asifma
Growing Asia's Markets

18 November 2022

To,
T.K. Rajan
Chief General Manager
Department of Supervision
Reserve Bank of India (RBI)

Dear Sirs,

RE: Representation in relation to RBI's Draft Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, dated October 20, 2022.

On behalf of ASIFMA[1] members, we have been working with Shehryar Khanum (Consultant, Cyril Amarchand Mangaldas) on this Reserve Bank of India ("RBI") Consultation to share with you the industry's suggestions in relation to the RBI's Draft Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices ("Draft IT Governance MD"), dated October 20, 2022.

1. We would like to thank the RBI for the opportunity to comment on the Draft IT Governance MD. We recognise RBI's intent to develop a risk management framework to address risks associated with the adoption of newer technologies. We hope that RBI will work closely with the industry to develop an implementable framework that is aligned with international best practices.

2. However, we believe that there are serious concerns in complying with various provisions of the Draft IT Governance MD in its present form. We have highlighted our concerns with regards to these provisions and have provided our suggestions in a chapter-wise manner which is set out in the table below:

[1] *ASIFMA is an independent, regional trade association with over 165 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region. More information about ASIFMA can be found at: www.asifma.org.*

Chapter II: IT Governance

S. No.	Provision	Brief Description	Comments
1.	Para. # 5	Para. # 5 requires the Regulated Entities ("REs") to place a robust Information Technology ("IT") Governance Framework comprising of governance structure and processes necessary to meet the RE's business/strategic objectives.	We recommend that the term "business risks" be replaced with "IT risks", given that IT governance frameworks are focused on mitigating IT risks. Further, we recommend replacing the term "Business Continuity/Disaster Recovery Management" with IT resilience.
2.	Para. # 6	Para. # 6 requires the REs to review their policies related to IT, Information Systems ("IS"), Business Continuity, Information Security, Cyber Security (including Incident Response and Recovery Management/ Cyber Crisis Management) to be approved by the Board and reviewed at least annually.	We recommend that RBI allows the REs to take a risk-based approach to determine the frequency for approvals by the Board instead of a mandatory approval on a yearly basis. While reviews of the policies can be conducted annually, approvals may not be necessary unless there are material changes. We also recommend that the RBI allows the Board/Local Management Committee of an RE, which is a branch or subsidiary of a foreign firm, be able to leverage the global frameworks while remaining accountable for the local oversight and, as a result, without being required to approve each of the global policies and standards. Moreover, we recommend that the term "business continuity" in Para. # 6 be specified to relate only to IT resilience and not generic business of REs.
3.	Para. # 7	Para. # 7 requires the REs to establish a Board level IT Strategy Committee ("ITSC"), Para. # 10 requires the REs to	We recommend that RBI provides REs with the flexibility to a) leverage global/regional committees if local IT footprint is limited or b) (where run locally), determine the composition of the ITSC and IT Steering Committees based upon their operations. This is because some global

		establish an IT Steering Committee.	financial firms leverage global or regional committees if their scope covers India branch as well, while others may have one local IT committee that could serve as ITSC and the IT Steering Committee both, since both these committees are working towards common objectives and do not have conflicting roles.
4.	Para. # 8	Para. # 8 provides the roles and responsibilities of the ITSC.	There is a further need for clarification in Para. # 8(f) to the extent that the meaning of 'Business Continuity Planning and Disaster Recovery Management' should be specified to focus narrowly on IT issues, because Business Continuity Planning ("BCP") in itself is a term of much wider ambit and may also include non-IT issues. Thus, it is recommended to specify the meaning of BCP in relation to the IT issues only. Also, for #8(e), for foreign banks, the global IT & Cyber budget would be a composite number covering all geographies including India and hence may not have an attributable figure for India branch alone.
5.	Para. # 10	Para. # 10 requires the REs to establish an IT Steering Committee and prescribes its roles and responsibilities.	We recommend that Para. # 10(c) be specified to mean that the ambit of terms 'BCP and Disaster Recovery Management' here pertains only to IT issues and not a generic reference.
6.	Para. # 12	Para. # 12 requires the REs to implement & manage IT architecture	Foreign banks use standardised global platform across the firm and firm-wide IT Strategy (after consulting for India branch needs) and projects execution covering all branches. This is especially true for banks with limited local IT footprint. So, clarification would be needed on whether this model would help meet the Para #12 requirement.
7.	Para. # 13	Para. # 13 requires the REs to organise training on	We recommend that RBI should allow individual REs to determine the frequency of IS training based on their own risk assessment.

		aspects pertaining to IT and Information Security ("IS").	

