# SRI LANKA – BANKS

# GUIDANCE ON COMPLYING WITH REGULATORY REQUIREMENTS APPLICABLE TO FINANCIAL SERVICES INSTITUTIONS USING CLOUD COMPUTING (AZURE)

Last updated: November 2014

## 1. WHAT DOES THIS MICROSOFT GUIDANCE CONTAIN?

1.1 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 banks ("**FSIs**").

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 the mandatory contractual requirements required by relevant regulation.

Note that this document is not intended as legal or regulatory advice and does not constitute any warranty or contractual commitment on the part of Microsoft or its affiliates. Instead, it is intended to streamline the process for you. You should seek independent legal advice on your technology

outsourcing project and your legal and regulatory obligations. If you have any questions, please do not hesitate to get in touch with your Microsoft contact.

## 2. WHAT REGULATIONS AND GUIDANCE ARE RELEVANT?

CBSL issued a direction on outsourcing by banks, the 'Banking Act Directions No.2 of 2012 Outsourcing of Business Operations of a Licensed Commercial Bank and a Licensed Specialised Bank', on 21 December 2012 (the **"Banking Act Directions No.2 of 2012"**) which contains important details about activities which can and cannot be outsourced and the way in which such outsourcing arrangements should be managed.

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

The Central Bank of Sri Lanka (**"CBSL"**)

## 4. IS REGULATORY APPROVAL REQUIRED IN SRI LANKA?

No.

CBSL does not require approval before banks in Sri Lanka outsource IT functionality to a cloud services solution such as Microsoft Azure.

## 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 a bank must complete when considering cloud computing solutions.

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

Yes.

CBSL does stipulate some specific points that Banks must ensure are incorporated in their outsourcing contracts. These are set out in section 4(1)(viii) of the Banking Act Directions No.2 of 2012. We have incorporated responses to these points in the main document and in Appendix One we have mapped the specific requirements against the sections in the Microsoft document where you will find them addressed.

