Microsoft also implements traffic throttling to prevent denial-of-service attacks. Customer data in Office 365 exists in two states: (i) at rest on storage media; and (ii) in transit from a data center over a network to a customer device. All email content is encrypted on disk using BitLocker AES (as defined above) encryption. Protection covers all disks on mailbox servers and includes mailbox database files, mailbox transaction log files, search content index files, transport database files, transport transaction log files, and page file OS system disk tracing/message tracking logs. Office 365 also transports and stores secure/multipurpose Internet mail extensions (**"S/MIME"**) messages. Office 365 will transport and store messages that are encrypted using client-side, third-party encryption solutions such as Pretty Good Privacy (**"PGP"**).
16.	How are customers authenticated? For internal systems, how are staff in your organization authenticated?	*Paragraph 2(a), Part III of the BNM's Guidelines on Management of IT Environment. You will need to supplement this with details of your own internal authentication processes for internal systems.* Yes. Office 365 uses two-factor authentication to enhance security. Typical authentication practices that require only a password to access resources may not provide the appropriate level of protection for information that is sensitive or vulnerable. Two-factor authentication is an authentication method that applies a stronger means of identifying the user. The Microsoft phone-based two-factor authentication solution allows users to receive their PINs sent as messages to their phones, and then they enter their PINs as a second password to log on to their services.
17.	Is the Service Provider able to isolate and clearly identify your customer	*Paragraph 6(b), Part II of the BNM's Guidelines on Management of IT Environment and FSA as above.*

Ref.	Question/requirement	Template response and guidance
	data, documents, records and assets to protect their confidentiality?	Yes. Microsoft's transparency as to data location was a key consideration as part of the service provider selection process. Active Directory isolates customers using security boundaries (also known as silos). This safeguards a customer's data so that the data cannot be accessed or compromised by co-tenants.
18.	Are there documented system for monitoring and managing the computer center's resources (i.e. utilization of the central processing unit (**"CPU"**), hard disk and memory, problem reporting and prioritization, equipment malfunctions, frequency and duration of system down time and network activities to detect suspicious trends and attempts to gain access to the system)?	*See paragraph 3(g), Part V of the BNM's Guidelines on Management of IT Environment.* Yes. The security procedures for safeguarding hardware, software and security are documented in detail by Microsoft in its Standard Response to Request for Information – Security and Privacy. This confirms how the following aspects of Microsoft's operations safeguard hardware, software and data: • Compliance; • Data Governance; • Facility; • Human Resources; • Information Security; • Legal; • Operations;

Ref.	Question/requirement	Template response and guidance
		• Risk Management; • Release Management; • Resiliency; and • Security Architecture.
19.	Are the following physical and environmental controls available at the data center? (a) All computer and telecommunications peripherals adequately labeled for proper identification (b) Uninterruptible power supply (c) Air conditioning system (d) Temperature sensor (e) Fire detector (f) Smoke detector	*Part V of the BNM's Guidelines on Management of IT Environment.* Yes. Taking each one in turn: **(a) All computer and telecommunications peripherals adequately labeled for proper identification.** Yes. **(b) Uninterruptible power supply ("UPS").** Microsoft's data centers have dedicated 24x7 UPS and emergency power support, i.e. generators. Regular maintenance and testing is conducted for both the UPS and generators. Data centers have made arrangements for emergency fuel delivery. The data centers have dedicated Facility Operations Centers to monitor the power systems, including all critical electrical components – generators, transfer switch, main switchgear, power management module and UPS equipment. **(c) Air conditioning system.** Microsoft has implemented environmental controls to protect the data centers including ventilation and air conditioning. **(d) Temperature sensor.** Microsoft has implemented environmental controls to protect the data centers