Chapter III: IT Infrastructure & Services Management

S. No.	Provision	Brief Description	Comments
1.	Para. # 18	Para. # 18 requires the REs to follow the instructions given therein for third-party arrangement in the Information Technology/ Cyber Security ecosystem that are either not considered as "outsourcing" of IT Services arrangement (or) not considered as "material" outsourcing of IT Services.	There is a further need for clarification on the definitive example of what the outsourcing arrangements are that would fall under 'non-IT Services Outsourcing' and 'non-material IT services outsourcing' mentioned in Para. # 18. Moreover, there is a need for clarification on the meaning of 'conflict of interest' in Para. # 18(a).
2.	Para. # 25	Para. # 25 requires the REs to obtain a certificate from the application developer stating that the application is	We recommend that the REs are provided with the option to seek assurance from the application developer that the application is free from known vulnerabilities, malwares and any covert channels in the code, through contractual clauses rather than certificates, as mentioned by Para. # 25.

		free of known vulnerabilities, malwares and any covert channels in the code.	

Chapter – IV: IT Risk and Information Security

S. No.	Provision	Brief Description	Comments
1.	Para. # 35	Para. # 35 requires the REs to establish a robust IT Risk Management Framework covering various salient aspects including roles and responsibilities of stakeholders involved in risk management and identification of Crown Jewels of the organisation.	Given that global firms may have a firmwide methodology to determine the firm's Crown Jewels, we are confirming that this arrangement meets the requirement as per Para. # 35 (e). There is a further need for clarification on the specific list of "extant instructions" that pertains to critical information infrastructure (CII) as per Para. # 35 (f).
2.	Para. # 38	Para. # 38 requires the REs to establish an Information Security Policy and Cyber Security Policy.	We recommend aligning the aspects of the Cyber Crisis Management Plan to National Institute of Security and Technology's Cybersecurity Framework ("NIST CSF") core functions which are "identify, protect, detect, respond, and recover." The same core functions are used by the Cyber Risk Institute's Profile or previously known as the Financial Services Cybersecurity Profile ("FSP"), a cyber risk management assessment tool that financial industry created which allows an organisation to diagnose cyber risk and apply relevant standards and best practices to appropriately manage that risk. The profile is

			based off NIST CSF, and synthesises the best cyber practices from industry, as well as regulators in different jurisdictions. International financial regulators have continued to express their support for the Profile. Most recently in October 2022, the Federal Financial Institutions Examination Council ("FFIEC") issued an update to its 2018 Cybersecurity Resource Guide for Financial Institutions and the FSP was listed as one of the resources for assessments. The purpose of this guide is to help FIs meet their security control objectives and prepare to respond to cyber incidents. In April 2021, the Reserve Bank of New Zealand ("RBNZ") published its "Guidance on Cyber Resilience" and officially recognises FSP as one of the recommended frameworks for FIs to make reference.
3.	Para. # 39	Para. # 39 outlines the responsibilities of the Information Security Committee.	We recommend that there may not be a separate requirement of an Information Security Committee in addition to the IT Strategy Committee and IT Steering Committee because for REs such as global banks, these roles may be performed by a global/regional committee (given global IT platform usage) or a single local committee, with support from the global teams. Also, for Para. 39 (b), for foreign banks, information security plans and budgets drawn globally apply for the India branch as well since the branch is consulted. Clarification needed on whether this arrangement would meet the para requirements.
4.	Para. # 40	Para. # 40 requires the REs to appoint a Chief Information Security Officer ("CISO") and outlines the roles and responsibilities of the designation.	Para. # 40 (b) requires the CISO to be appointed for a reasonable minimum term. However, in practice, the employment terms of the CISOs are like any other employee and the usual employment terms apply to them. There may be no stipulation around the length of time that they are required to stay in that role except for a notice period should they resign from the role. We propose the removal of the minimum term requirement. Para. # 40 (d) requires the budget for the information/cyber security and the CISO's Office to be determined

			keeping in view the current/emerging threat landscape. However, as per the prevailing practice, for global firms, the budget allocation is determined by the global headquarters in consultation with the country team. Hence, there is a further need for clarification and modification in Para. # 40 (d) in light of this prevailing practice amongst stakeholders.
5.	Para. #41	Para #41 details the roles and responsibilities of the CISO	For global firms, the SOC is managed & monitored by a central team firm-wide with access to the best of tools and technology. Similarly, the cyber security projects, KRI and KPI generation are driven centrally with cascading benefit to all branches. All these take into account the country needs. So, we need clarification and modification in Para. # 41 (e) & 41 (g).
6.	Para. # 49	Para. # 49 requires the REs to adopt a “Straight Through Processing” (“STP”) and minimise manual intervention while transferring data from one application to another particularly in respect of critical or financial applications.	Since different applications may have different organisational setup and there may be technical challenges in implementing STP for every application, we are suggesting compensating control that would address similar risks. There may also be a situation where the technology does not support “straight through processing” especially with legacy systems. Accordingly, we suggest the following modified wording to Para. # 49: “*Data transfer from one process to another or from one application to another, particularly in respect of critical or financial applications, shall not have any manual intervention in order to prevent any unauthorised modification. Where feasible, the process can be automated and integrate “Straight Through Processing” methodology with an appropriate authentication mechanism and audit trails if the technology allows*.”
7.	Para. # 54	Para. # 54 provides a non-exhaustive list of the controls that the REs have to put in place in a	There is a further need for clarification on Para. # 54(d), since the specific requirement of securing the RE’s system appropriately is unclear in the present form.