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. The suggested responses may provide sufficient detail but if you require further information, Microsoft will be happy to provide this if you get in touch with your Microsoft contact. 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. INFORMATION REQUIRED FOR ANNUAL NOTIFICATION TO CBSL**<br><br>***A bank must inform CBSL of the proposed outsourcing arrangements for each calendar year by 31 January of that year. The format that must be used to provide this information is set out in the Annex to the Banking Act Directions No.2 of 2012.*** | | |
| 1. | Activity/function/process to be outsourced | *Banking Act Directions No.2 of 2012, section 9(1) and Annex.*<br><br>Certain IT functions will be outsourced through the use of Microsoft's "Azure" cloud-based service, which is described in more detail here: Azure.<br><br>We will not be outsourcing any core or inherent banking functions such as services associated with acceptance of deposits and withdrawals or sanctioning of loans.<br><br>We are therefore satisfied that the IT functions being outsourced fall within the permitted functions set out in section 3(4) of the Banking Act Directions No.2 of 2012. |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| 2. | Name of service provider | *Banking Act Directions No.2 of 2012, section 9(1) and Annex.*<br><br>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. |
| 3. | Address of service provider | *Banking Act Directions No.2 of 2012, section 9(1) and Annex.*<br><br>1 Marina Boulevard #22-01, One Marina Boulevard, Singapore, 018989. |
| 4. | Data of commencement | *Banking Act Directions No.2 of 2012, section 9(1) and Annex. You will need to insert details of the date on which you signed up for Azure (i.e. the commencement date of the service). If you have any questions, please reach out to your Microsoft contact.* |
| 5. | Period | *Banking Act Directions No.2 of 2012, section 9(1) and Annex. You will need to insert details of the term for which you have signed up for Azure. If you have any questions, please reach out to your Microsoft contact.* |
| 6. | No of persons involved/authorized | *Banking Act Directions No.2 of 2012, section 9(1) and Annex.*<br><br>Microsoft is providing the service. Microsoft does use sub-contractors to provide certain ancillary assistance, but not for any critical path roles. An up-to-date list of all subcontractors used to provide the ancillary services (including exact services) is available at http://azure.microsoft.com/en-us/support/trust-center/. |
| 7. | Deliverables/services | *Banking Act Directions No.2 of 2012, section 9(1) and Annex.* |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | Amongst other things, the Microsoft Azure service includes:<br><br>• Compute<br>• Data & Storage<br>• Networking<br>• Identity & Access Management<br>• IT support services.<br><br>The Azure service is described in more detail here: Azure. |
| 8. | Cost (per annum) | *Banking Act Directions No.2 of 2012, section 9(1) and Annex. You will need to insert details of the charges for your Azure service per year. If you have any questions, please reach out to your Microsoft contact.* |
| **B. GENERAL** | | |
| 9. | Please confirm that you will not be outsourcing the following operations or functions:<br><br>(a) Services associated with acceptance of deposits and withdrawals;<br><br>(b) Assets and liabilities management; | *Banking Act Directions No.2 of 2012, section 3(1). The list of permitted IT functions that can be outsourced is contained in section 3(4).*<br><br>None of these functions or operations will be outsourced or affected by the outsourcing. The outsourcing in our view falls within the activities set out in section 3(4) and will comprise only the services set out in section A above. |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | (c) Compliance function;<br><br>(d) Customer due diligence and know your client procedures;<br><br>(e) Treasury functions, foreign exchange trading and management;<br><br>(f) Risk management;<br><br>(g) Strategic planning and decision-making;<br><br>(h) Sanctioning of loans except where the basis of approval has been previously approved by the board;<br><br>(i) Internal audit functions; or<br><br>(j) Information technology related services other than those which are on the permitted list. | |
| **C. OUTSOURCING POLICY AND SELECTION OF SERVICE PROVIDER** | | |
| 10. | Do you have a comprehensive policy to guide your assessment as to how your operations are to be outsourced? | *Banking Act Directions No.2 of 2012, section 4(1).*<br><br>*CBSL requires that banks have in place a comprehensive policy on outsourcing. The Banking Act Directions No.2 of 2012, section 4(1) do not provide a lot of detail on the policy other than a list of* |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | *areas which they would expect to see covered in such a policy and which are set out in the next sections. Policies will of course differ from one organization to another and we have provided below some information and template responses that may be useful for you to include in your policy to show that the specific areas that CBSL are concerned with are covered.* |
| | Does your policy contain at least the following: | *Banking Act Directions No.2 of 2012, section 4(1).* |
| 11. | (i) The placing of overall responsibility on the Board of Directors or the Audit Committee and senior management for the outsourcing of activities and for the formulation of policy therefor. | *Banking Act Directions No.2 of 2012, section 4(1)(i). The CBSL wants to ensure that there is requisite senior oversight and responsibility for the outsourcing. It may be useful in this section to expand to outline the approval process that you went through with senior management and any specific directors and other senior managers who were involved and will be responsible.*<br><br>Yes.<br><br>Overall responsibility for the outsourcing activities rests with *[insert details]*. [The Board of Directors] has signed off on our outsourcing policy and the specific outsourcing arrangement with Microsoft that we are entering into.<br><br>Essential to us is that, despite the outsourcing, we retain control over our own business operations, including control and oversight 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 mandatory provisions required by CBSL. At a practical level, we have selected the Azure 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 Azure services. |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| 12. | (ii) A framework for identification and effective management of risks that could arise from outsourcing of activities. | *Banking Act Directions No.2 of 2012, section 4(1)(ii). Below are some common risk issues that Banks seek to address in their policy and analysis. You will need to amend as relevant to reflect your own framework.*<br><br>Yes.