New MAS Outsourcing Guidelines important changes for financial institutions and insurers in Singapore

5 August 2016

The Monetary Authority of Singapore (the "**MAS**") last week issued new *Guidelines on Outsourcing Risk Management* (the "**Guidelines**"), the result of an industry wide consultation process which began in October 2014. The Guidelines are intended to consolidate the MAS's approach to regulation of outsourcing activities. They replace both the 2005 Outsourcing Guidelines (last updated on 1 July 2005) and the *Circular on Information Technology Outsourcing* (issued on 14 July 2011).

Our take on the Guidelines

The Guidelines will provide some comfort to regulated institutions and vendors alike. Highlights include eliminating the expectation to pre-notify the MAS of material outsourcings and the withdrawal of the MAS Technology Questionnaire for Outsourcing, which was previously required to be submitted to the MAS before institutions made any significant IT outsourcing commitments. These changes reflect an awareness that outsourcing is ubiquitous to the industry and that the increasingly complex nature of institutions' outsourcing arrangements called for a change in regulatory approach. By introducing these changes, the MAS has expressly called for institutions to refine their risk-based approach to assessing material outsourcings and to be ready to demonstrate that appropriate due diligence and risk management principles have been applied whenever they are called upon to do so by the MAS.

The other significant step forward in the Guidelines is the recognition that cloud services are just another variant of outsourcing that can be addressed from a risk management perspective in the same way as any other technology outsourcings, noting that some cloud services structures may raise unique issues that will have to be addressed. This is a welcome development that removes a degree of stigma that has come to be attached to cloud-based solutions, irrespective of advances that have been made over the years in areas such as data security.

As noted in more detail below, there remain some areas of concern for institutions in relation to the Guidelines – particularly with respect to the scope of the definitions of "outsourcing arrangements" and "material outsourcing arrangements". These definitions cast a very wide net for the effective scope of the Guidelines, bringing in various types of procurement activity that we believe many institutions will not understand to be outsourcings.

All in all, we believe that the Guidelines represent an important step forward for the regulation of outsourcings by Singaporean institutions. While the Guidelines apply to all outsourcings, some of the key changes reflect a preoccupation with technology developments, in keeping with Singapore's ambitions to be ASEAN's leading financial hub and FinTech centre. The Guidelines recognise the benefits of IT innovation and the pervasive nature of outsourcing, but at the same time showcase the MAS's increasing focus on cyber security and technology risk management.

Scope and legal effect of the Guidelines

The Guidelines apply to all MAS regulated financial institutions, including banks, insurance companies and intermediaries, financial advisers, money changers and stored value facility holders ("**institutions**"). Institutions are expected to carry out a self-assessment of all existing outsourcing arrangements against the Guidelines by 27 October 2016 and rectify any deficiencies by 27 July 2017.

Whether or not the Guidelines will remain a "best practice" advisory note like the predecessor 2005 Guidelines or will be legally binding in nature remains an open question. When the MAS launched its consultation on material outsourcing requirements in October 2014, the published materials included a draft statutory notice as well as an earlier draft of the Guidelines. The effect of a statutory notice would be to make the Guidelines (as reproduced in the statutory notice) legally binding on institutions. At the time, this signalled an intention by the MAS to bring firmer expectations to the regulation of material outsourcings. The MAS has indicated in its published comments to the Guidelines that it will issue such a statutory notice in the future, pending review of industry feedback.

What has changed?

1. New test for "materiality" of outsourcing arrangement

"Material outsourcing" was defined under the 2005 Guidelines as "*an outsourcing arrangement which, if disrupted, has the potential to significantly impact an institution's business operations, reputation or profitability.*" This allowed considerable flexibility for an institution to devise its own 'checkpoints' for materiality within the context of its own compliance framework.

Under the Guidelines, "material outsourcing" is now defined as an outsourcing:

a) *which, in the event of a service failure or security breach, has the potential to either materially impact an institution's –*

(i) business operations, reputation or profitability; or

(ii) ability to manage risk and comply with applicable laws and regulations,

or

b) ***which involves customer information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may have a material impact on an institution's customers" (emphasis added)***

While the outsourcing of customer information would normally have been one of the checkpoints in determining the materiality of an outsourcing arrangement, the new definition means that any outsourcing which gives a vendor access to customer information will likely constitute a material outsourcing. The above paragraph (b) does not necessarily read as applying to the institution's customers as a whole, and so could be read to trigger materiality by virtue of a potential material impact on (for example) a small number of an institution's customers.

Outsourcing can of course create a "weak link" in an institution's security perimeter, presenting a heightened risk of customer information being lost, stolen or corrupted. The revised definition clearly recognises that risk and corresponds with moves by Singapore's lawmakers to focus more closely on data protection with the enactment of the Personal Data Protection Act 2012 (the "**PDPA**") and cyber security issues.

It should be noted that customer information in this context does not include securely encrypted information (see section 4 below).

2. No requirement to notify material outsourcing arrangements

The 2005 Guidelines set an expectation that institutions would notify the MAS of all material outsourcing arrangements. While the new Guidelines state that the MAS is "*particularly interested in materials outsourcing arrangements*", there will no longer be a strict pre-notification process.

The notification process is replaced by a requirement for institutions to submit a register of outsourcing arrangements, in a prescribed form, to the MAS at least annually or upon request. The MAS may then require an institution to take specific steps to remedy any deficiencies identified.