		teleworking environment. Specifically point (d) mentions: “Teleworking, where remote access to the RE’s systems is not provided shall be secured appropriately depending upon the sensitivity of the data/ information shared/ handled.”	
8.	Para. # 55	Para. # 55 requires the REs to periodically conduct Vulnerability Assessment/ Penetration Testing (“VA / PT”) of the IT assets.	Since internet facing applications are a key risk factor used by REs to assess inherent risks in the IT assets, we recommend that RBI aligns the current text of Para. # 55 in line with RBI’s Notification on Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach. We recommend the following modified wording of Para. # 55: “*REs shall periodically conduct Vulnerability Assessment/ Penetration Testing (VA / PT) of* ***“internet facing”*** *IT assets (applications, systems and infrastructure) throughout their lifecycle (pre-implementation, post implementation, after major changes, etc.)*” Additionally, we recommend “Internal” IT Assets such as the applications, systems, and infrastructure etc. to be kept out of scope of Penetration Testing requirements. We are also confirming that REs’ internal information security experts are included in the category of ‘*appropriately trained and independent information security experts/ auditors*’ as per Para. # 55.

9.	Para. # 56	Para. # 56 specifies that in the post implementation (of IT project/ system upgrade, etc.) scenario, the VA/ PT shall be performed on the production environment. Under unavoidable circumstances, if the PT is conducted in test environment, REs shall ensure that the version and configuration of the test environment resembles the production environment. Any deviation should be documented and approved by the ISC.	We recommend that the text "*where appropriate*" should be added to Para. # 56 so as to provide REs with the flexibility to leverage VA/PT conducted in test and production environment based on a risk-based approach. Based upon this, we recommend the following modified wording of the Para. # 56: *"In the post implementation (of IT project/ system upgrade, etc.) scenario, the VA/PT shall* ***where appropriate*** *be performed on the production environment. Under unavoidable circumstances, if the PT is conducted in test environment, REs shall ensure that the version and configuration of the test environment resembles the production environment. Any deviation should be documented and approved by the ISC."*
10.	Para. # 59	Para. # 59 requires REs to ensure that all vulnerability scanning is performed in authenticated mode.	Given that there are other compensatory controls implemented by the REs, we recommend that RBI provides REs the flexibility to take a 'risk-based approach' and determine when authenticated and unauthenticated scanning are deployed. There are risks involved in the use of authenticated scanning which makes it unsuitable to deployment across the board. For example, authenticated scanning generally requires that administrative passwords be created and stored centrally on the VA scanner. This poses a security risk as it is a single point of compromise which would provide a

			malicious attacker password for a large population of systems. Thus, we recommend the wording of Para. # 59 be accordingly modified to incorporate the 'risk-based approach'.
11.	Para. # 60	Para. # 60 requires the REs to have a mechanism in place to carry out the PTs in a controlled manner within the scoped IT system components/ applications for any known as well as unknown vulnerability which may exist before the PT exploits.	We suggest replacing the term "*IT systems components*" to align with Para. # 55 and recommend the following modified wording of Para. # 60: "*REs shall have a mechanism in place to carry out the PTs in a controlled manner within the scoped ~~IT system components~~* ***IT assets applications, systems and infrastructure*** *for any known as well as unknown vulnerability which may exist before the PT exploits.*"
12.	Para. # 67	Para. # 67 requires the REs to have clear communication plans for escalation and reporting the incidents to the Board, Senior Management, the customers and to pro-actively notify CERT-In, RBI and Indian Banks – Centre for Analysis of Risks and Threats (IB-CART) set up by IDRBT regarding	We would recommend that the reporting requirement as per Para. # 67 to be limited to cybersecurity incidents which industry defines as incidents where there is evidence of actual harm, resulting from a malicious activity. The scope of reporting requirement should not be determined according to Para. # 63 because its scope is wide and may include broader technology incident rather than just cybersecurity incidents. As we understand, the purpose of the reporting requirement as per Para. # 67 is to enable regulators to alert the wider community about an ongoing threat. Hence, it should be limited to cybersecurity incidents that may have a potential impact on the wider community. In contrast with cybersecurity incidents, in technology incident there is no malicious intent and such incidents are limited to a single