<br><br>Our policy requires consideration of various different potential risks. We set out below the key areas of risk and how we believe they are addressed in the context of this proposed outsourcing:<br><br>• **Strategic risks.** We have no reason to believe that any activities carried out by the Service Provider on its own behalf would be inconsistent with our overall strategic goals. Quite the contrary, we have selected a Service Provider with a very strong track record and experience of understanding the requirements of financial institutions. We are also very confident that the contractual protections and nature of the service offering enable us to have appropriate oversight of the Service Provider and tools which are very easy to use to ensure this oversight as opposed to demanding the development of new skillsets and high levels of expertise in order to manage it on our side. Microsoft will not have interactions with customers. The strategic risks in our view are therefore low.<br><br>• **Reputational risks.** Again, we see the risks as very low since we have undertaken a very thorough due diligence process and chosen a world-class and highly experienced Service Provider who is able to provide contractually backed up assurances of quality of service. We also have numerous protections in the contract itself in order to monitor the service performance and take action in the event that any issues arise.<br><br>• **Compliance risks.** We are not outsourcing core business activities. In that respect the risks of market conduct regulations not being complied with purely as a result of these outsourced services are very low. There are very strong security arrangements and safeguards in place to |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | prevent any damage to customer data confidentiality.<br><br>• **Operational risks.** The service provides high service level agreement (**"SLA"**) commitments but also ensures that a raft of different safeguards and arrangements are in place to prevent and minimize the impact of any technology failure. Microsoft is subject to very high international auditing standards in this regard which provide us with a great deal of comfort. The size and resources that Microsoft has in place also mean that we do not foresee risks in relation to the adequacy of Microsoft to fulfill obligations or provide remedies and restitution. The nature of the services that are being outsourced also mean that there are low risks of fraud or error. In relation to risks in respect of our failure to undertake inspections (for practical or cost considerations) we have assurance in the fact that Microsoft is also subject to its own regular reviews as well as independent auditing by a third party – the reports of which are made available to us.<br><br>• **Exit strategy risks.** Our contract with Microsoft provides various opportunities to terminate the service even at short notice as well as contractual obligations on the part of Microsoft to enable the transfer of services to another service provider or back in-house. These are not services which would commonly be provided by any Bank in-house in any event however.<br><br>• **Counter party risks.** We do not see any risks in relation to inappropriate credit assessments given the nature of the services being outsourced.<br><br>• **Country risks.** We carefully considered the location risks relevant to the service. We are comfortable that the risks are low for several reasons. First, Microsoft informs us that it takes a regional approach to hosting of Azure data. For customers like us with a presence in the Asia-Pacific region, the applicable Azure services will be hosted out of Microsoft's highly-secure data centers that have been selected by Microsoft taking into careful account the country and socio-economic factors. Microsoft data center locations are made public on the Microsoft Trust |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | Center. Second, we took into account that the Microsoft data centers have been built in seismically safe zones. Environmental controls have been implemented to protect the data centers including temperature control, heating, ventilation and air-conditioning, fire detection and suppression systems and power management systems, 24-hour monitored physical hardware and seismically-braced racks. These requirements are covered by Microsoft's ISO/IEC 27001 accreditation for Azure. Azure offers data-location transparency so that the organizations and regulators are informed of the jurisdiction(s) in which data is hosted. We are confident that Microsoft's data center locations offer extremely stable political and socio-economic environments with robust and transparent legal frameworks.<br><br>• **Contractual risks.** We are not concerned regarding any inability to enforce the contract since it contains various remedies including service credits and also the ability to terminate the service quickly and easily.<br><br>• **Information risks.** We do not foresee risks connected with inaccurate information provided by the Service Provider given the nature of the services that are being provided. Further, in relation to any information that is provided to us by Microsoft, we have assurances in the fact that the**y** are subject to independent audit and international standards and also that we and CBSL have audit rights. Microsoft's service ensures the provision of real-time information via their dashboard and various protections detailed elsewhere in this document to ensure the protection of commercially sensitive and customer information. |
| 13. | (iii) Cost-benefit analysis on each activity or function or process to be outsourced. | *Banking Act Directions No.2 of 2012, section 4(1)(iii). You will need to include here details of any financial analysis and forecasting that you have conducted in relation to your business requirements and this specific outsourcing.* |
| 14. | (iv) Tender procedures to be followed for the procurement of outsourced | *Banking Act Directions No.2 of 2012, section 4(1)(iv).* |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | services. | Yes.<br><br>We do have specific tender processes for outsourcing arrangements. These include the following:<br><br>***[You will need to insert details of how you run your specific tender processes.]***<br><br>An important part of our tender processes is our robust due diligence that we conduct on all potential service providers. More details of this process can be seen in section 22 below. |