Ref.	Question/requirement	Template response and guidance
	(g) Fire suppression system (h) Raised floor (i) Water leakage detection system	including temperature control and heating. The data centers' Facility Operations Centers monitor the heating, ventilation and air conditioning system, which controls and monitors space temperature and humidity within the data centers, space pressurization and outside air intake. **(e) Fire detector.** Fire Detection and Suppression systems exist at all Microsoft's data centers. Additionally, portable fire extinguishers are available at various locations in the data center. Routine maintenance is performed on facility and environmental protection equipment. **(f) Smoke detector.** See above. In addition, Microsoft's equipment is placed in environments which have been engineered to be protective from environmental risks such as smoke. **(g) Fire suppression system.** Fire Detection and Suppression systems exist at all Microsoft's data centers. Additionally, portable fire extinguishers are available at various locations in the data center. Routine maintenance is performed on facility and environmental protection equipment. **(h) Raised floor.** Microsoft's equipment is placed in environments which have been engineered to be protective from environmental risks such as water. **(i) Water leakage detection system.** Microsoft has water leakage detection systems for water-cooling data centers.
20.	Who is primarily in charge of security administration and systems access functions?	*Paragraph 1(e), Part III of the BNM's Guidelines on Management of IT Environment which provides that a security administrator and/or a system administrator who are responsible for the system security and/or administration functions and to implement policies as well as adopted standards, should be formally appointed.* Overall responsibility for these matters remains with our organization and we have procedures in place to monitor overall performance. Our [security administrator/system administrator is *insert name*].

Ref.	Question/requirement	Template response and guidance
		Microsoft will perform the *technical* monitoring and management functions on our behalf. System level data such as configuration data/file and commands are managed as part of the configuration management system. Any changes or updates to or deletion of those data/files/commands will be automatically deleted by the configuration management system as anomalies. We will receive information about system integrity, security monitoring and network performance through the Office 365 Service Health Dashboard, as described above.
G. DATA BACKUP AND DISASTER RECOVERY		
21.	Does the Service Provider have a fully documented and adequately resourced business continuity plan (**"BCP"**) and disaster recovery plan (**"DRP"**)? If yes, provide documentation or details.	*Paragraph 112 of the BNM's BCM Guidelines.* Yes. Microsoft offers contractually-guaranteed 99.9% uptime, globally available data centers for primary and backup storage, physical redundancy at disk, NIC, power supply and server levels, constant content replication, robust backup, restoration and failover capabilities, real-time issue detection and automated response such that workloads can be moved off any failing infrastructure components with no perceptible impact on the service, 24/7 on-call engineering teams. Microsoft's arrangements are as follows: **Redundancy** • Physical redundancy at server, data center, and service levels; • Data redundancy with robust failover capabilities; and

Ref.	Question/requirement	Template response and guidance
		• Functional redundancy with offline functionality. **Resiliency** • Active load balancing; • Automated failover with human backup; and • Recovery testing across failure domains. **Distributed Services** • Distributed component services like Exchange Online, SharePoint Online, and Lync Online limit scope and impact of any failures in a component; • Directory data replicated across component services insulates one service from another in any failure events; and • Simplified operations and deployment. **Monitoring** • Internal monitoring built to drive automatic recovery; • Outside-in monitoring raises alerts about incidents; and • Extensive diagnostics provide logging, auditing, and granular tracing.

Ref.	Question/requirement	Template response and guidance
		Simplification • Standardized hardware reduces issue isolation complexities; • Fully automated deployment models; and • Standard built-in management mechanism. **Human backup** • Automated recovery actions with 24/7 on-call support; • Team with diverse skills on the call provides rapid response and resolution; and • Continuous improvement by learning from the on-call teams. **Continuous learning** • If an incident occurs, Microsoft does a thorough post-incident review every time; and • Microsoft's post-incident review consists of analysis of what happened, Microsoft's response, and Microsoft's plan to prevent it in the future. For the avoidance of doubt, the nature of the services provided as part of Office 365 does not give rise to a risk that the Bank itself could become "offline" (i.e. there would be no implication for core banking functions such as transaction processing).
22.	What are the data backup and recovery arrangements for your	*Paragraph 71 of the BNM's BCM Guidelines, which states that an institution should make available a functional alternate and recovery site for their business functions and technology in the event the business premises, key*