In addition, "adverse developments" in relation to outsourcing arrangements remain notifiable to the MAS, and the MAS will expect such developments to be notified even if they only affect an institution's group company. "Adverse developments" include any event that could lead to prolonged service failure or a breach of security or confidentiality of customer information.

3. New section on cloud services

The Guidelines include a clear statement by the MAS that cloud services are no different in principle from other outsourced services. While there are unique risks associated with cloud services, these should be evaluated and managed in the same way as other outsourcing risks. At the same time, the reference to "information systems hosting (e.g., *software-as-a-service,*

platform-as-a-service, infrastructure-as-a-service)" in the Guidelines' Annex 1 list of examples of "outsourcing arrangements" suggests that almost any kind of cloud arrangement will, prima facie, be considered an "outsourcing arrangement".

The Guidelines recognise that cloud technology has matured considerably in recent years and that measures such as robust authentication, access controls, tokenisation and data encryption can help mitigate cloud-related risks.

Apart from developing and applying appropriate risk management principles for cloud services arrangements that meet the expectations set out in the Guidelines, institutions continue to face the challenge of agreeing terms and conditions with cloud services providers that align with the standards set out in the Guidelines. Cloud services are often offered on "non-negotiable" standard terms and conditions, except occasionally in situations involving significant customer organisation purchasing power or in the case of niche service providers targeting regulated business. We are seeing progress on this front, and the MAS's move to "de-stigmatise" cloud services and recognise these services as just another variety of outsourcing is constructive.

4. New definition of customer information

"Customer information" was not defined in the 2005 Guidelines. The new Guidelines specifically define customer information handled by clearing houses, exchanges, and trade repositories. For all other institutions, customer information means:

"**… information that relates to its customers and these include customers' accounts, particulars, transaction details and dealings with the financial institutions, but does not include any information that is public, anonymised, or encrypted in a secure manner such that the identities of the customers cannot be readily inferred.**"

It is noteworthy that this definition excludes public information (in line with an important exemption for this kind of information under the PDPA) and information in encrypted form. The FAQs issued by the MAS along with the Guidelines state that institutions should adopt encryption algorithms of international standards and should subject encryption to appropriate scrutiny to ensure it is adequate. The carving out of encrypted customer information should benefit proposals to outsource various kinds of "big data" and customer analytics, which is in keeping with Singapore's objective to be an important regional FinTech hub.

What has not changed?

1. The key themes

Notwithstanding the substantive changes to the Guidelines, the key messages from the 2005 Guidelines remain the same, including:

- The management of outsourcing risks should form a key part of an institution's overall risk management strategy. Responsibility for an institution's outsourcing risk management strategy lies with the board, and a top-down approach is required in order to foster a culture of risk management when engaging vendors;
- An institution's risk management framework should equally address the risks of intra-group outsourcing arrangements as well as arm's length arrangements;
- The protection of customer information is a critical consideration in any outsourcing arrangement; and
- Risk evaluation should be an ongoing activity throughout an *outsourcing arrangement.*

2. Technology Risk Management Guidelines and Business Continuity Management Guidelines

While the Guidelines consolidate the MAS' approach to outsourcing activities, the Technology Risk Management (TRM) Guidelines (issued on June 2013) still apply to the management of technology risk in general, and these should still be considered by institutions in relation to any technology outsourcing.

In addition, the Business Continuity Management Guidelines (issued on June 2003) will continue to apply in the context of any outsourcing arrangement that may have an impact on business continuity, whether IT-related or not.

3. Audit rights

The 2005 Guidelines required all outsourcing agreements to permit audits of the relevant vendor by institutions and the MAS. In addition to this requirement, the draft 2014 Guidelines proposed that all outsourcing agreements must include provisions indemnifying the MAS and its officers, agents and employees in respect of any vendor audits undertaken by MAS pursuant to such right.

Various respondents during the consultation process objected to this proposed indemnity on the basis that service providers would likely object to it, and our experience in presenting such clauses to vendors is consistent with this objection. The draft indemnity requirement has not been included in the final Guidelines, but the existing requirement for audit rights in favour of institutions and the MAS has been retained.

What should institutions do now?

Institutions should:

- Examine their current outsourcing framework in line with the Guidelines and identify and address any gaps. The Guidelines emphasise the need for adequate institution-wide processes to ensure appropriate risk management in outsourcing;

- Review their standard contracts to align with the clauses required in the Guidelines and ensure that ongoing tenders and negotiations introduce these new requirements to the internal review process and the contractual documentation;
- Consider a training programme for procurement and vendor management teams to ensure that processes are properly communicated and that service interruptions or other problems are escalated when needed, since these may turn into notifiable events; and
- Evaluate existing supplier arrangements, as the Guidelines apply to both existing and new arrangements. Institutions have three months from the Guideline's effective date (i.e. until 27 October 2016) to undertake an evaluation of existing arrangements, and have 12 months (i.e. until 26 July 2017) to rectify any issues identified from such evaluation.

As noted above, the MAS is continuing to consider issuing a statutory notice in connection with the Guidelines (based on the draft statutory notice published for comment as part of the September 2014 consultation). If such a statutory notice is issued, then the Guidelines will have the force of law and offences found under the institution's statutory framework would apply, adding to the urgency for institutions to complete appropriate reviews in good time.

Contacts

Mark
Parsons

Partner

> Read the full article online