| 15. | (v) Setting up of a monitoring and control unit in the event of having several outsourcing arrangements. | *Banking Act Directions No.2 of 2012, section 4(1)(v).*<br><br>Yes.<br><br>Monitoring and control is very important to us and the facilities that Microsoft provides in this respect was a key factor in our decision making. This outsourcing will provide us with the following monitoring and control functions:<br><br>• Microsoft's SLA applies to the Azure product. Our IT administrators also have access to the Azure Service Health Dashboard, which provides real-time and continuous monitoring of the Azure 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.<br><br>• Amongst other things, it provides a contractual uptime guarantee for the Azure product and covers performance monitoring and reporting requirements which enable us to monitor Microsoft's performance on a continuous basis against service levels. |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | • 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.<br><br>• We also have extensive audit rights which go beyond those offered by other service providers. In particular, the following audit protections are made available by Microsoft:<br><br>**(i)** 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 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.<br><br>**(ii)** CBSL 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.<br><br>**(iii)** As a customer, we also have a contractual right of audit/inspection of Microsoft so that we can also assess and examine compliance with agreed policies, procedures, security controls and regulatory requirements. |
| 16. | (vi) A framework to conduct KYC and due diligence process of the service | *Banking Act Directions No.2 of 2012, section 4(1)(vi).* |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | provider. | This is not applicable to this outsourcing arrangement. |
| 17. | (vii) A procedure to assess the service provider's capacity, capability and mode/basis of payment to perform the obligations under the outsourcing arrangement. | *Banking Act Directions No.2 of 2012, section 4(1)(vii).*<br><br>Yes.<br><br>We followed a rigorous review and assessment process. Section 22 below details the specific areas we considered and Microsoft's capacity and capability against these. |
| 18. | (viii) A format of the legally binding contract/agreement for outsourcing arrangement which should include at least the following:<br><br>• Service standards;<br><br>• Rights, responsibilities and expectations of all parties;<br><br>• Dispute resolution mechanism;<br><br>• Confidentiality and security of information;<br><br>• Termination of contract;<br><br>• Sub-contracting if involved; and | *Banking Act Directions No.2 of 2012, section 4(1)(viii).*<br><br>The provision of Azure is subject to the following contractual documents:<br><br>• Microsoft Online Business and Services Agreement (a copy of which is available on request); and<br><br>• Service Level Agreement, a copy of which is available at: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37<br><br>Taking each of the points in turn:<br><br>**Service standards**<br><br>We have a detailed SLA (as defined above) with Microsoft. Microsoft provides a contractual financially-backed uptime guarantee for the Azure 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 |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | • Business continuity management. | 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.<br><br>**Rights, responsibilities and expectations of all parties**<br><br>Our contract with Microsoft clearly sets out the rights and responsibilities of each of the parties.<br><br>**Dispute resolution mechanism**<br><br>Our contract is subject to Washington state law and jurisdiction. We have sought advice on this and are comfortable with this position. The contract also includes dispute escalation procedures.<br><br>**Confidentiality and security of information**<br><br>Microsoft offers very robust confidentiality commitments and security protections. Details are included in section D below.<br><br>**Termination of contract**<br><br>The Microsoft Business and Services Agreement (**"MBSA"**) contains usual termination provisions. The SLA is contained within the MBSA and 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.<br><br>On termination, Microsoft uses best practice procedures and a wiping solution that is NIST 800-88 |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | compliant. For hard drives that can't be wiped it uses a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. All Microsoft Online Services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle. "Secure disposal or re-use of equipment and disposal of media" is covered under the ISO/IEC 27001 standards against which Microsoft is certified.<br><br>**Sub-contracting if involved**<br><br>Microsoft does use sub-contractors to provide certain ancillary assistance, but not for any critical path roles. An up-to-date list of all subcontractors used to provide the ancillary services (including exact services) is available at http://azure.microsoft.com/en-us/support/trust-center/. Microsoft ensures that all sub-contractors that it deals with are subject to stringent requirements and is experienced at managing such relationships.<br><br>**Business continuity management**<br><br>Microsoft offers contractually-guaranteed 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.<br><br>Microsoft's arrangements are as follows:<br><br>***Redundancy:*** |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | • Physical redundancy at server, data center, and service levels;<br>• Data redundancy with robust failover capabilities; and<br>• Functional redundancy with offline functionality.<br><br>***Resiliency:***<br><br>• Active load balancing;<br>• Automated failover with human backup; and<br>• Recovery testing across failure domains.<br><br>***Distributed Services:***<br><br>• Distributed component services limit scope and impact of any failures in a component;<br>• Directory data replicated across component services insulates one service from another in any failure events; and<br>• Simplified operations and deployment.<br><br>***Monitoring:***<br><br>• Internal monitoring built to drive automatic recovery;<br>• Outside-in monitoring raises alerts about incidents; and |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | • Extensive diagnostics provide logging, auditing, and granular tracing.<br><br>***Simplification:***<br><br>• Standardized hardware reduces issue isolation complexities;<br><br>• Fully automated deployment models; and<br><br>• Standard built-in management mechanism.<br><br>***Human backup:***<br><br>• Automated recovery actions with 24/7 on-call support;<br><br>• Team with diverse skills on the call provides rapid response and resolution; and<br><br>• Continuous improvement by learning from the on-call teams.<br><br>***Continuous learning:***<br><br>• If an incident occurs, Microsoft does a thorough post-incident review every time; and<br><br>• Microsoft's post-incident review consists of analysis of what happened, Microsoft's response, and Microsoft's plan to prevent it in the future.<br><br>For the avoidance of doubt, the nature of the services provided as part of Azure 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). |