Ref.	Question/requirement	Template response and guidance
	organization's data that reside with the Service Provider?	*infrastructure and systems supporting critical business functions become unavailable. Pursuant to paragraph 110 of the BNM's BCM Guidelines, the institution should ensure that the service provider is subjected to the BCM Guidelines, where appropriate. Therefore, the service provider should ensure that it has a functional alternate and recovery site.* See response directly above for details.
23.	Has a testing of the BCP and DRP of the Service Provider been conducted?	*Paragraph 112 of the BNM's BCM Guidelines which provides that the institution should ensure that periodic testing is conducted by the outsourcing vendor on its BCP and DRP at least annually and twice a year, respectively.* Yes. Microsoft carries out disaster recovery testing at least once per year. In addition, as part of Microsoft's certification requirements, it is required to undergo regular independent third party auditing and Microsoft shares with us the independent third party audit reports. These reports will include details of the BCP and DRP testing.
24.	How frequently does the Service Provider conduct tests on its BCP and DRP?	*Paragraph 112 of the BNM's BCM Guidelines which provides that periodic testing should be conducted by the outsourcing vendor at least twice a year on its BCP and DRP, respectively.* Microsoft carries out disaster recovery testing at least once per year.
25.	Does your organization's BCP address the reasonably foreseeable situations in the event that the Service Provider fails to provide the required services, causing disruptions to your	*Paragraph 115 of BNM's BCM Guidelines which provides that the institution's own BCP should address reasonably foreseeable situations where the outsourcing vendor fails to provide the required services, causing disruptions to the institution's operations. See also paragraph 13.3(g) of the BNM's Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions which requires you to have appropriate contingency plans.*

Ref.	Question/requirement	Template response and guidance
	organization's operations?	*Note, this question, primarily concerns your own internal BCP. If you have any questions or we can help in any way, just let us know.*
26.	Have you tailored and tested your disaster recovery or business continuity plan?	*Part B.2.9 of the BNM's BCM Guidelines which provides for the testing of the BCP and DRP by the institution. BCP should be tested at least once a year for all critical business functions, while the DRP for all critical application systems should be tested at least twice a year, of which one of the tests should be a "live run".* *This question concerns your own testing as opposed to that which Microsoft carries out. You will need to be able to demonstrate that you comply with the requirements set out above in terms of frequency of testing.*
27.	Is the Service Provider required to notify you in the event that it makes significant changes to its BCP and DRP, or encounters other circumstances that might have a serious impact on its services?	*Paragraph 114 of the BNM's BCM Guidelines.* Yes. Microsoft will inform us if there are any important changes to the service with respect to security, privacy, and compliance. Microsoft will also promptly notify us if your data has been accessed improperly. In the event that a security incident or violation is detected, Microsoft Customer Service and Support notifies Office 365 subscribers by updating the Service Health Dashboard that is available on the Office 365 portal. We would have access to Microsoft's dedicated support staff, who have a deep knowledge of the service. Microsoft provides a Recovery Time Objective (RTO) of 1 hour or less for Microsoft Exchange Online and 6 hours of less for SharePoint Online, and a Recovery Point Objective (RPO) of 45 minutes or less for Microsoft Exchange Online and 2 hours or less for SharePoint Online. Finally, after the incident, Microsoft provides a thorough post-incident review report (PIR). The PIR includes: • An incident summary and event timeline.

Ref.	Question/requirement	Template response and guidance
		• Broad customer impact and root cause analysis. • Actions being taken for continuous improvement. Microsoft will provide the PIR within five business days following resolution of the service incident. Administrators can also request a PIR using a standard online service request submission through the Office 365 portal or a phone call to Microsoft Customer Service and Support.
28.	What are the RTO (as defined above) of systems or applications outsourced to the Service Provider?	*Part G of the BNM's BCM Guidelines, 'Recovery Time Objective'.* RTO: 1 hour or less for Microsoft Exchange Online, 6 hours or less for SharePoint Online.
H. EXIT STRATEGY		
29.	Do you have the right to terminate the SA in the event of default?	*Paragraph 4(v) of the BNM's Guidelines on Outsourcing of Banking Operations which provides that banks must have the right to terminate the SA if the Service Provider fails to comply with the conditions in the SA.* Yes. Our main agreement with Microsoft contains usual termination provisions. The SLA is contained with the MBSA is terminable by us for convenience at any time by providing not less than 60 days' notice. Any sub-agreements to the MBSA are terminable by us for convenience at any time by providing not less than 30 days' notice. In addition, we have standard rights of termination for material breach. This gives us the flexibility and control we need to manage the relationship with Microsoft because it means that we can terminate the arrangements whether with or without cause.
30.	Is there a contingency plan for replacing the Service Provider in the	*Paragraph 4(ix) of BNM's Circular on Outsourcing of Banking Operations.*

Ref.	Question/requirement	Template response and guidance
	event of its cessation?	Yes. In the event of cessation, we would either move back on premise or to an alternate Cloud Service Provider (**"CSP"**). Microsoft is contractually required to hold our data for an agreed period to enable such transition to occur in an orderly manner.