		cyber security incidents, as per regulatory requirements.	institution and there is no impact on the wider community. Hence, there is no real purpose of reporting such non-malicious technology incidents to regulators. This approach would help prevent overreporting and streamline the notification approach. There is a further need to modify the reporting requirement prescribed by RBI's Cyber Security Framework in Banks of security incident reporting within two to six hours since it is difficult to implement for the stakeholders. We recommend that the time period for reporting be aligned with 72-hour time period as per international practice.
13.	Para. # 68	Para. # 68 provides that REs should establish processes to improve incident response and recovery activities and capabilities through lessons learnt from past incidents as well as from the conduct of tests and drills along with stakeholders (including service providers).	Since not all scenarios require the involvement of external service providers, specifically from a Cyber Readiness Exercise perspective, it would be reasonable to allow REs the flexibility to decide on the involvement of third-party service providers taking a risk-based approach. Accordingly, we suggest the following wording to be added to the end of the sentence in Para. # 68: *"if deemed necessary"* or "*…if the scenario calls for*".

Chapter V - Business Continuity and Disaster Recovery Management

S. No.	Provision	Brief Description	Comments
1.	Para. # 70 - Para. # 78	Overall	While BCP may have some overlap with IT resilience, BCP covers a broad range of scenarios such as natural disasters or pandemics. Therefore, we recommend RBI to address BCP as an independent domain. IT governance, risk, and control frameworks are typically focused on IT resilience and these are already covered under specific portions of the document such as Para. # 51 and Para. # 69. Since the scope of BCP is broader than IT, we recommend that BCP should ideally be covered in a separate regulation. Hence, we propose the removal of this section dealing with BCP. If RBI intends to retain this section, we recommend that the scope of BCP should be limited to IT issues only.
2.	Para. # 73	Para. # 73 requires the DR drills for critical systems to be conducted at least on a half-yearly basis and for all other systems at least on a yearly basis.	Since REs vary in size and have a varying impact on the India financial system, we recommend that RBI does not prescribe the frequency of DR drills and instead allows the REs to take a 'risk-based approach' towards testing of the RE's critical systems. Also, given India branches of foreign banks use global systems primarily, the frequency of the DR drill for such systems (including critical) is determined based on firm-wide business criticality and risk inputs. Hence, having a country specific frequency would be feasible only for local systems. So, there is a further need for clarification and modification in Para. # 73 in light of this constraint.
3.	Para. # 74	Para. # 74 requires the REs to backup data and periodically restore such backed-up	We are confirming that DR testing as per Para. # 73 would also fulfil the requirement of Para. # 74 to backup data.

		data to check its usability.	
4.	Para #77	Para 77 requires the Res to ensure similar configurations for both the DR and DR	Even while identical infra and configurations are a must for the critical systems, we recommend that the Para #77 provides flexibility for the REs to adopt a “Risk based” approach in the DR implementation, as the Resiliency needs also determine the DR configurations for the systems.

Miscellaneous

S. No.	Provisions	Brief Description	Comments
1.	Overall		We note that this Draft IT Governance MD repeals some existing circulars but it will also complement the IT Outsourcing Circular that is still in draft stage. As these guidelines are still being finalised and they stipulate new requirements for the REs to comply with, we recommend RBI to provide REs with a longer time period to enable them to make the necessary adjustments. There is also a further need of clarification on whether in the areas where there are overlaps between the present framework and the cybersecurity framework, which framework the REs would be expected to follow.
2.	Overall		We appreciate RBI’s recognition of a ‘risk-based approach’ for IT governance, and we hope this approach can be extended to take into account the operating models of global financial firms where the REs may have firmwide methodology around identification of Crown Jewels, conducting of vulnerability assessments and penetration testing, formation of strategic/steering/security committees etc.

In view of the above conceptual and practical concerns, we submit that the Draft IT Governance MD cannot be implemented in its current form. We would like to better understand RBI’s regulatory objective and engage in a constructive dialogue with the RBI to find a solution that both addresses the regulatory concerns and is workable for the industry.

We humbly request the RBI to kindly review the concerns and suggestions aforementioned. We stand ready to discuss this request in further detail and look forward to your response. Please do not hesitate to reach out to myself or Laurence Van der Loo, at lvanderloo@asifma.org for any questions. In the meantime, we remain at your disposal if you wish to discuss any further details.

Sincerely,

Laurence Van der Loo
Executive Director
Technology & Operations
ASIFMA