| Ref. | Question/requirement | | Template response and guidance |
|---|---|---|---|
| 19. | (ix) | A specific contingency plan to bring the outsourced activity back in-house in an emergency situation which could arise due to service provider's inability to provide and the costs, time and resources that would involve. | *Banking Act Directions No.2 of 2012, section 4(1)(ix).*<br><br>Yes.<br><br>Our contract with Microsoft provides various opportunities to terminate the service even at short notice as well as contractual obligations on the part of Microsoft to enable the transfer of services to another service provider or back in-house. These are not services which would commonly be provided by any Bank in-house in any event however. |
| 20. | (x) | A framework for cross-border outsourcing, taking into account the differences in country environments. | *Banking Act Directions No.2 of 2012, section 4(1)(x).*<br><br>Yes.<br><br>We carefully considered the location issues relevant to the service. We are comfortable with the solution for various reasons. First, Microsoft informs us that it takes a regional approach to hosting of Azure data. For customers like us with a presence in the Asia-Pacific region, the applicable Azure services will be hosted out of Microsoft's highly-secure data centers that have been selected by Microsoft taking into careful account the country and socio-economic factors. Second, we took into account that the Microsoft data centers have been built in seismically safe zones. Environmental controls have been implemented to protect the data centers including temperature control, heating, ventilation and air-conditioning, fire detection and suppression systems and power management systems, 24-hour monitored physical hardware and seismically-braced racks. These requirements are covered by Microsoft's ISO/IEC 27001 accreditation for Azure. Azure offers data-location transparency so that the organizations and regulators are informed of the jurisdiction(s) in which data is hosted. We are confident that Microsoft's data center locations offer extremely stable political and socio-economic environments with robust and transparent legal frameworks. |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| 21. | (xi) Limits on maximum exposure to a single service provider both in terms of value and the number of contracts. | *Banking Act Directions No.2 of 2012, section 4(1)(xi).*<br><br>Yes.<br><br>We consider concentration and exposure risks as part of our policy. We are not placing undue reliance on one service provider for multiple activities in making this outsourcing. The arrangement is for the provision of certain IT services only and not of the nature that would usually be split between different service providers. We also believe we have sufficient limits in terms of financial exposure. |
| 22. | Are you confident that you are entering into an outsourcing arrangement with a service provider of who has the specialized resources and skills to perform the related services? | *Banking Act Directions No.2 of 2012, section 2(4).*<br><br>Yes.<br><br>We are very confident in our selection of Microsoft as service provider. In particular we took note of the following in making our decision:<br><br>**a. Competence and experience.** Microsoft is an industry leader in cloud computing. Azure 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.<br><br>**b. Past track-record.** 40% of the world's top brands use Azure. We consulted various case studies relating to Azure, 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 financial institutions.<br><br>**c. Specific financial services credentials.** Financial Institution customers in leading markets, including in the UK, France, Germany, Australia, Singapore, Canada, the United States and many |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | other countries have performed their due diligence and, working with their regulators, are satisfied that Azure meets their respective regulatory requirements. This gives us confidence that Microsoft is able to help meet the high burden of financial services regulation and is experienced in meeting these requirements.<br><br>**d. Financial strength of Microsoft.** 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. |
| 23. | Can you confirm that you are not entering into an outsourcing arrangement with a service provider of which the majority of the ownership is held by employees and/or close relatives of an employee of the Bank? | *Banking Act Directions No.2 of 2012, section 2(5).*<br><br>Yes.<br><br>We can confirm that we are not entering into an outsourcing arrangement with a service provider of which the majority of the ownership is held by employees and/or close relatives of an employee of the Bank. |
| **D. MONITORING, CONTROL AND SECURITY** | | |
| 24. | Do you have a specifically designated unit/division at the Head Office to handle all outsourcing arrangements? A Licensed Bank incorporated outside Sri Lanka shall have the designated unit/division at the local Head Office. | *Banking Act Directions No.2 of 2012, section 6(1).*<br><br>Yes.<br><br>Our specifically designated unit/division is *[insert details]* and is based in our Head Office. |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| 25. | Please explain your system to ensure the effective management to enable the monitoring of the outsourced service activity. | *Banking Act Directions No.2 of 2012, section 6(3).*<br><br>See response at section 15 above which outlines the various and robust monitoring tools and processes we have available to us. |
| 26. | Do you have in place security procedures and controls to ensure that the service provider exercises a high standard of care and diligence to protect the confidentiality and security of banks' sensitive information especially relating to customers, hardware, operating systems and application software? Please explain the controls. | *Banking Act Directions No.2 of 2012, section 3(5).*<br><br>Yes.<br><br>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, Azure is designed for security with controls for encryption of data at rest and secure 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 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 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.<br><br>The following security features are also relevant to protecting the transmission and storage of information/data within the Microsoft infrastructure: |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | 1. The Microsoft Azure 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.<br><br>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 Azure. 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.<br><br>3. Networks within the Azure 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. Azure uses industry-standard transport protocols such as SSL and TLS between user devices and Microsoft data centers, and within data centers themselves. With virtual networks, industry standard IPsec protocol can be used to encrypt traffic between the corporate VPN gateway and Azure. Encryption can be enabled for traffic between VMs and end users. Microsoft also implements traffic throttling to prevent denial-of-service attacks.<br><br>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 |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | privilege access, and checking employee backgrounds is a highly scrutinized, manual-approval process.<br><br>5. Azure offers a wide range of data encryption capabilities up to AES-256. Options include .NET cryptographic services, Windows Server public key infrastructure (PKK) components, Active Directory Rights Management Services (AD RMS), and Bitlocker for data import/export scenarios. |
| **E. BUSINESS CONTINUITY MANAGEMENT** | | |
| 27. | Do you have in place a Business Continuity Plan which contains all relevant operations including outsourcing arrangements? | *Banking Act Directions No.2 of 2012, section 5(1). You will need to confirm that you have a Business Continuity Plan and provide details and/or a copy.* |
| 28. | Have you confirmed that your service provider has a satisfactory Business Continuity Plan and performs regular tests on it? | *Banking Act Directions No.2 of 2012, section 5(2).*<br><br>Yes.<br><br>Our response at section 18(viii) above contains details of Microsoft's business continuity arrangements. |
| **F. OTHER CONSIDERATIONS**<br><br>***This section contains additional information that is relevant to outsourcing cloud services to a service provider but is not specifically set out in the Banking Act Directions No.2 of 2012.*** | | |
| 29. | Does the service provider provide CBSL with | Yes. |