APPENDIX ONE

MANDATORY CONTRACTUAL REQUIREMENTS

This table sets out the specific items that must be covered in the FSI's agreement with the Service Provider.

Key:

Where relevant, a cross-reference is included in *red italics* to the underlying regulation that sets out the contractual requirement.

In blue text, Microsoft has provided you with a reference to where in the agreement the contractual requirement is covered for ease of reference.

Terms used below as follows:

OST = *Online Services Terms*

EA = *Enterprise Agreement*

Enrolment = *Enterprise Enrolment*

FSA = *Financial Services Amendment*

MBSA = *Microsoft Business and Services Agreement*

PUR = *Product Use Rights*

SLA = *Online Services Service Level Agreement*

Ref.	Requirement	Microsoft agreement reference
1.	The Service Provider should provide a written undertaking to protect and maintain the confidentiality of your customer data in compliance with the secrecy provision pursuant to section 133 of the FSA.	*Section 133 of the FSA; Paragraph 4(iii) of the BNM's Circular on Outsourcing of Banking Operations; and Paragraph 13.3(e) of the BNM's Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions* Yes. MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose our confidential information (which includes our data) to third parties and to only use our confidential information for the purposes of Microsoft's business relationship with us. If there is a breach of confidentiality by Microsoft, we are able to bring a claim for breach of contract against Microsoft. MBSA section 11m states that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations. The customer retains the ability to access its Customer Data at all times (OST, page 10), and Microsoft will deal with Customer Data in accordance with Enrollment and the OST. In summary: following termination Microsoft will (unless otherwise directed by the customer) delete the Customer Data after a 90 day retention period. Finally, from a technical perspective the wide availability and usage of Microsoft's products means that Customer Data can generally be extracted in a format compatible with commonly available alternative products Microsoft also makes specific commitments with respect to Customer Data in

Ref.	Requirement	Microsoft agreement reference
		the OST. In summary Microsoft commits that: 1. Ownership of Customer Data remains at all times with the customer (see OST, page 8). 2. Customer Data will only be used to provide the online services to the customer. Customer Data will not be used for any other purposes, including for advertising or other commercial purposes (see OST, page 8). 3. Microsoft will not disclose Customer Data to law enforcement unless it is legally obliged to do so, and only after not being able to redirect the request to the customer (see OST, page 8). 4. Microsoft will implement and maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction (see OST, page 8 and pages 11-13 for more details). 5. Microsoft will notify the customer if it becomes aware of any security incident, and will take reasonable steps to mitigate the effects and minimize the damage resulting from the security incident (see OST, page 9). Microsoft commits to reimburse customer's reasonable remediation costs incurred as a consequence of a security incident involving Customer Data

Ref.	Requirement	Microsoft agreement reference
		(see FSA under "Security Incident Notification").
2.	The service agreement should include a clause on professional ethics and conduct in relation to the Service Provider's performance of its duties.	*Paragraph 4(iv) of the BNM's Circular on Outsourcing of Banking Operations* Yes. MBSA section 4(a)(i) deals with professional conduct. Microsoft warrants that its services will be performed with professional care and skill.
3.	The service agreement should clearly define the contractual accountability of the parties e.g. responsibilities for providing information to and receiving information from the Service Provider.	*Paragraph 13.3(c) of the BNM's Guidelines on the Provision of Electronic Banking (e-banking) Services by Financial Institutions* Yes. The contract pack comprehensively sets out the scope of the arrangement and the respective commitments of the parties. The services are broadly described, along with the applicable usage rights, in the OST. The services are described in more detail in the OST, which includes a list of service functionality at OST, page 10 and core features of the Office 365 Services at pages 15-25. The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. This commitment is reiterated in the FSA. The customer may monitor the performance of the online services via the administrative dashboard, which includes real time information as to Microsoft