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | audit rights? | CBSL 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. |
| 30. | Is the service provider subject to any third party audits and do they agree to make the results of any such audit available to you? | Yes.<br><br>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 to customer right to monitor and supervise.<br><br>*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.* |
| 31. | Does the service provider confirm that it will only use Bank and customer data for the purposes of providing the services and not for any other purpose? | Yes.<br><br>Microsoft commits to never allow Bank or customer data to be used for any purposes other than providing the contracted services to the Bank. In the OST, page 8, Microsoft commits that Customer Data will only be used to provide the online services to the customer and Customer Data will not be used for any other purposes, including for advertising or other commercial purposes. |
| 32. | Is customer data and bank confidential information kept separate from that of other customers of the service provider? | Yes.<br><br>Microsoft's 'Active Directory' function 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- |

<table>
<tr><th>Ref.</th><th>Question/requirement</th><th>Template response and guidance</th></tr>
<tr><td></td><td></td><td>tenants, where applicable.</td></tr>
<tr><td>33.</td><td>Do you have transparency as to where your data is being held?</td><td>Yes.<br><br>Microsoft informs us that it takes a regional approach to hosting of Azure data. Microsoft is transparent in relation to the location of our data. Microsoft data center locations are made public on the Microsoft Trust Center.<br><br>Microsoft enables customers to select the region that it is provisioned from. Under the OST, Microsoft commits that if a customer provisions its tenant in the United States or EU, Microsoft will store the customer's data at rest in the United States or EU, as applicable.<br><br>The table below will need to be amended depending on the specific solution that you are taking up.
<table>
<tr><th>#</th><th>Locations of Data Centre</th><th>Classification of DC: Tier I, II, III or IV</th><th>Storing your organization's data (Y/N)</th></tr>
<tr><td>1.</td><td></td><td></td><td></td></tr>
<tr><td>2.</td><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>34.</td><td>Did you carefully consider different the different types of cloud solution available?</td><td>Yes.<br><br>Microsoft's "Azure" service, which is described in more detail here: Azure. Azure is a multi-tenant service. Data storage and processing for each tenant is segregated through Active Directory structure and capabilities specifically developed to help build, manage, and secure multi-tenant environments. Active Directory isolates customers using security boundaries (also known as silos). This safeguards a</td></tr>
</table>

| Ref. | Question/requirement | Template response and guidance |
|---|---|---|
| | | customer's data so that the data cannot be accessed or compromised by co-tenants. |

## 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 Bank should have in place a legally binding contract/agreement for the outsourcing arrangement which should include at least the following: | *Banking Act Directions No.2 of 2012, section 4(1)(viii)*<br><br>Yes.<br><br>The Microsoft contract is a legally binding agreement. |
| 2. | Service standards. | *Banking Act Directions No.2 of 2012, section 4(1)(viii)(a)*<br><br>Yes.<br><br>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 or renewal term of the Enrollment are fixed for the duration of that term.<br><br>A copy of the SLA is available here: http://azure.microsoft.com/en-us/support/legal/sla/ |
| 3. | Rights, responsibilities and expectations of all parties. | *Banking Act Directions No.2 of 2012, section 4(1)(viii)(b)*<br><br>Yes.<br><br>The contract pack comprehensively sets out the scope of the arrangement and the respective commitments of the parties. The online services are ordered under the Enrollment, and the order will set out the online services and relevant prices.<br><br>The services are described, along with the applicable usage rights, in the Product List and OST (pages 14 and 15). The services are described in detail in the Services Description, which is not part of the contract. However, Microsoft makes a functionality commitment in the Core Features |

| Ref. | Requirement | Microsoft agreement reference |
|---|---|---|
| | | Amendment and as a minimum the online services will meet that commitment.<br><br>MBSA section 6 deals with liability and rights of action. MBSA section 5 sets out Microsoft's obligation to defend the regulated entity against third party infringement and breach of confidence claims. Microsoft's liability under section 5 is unlimited. |
| 4. | Dispute resolution mechanism. | *Banking Act Directions No.2 of 2012, section 4(1)(viii)(c)*<br><br>Yes.<br><br>MBSA section 11 contains provisions that describe how a dispute under the contract is to be conducted.<br><br>MBSA section 11e sets out the jurisdictions in which parties should bring their actions. Microsoft must bring actions against the customer in the countries where the customer's contracting party is headquartered. The customer must bring actions against: (a) in Ireland if the action is against a Microsoft affiliates in Europe; (b) in the State of Washington, if the action is against a Microsoft affiliate outside of Europe; or (c) in the country where the Microsoft affiliate delivering the services has its headquarters if the action is to enforce a Statement of Services.<br><br>MBSA section 11h sets out the choice of law provision. Either, the contract is governed by the laws of the State of Washington if the contract is with a Microsoft affiliate located outside of Europe; or the contract is governed by the laws of Ireland if the contract is with a European Microsoft affiliate.<br><br>MBSA section 6 deals with liability and rights of action. MBSA section 5 sets out Microsoft's obligation to defend the regulated entity against third party infringement and breach of confidence claims. Subject to the terms of the MBSA, Microsoft's liability under section 5 is unlimited. |