Ref.	Requirement	Microsoft agreement reference
		compliance with its SLA commitments. In addition, in our agreement with Microsoft, it agrees that it will notify us if it becomes aware of any security incident, and will take reasonable steps to mitigate the effects and minimize the damage resulting from the security incident (see OST, page 9). We can also review the manner in which Microsoft provides the online services. As set out on page 13 of the OST, the customer is entitled to access the Microsoft Online Information Security Policy, which is the document where Microsoft sets out its information security management processes. Microsoft also commits to providing the customer with a summary of Microsoft's annual audit report, which is performed by an independent third party and measures compliance against Microsoft's certifications. Finally, Clause 1f of the FSA gives the customer the opportunity to participate in the Microsoft Online Services Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to (a) assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with additional notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services.
4.	The service agreement should specify the requirements for ensuring the continuity of the outsourcing vendor's services. Recovery time objectives (**"RTO"**) should be built into the outsourcing contract with provisions for legal liability should the RTO not be achieved.	*Paragraph 111, BCM Guidelines* Yes. Business Continuity Management forms part of the scope of the accreditation

Ref.	Requirement	Microsoft agreement reference
		that Microsoft remains in relation to the online services, and Microsoft commits to maintain a data security policy that complies with these accreditations (see OST page 13). Business Continuity Management also forms part of the scope of Microsoft's annual third party compliance audit. RTO requirements are set out in the SLA and this also includes the provision for service credits if Microsoft fails to meet the commitments in the SLA. If a failure by Microsoft also constitutes a breach of contract to which the service credits regime does not apply, we would of course have ordinary contractual claims available to us too under the contract.
5.	Service agreements for contracted services should clearly prohibit the unauthorized disclosure of confidential data by the external party and provide for adequate remedies.	*Paragraph 4.25, Guidelines on Data Management and MIS Framework* Yes. MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose our confidential information (which includes our data) to third parties and to only use our confidential information for the purposes of Microsoft's business relationship with us. If there is a breach of confidentiality by Microsoft, we are able to bring a claim for breach of contract against Microsoft.
6.	The written, enforceable agreement should set out the governing roles, relationships, obligations and responsibilities of all contracting parties. It should also cover: performance expectations, service levels, availability, reliability, scalability, compliance, security and confidentiality, back processes facility, contingency planning, right to audit contractual	*Section II, paragraph 15(c), Guidelines on Management of IT Environment* Yes.

Ref.	Requirement	Microsoft agreement reference
	responsibilities and discontinuation of services and returning all information.	All of these points are covered, taking each in turn: 1. The contract pack comprehensively sets out the scope of the arrangement and the respective commitments of the parties. The services are broadly described, along with the applicable usage rights, in the Product List and the OST. The services are described in more detail in the OST, which includes a list of service functionality at OST, page 10 and core features of the Office 365 Services at pages 15-25. 2. The SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment. 3. MBSA section 11m states that Microsoft and the customer each commit to comply with all applicable privacy and data protection laws and regulations. 4. Microsoft also makes specific commitments with respect to Customer Data in the OST, including that Microsoft will implement and maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction (see OST, page 8 and pages 11-13 for more details). 5. MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose our confidential information (which includes our data) to third parties and to only use our confidential information for the purposes of Microsoft's business relationship with

Ref.	Requirement	Microsoft agreement reference
		us. If there is a breach of confidentiality by Microsoft, we are able to bring a claim for breach of contract against Microsoft. 6. Business Continuity Management forms part of the scope of the accreditation that Microsoft remains in relation to the online services, and Microsoft commits to maintain a data security policy that complies with these accreditations (see OST page 13). 7. The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. This commitment is reiterated in the FSA. 8. Online services may also be terminated or suspended in the circumstances described in section 6d of the EA, and as specified in the OST, pages 5, 11 and 30. The contract also allows the customer to terminate the arrangement with Microsoft for convenience (MBSA section 8). 9. Microsoft contractually commits to retain our data stored in the Online Service in a limited function account for 90 days after expiration or termination of our subscription so that we may extract the data. After the 90 day retention period ends, Microsoft will disable our account and delete our data (OST, page 5).
7.	The agreement should explicitly mention BNM's right to independently assess, when necessary and regardless of the location, the competence and the operational and financial performance of the service provider.	*Section II, paragraph 15(c), Guidelines on Management of IT Environment* Yes. The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security