| Ref. | Requirement | Microsoft agreement reference |
|---|---|---|
| 5. | Confidentiality and security of information. | *Banking Act Directions No.2 of 2012, section 4(1)(viii)(d)*<br><br>Yes.<br><br>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.<br><br>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 clause 6c(iv) 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<br><br>Microsoft also makes specific commitments with respect to Customer Data in the OST. In summary Microsoft commits that:<br><br>1. Ownership of Customer Data remains at all times with the customer (see OST, page 8).<br><br>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).<br><br>3. Microsoft will not disclose Customer Data to law enforcement unless it is legally obliged to do so, |

| Ref. | Requirement | Microsoft agreement reference |
|---|---|---|
| | | and only after not being able to redirect the request to the customer (see OST, page 8).<br><br>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).<br><br>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).<br><br>Microsoft commits to reimburse customer's reasonable remediation costs incurred as a consequence of a security incident involving Customer Data (see FSA under "Security Incident Notification"). |
| 6. | Termination of contract. | *Banking Act Directions No.2 of 2012, section 4(1)(viii)(e)*<br><br>Yes.<br><br>Termination rights for the Enrollment are set out in the Enrollment itself, and in section 6 of the EA. If the Enrollment is terminated, this will terminate all products and services ordered under the Enrollment (except to the extent that the customer has perpetual rights).<br><br>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.<br><br>In the event of default, the provisions of the SLA will apply to service level failures and page 9 of the OST sets out arrangements in the event of security incidents. Other defaults are addressed in the |

| Ref. | Requirement | Microsoft agreement reference |
|---|---|---|
| | | MBSA and EA. A termination right for cause is set out at section 6c of the EA.<br><br>The contract allows the customer to terminate the arrangement with Microsoft for convenience (MBSA section 8) which means the customer has the right to terminate in the event of default including change of ownership, insolvency or where there is a breach of security or confidentiality or demonstrable deterioration in the ability of the Service Provider to perform the service as contracted.<br><br>Note also that customers have control over the use they make of, and data they load into, the online service. |
| 7. | Subcontracting if involved. | *Banking Act Directions No.2 of 2012, section 4(1)(viii)(f)*<br><br>Yes.<br><br>See page 9 of the OST, under which Microsoft is permitted to hire subcontractors.<br><br>The confidentiality of our data is protected when Microsoft uses subcontractors because Microsoft commits that its subcontractors "will be permitted to obtain Customer Data only to deliver the services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose" (OST, page 9).<br><br>Microsoft commits that any subcontractors to whom Microsoft transfers our data will have entered into written agreements with Microsoft that are no less protective than the data processing terms in the OST (OST, page 11).<br><br>Under the terms of the OST, Microsoft remains contractually responsible (and therefore liable) for its subcontractors' compliance with Microsoft's obligations in the OST (OST, page 9). In addition, Microsoft's commitment to ISO/IEC 27018, requires Microsoft to ensure that its subcontractors are |

| Ref. | Requirement | Microsoft agreement reference |
|---|---|---|
| | | subject to the same security controls as Microsoft is subject to. Finally, the EU Model Clauses, which are included in the OST, require Microsoft to ensure that its subcontractors outside of Europe comply with the same requirements as Microsoft and set out in detail how Microsoft must achieve this.<br><br>Microsoft maintains a list of authorized subcontractors for the online services that have access to our data and provides us with a mechanism to obtain notice of any updates to that list (OST, page 10). The actual list is published on the applicable Trust Center. If we do not approve of a subcontractor that is added to the list, then we are entitled to terminate the affected online services. |
| 8. | Business continuity management. | *Banking Act Directions No.2 of 2012, section 4(1)(viii)(g)*<br><br>Yes.<br><br>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. |