Ref.	Requirement	Microsoft agreement reference
		and compliance standards. This commitment is reiterated in the FSA. In addition, clauses 1e and 1f of the Financial Services Amendment detail the examination and influence rights that are granted to the customer and BNM. Clause 1e sets out a process which can culminate in the regulator's examination of Microsoft's premises. Clause 1f gives the customer the opportunity to participate in the Microsoft Online Services Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to (a) assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with additional notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services.
8.	The agreement should be legally binding. It should outline all expected service levels and the agreement is properly executed to protect the institution's interests.	*Part IV, paragraph 1(e), Guidelines on Management of IT Environment* Yes. The contractual documents are all written and clear and legally binding. The SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment. The terms of the SLA current at the start of the applicable initial

Ref.	Requirement	Microsoft agreement reference
		or renewal term of the Enrollment are fixed for the duration of that term.
9.	The agreement should be legally binding and properly executed. The agreement should oblige vendors to comply with good business practices that maintain the confidentiality and integrity of information and permit their activities to be audited.	*Part V, paragraph 1(c), Guidelines on Management of IT Environment* Yes. The contractual documents are all written and clear and legally binding. The agreement is signed. MBSA section 4(a)(i) deals with professional conduct. Microsoft warrants that its services will be performed with professional care and skill. MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose our confidential information (which includes our data) to third parties and to only use our confidential information for the purposes of Microsoft's business relationship with us. If there is a breach of confidentiality by Microsoft, we are able to bring a claim for breach of contract against Microsoft. The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. This commitment is reiterated in the FSA.
10.	If communications services are obtained from external service providers, the institution should ensure that the roles and responsibilities and expected service levels are defined in formal and enforceable agreements. The agreement should specific arrangements for ensuring	*Part VI, paragraph 3(c), Guidelines on Management of IT Environment* Yes.

Ref.	Requirement	Microsoft agreement reference
	continuity of service (i.e. detection and recovery from service interruptions).	The contract pack comprehensively sets out the scope of the arrangement and the respective commitments of the parties. The SLA contains Microsoft's service level commitment, as well as the remedies for the customer in the event that Microsoft does not meet the commitment. Business Continuity Management forms part of the scope of the accreditation that Microsoft remains in relation to the online services, and Microsoft commits to maintain a data security policy that complies with these accreditations (see OST page 13). Business Continuity Management also forms part of the scope of Microsoft's annual third party compliance audit.
11.	The agreement should be legally binding and properly executed to protect the institution's interests. The agreement should oblige vendors to comply with good business practices that maintain the confidentiality and integrity of information, provide regular reports on network performance, maintain continuity of services in the event of a disaster and permit the vendor's activities to be audited.	*Part VI, paragraph 3(e), Guidelines on Management of IT Environment* Yes. The contractual documents are all written and clear and legally binding. All of these points are covered, taking each in turn: 1. MBSA section 4(a)(i) deals with professional conduct. Microsoft warrants that its services will be performed with professional care and skill. 2. MBSA section 3 deals with confidentiality. Under this section Microsoft commits not to disclose our confidential information (which includes our data) to third parties and to only use our confidential information for the purposes of Microsoft's business relationship with us. If there is a breach of confidentiality by Microsoft, we are able to

Ref.	Requirement	Microsoft agreement reference
		bring a claim for breach of contract against Microsoft. 3. The customer may monitor the performance of the online services via the administrative dashboard, which includes real time information as to Microsoft compliance with its SLA commitments. 4. Business Continuity Management forms part of the scope of the accreditation that Microsoft remains in relation to the online services, and Microsoft commits to maintain a data security policy that complies with these accreditations (see OST page 13). 5. The OST specifies the audit and monitoring mechanisms that Microsoft puts in place in order to verify that the online services meet appropriate security and compliance standards. This commitment is reiterated in the Financial Services Amendment. Clause 1f of the Financial Services Amendment gives the customer the opportunity to participate in the Microsoft Online Services Customer Compliance Program, which is a for-fee program that facilitates the customer's ability to (a) assess the services' controls and effectiveness, (b) access data related to service operations, (c) maintain insight into operational risks of the services, (d) be provided with additional notification of changes that may materially impact Microsoft's ability to provide the services, and (e) provide feedback on areas for improvement in the services.