HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B10/1C
          B1/15C

12 April 2018

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Feedback from Recent Thematic Review of AIs' Sanctions Screening Systems

I am writing to share key observations and good practices that have been identified in the recent thematic review of the financial sanctions screening systems of Authorized Institutions (AIs). The adequacy of AIs' sanctions screening systems and controls is a supervisory priority for the Hong Kong Monetary Authority (HKMA), especially in the light of recent geopolitical developments, and this review is part of a series of initiatives to strengthen the collective ability of AIs to meet their sanctions obligations[1].

Our review revealed that while the sanctions screening systems as examined are in general performing within industry benchmarks, there are some issues and good practices in relation to the effectiveness and efficiency of the systems, which warrant further attention by AIs. Details of our overall findings, including examples of good practices and areas for improvement, are set out in the Annex. Where weaknesses were identified, the AIs concerned have been required to undertake remedial actions.

To understand and optimize the performance of screening systems and processes, AIs are expected to (i) give consideration to adopting the good practices, where appropriate, and a gap analysis should be performed at a minimum; and (ii) to put in place, if not already, regular sanctions screening

---

[1] Including the HKMA's circulars on 31 January 2018 (Anti-Money Laundering / Counter-Terrorist Financing: United Nations Sanctions) and 8 March 2018 (FATF Guidance on Counter Proliferation Financing).

55th Floor, Two International Finance Centre,   香港中環金融街8號國際金融中心2期55樓
8 Finance Street, Central, Hong Kong   網址：www.hkma.gov.hk
Website: www.hkma.gov.hk

system testing that provides robust reporting and quality assurance[2] to senior management that the regulatory expectations set out in the Annex are being met. The HKMA will collect information from all AIs in the third quarter of 2018 on individual action plans and consider conducting further reviews on relevant data and results on AIs in due course following a risk-based approach.

To further communicate our regulatory expectations, the HKMA will host a seminar on 23 April 2018 in which key observations and practices from this review will also be discussed and to which AIs are encouraged to attend.

If you have any questions on this circular, please contact Ms Joyce Chan at 2878-8281 or Ms Queenie Chan at 2878-1514.

Yours faithfully,

Carmen Chu
Executive Director (Enforcement and AML)

Encl.

---

[2] This should be conducted by a party having subject matter expertise. While some AIs may have dedicated teams, others may need to seek external input depending on individual circumstances.

Feedback from Thematic Reviews of AIs' Sanctions Screening Systems

AIs should take adequate measures, which include effective sanctions screening systems which are appropriate to the nature and size of businesses, to meet their obligations under Hong Kong's financial sanctions regime. These obligations, together with other relevant considerations, are set out in Chapter 6 of the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (For AIs)[1] (AML Guideline). It is the HKMA's regulatory requirement on AIs that sanctions screening should be conducted for new customers and payments as well as for existing customers whenever new designations are published[2].

This note provides feedback from thematic reviews conducted over the past few months and aims to provide further guidance to AIs in implementing effective, risk-based screening systems. To provide greater clarity, specific regulatory expectations are included in text boxes and may be used by AIs as self-assessment questions. Key observations are provided together with some examples of good practices for reference, while AIs should note that these are not meant to be an exhaustive list for meeting regulatory expectations.

Given the focus of the thematic review exercise, this note does not cover other aspects of effective sanctions risk management, for example, the quality of data input (for completeness and accuracy) or the quality of the data output (how matches are being investigated and escalation handled). AIs should make further reference to the AML Guideline and the HKMA Guidance Paper 'Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting' issued in December 2013, adopting a risk-based approach in implementation.

---

[1] Chapter 6 'Financial Sanctions and Terrorist Financing'
[2] Paragraph 6.22 AML Guideline

1. | **AIs' senior management should consider the risk of sanctions breaches and determine the appropriate level of sanctions screening to manage the risk for the AI**

1.1 AIs should be able to demonstrate a proven methodology for determining system settings and performance, and which is consistent with compliance policies and risk appetite.   This includes a thorough understanding of the risks, the types of customer the AI has and the geographic regions the customers are operating in.   Most AIs as examined in the thematic review were able to articulate their respective choices of system configuration and settings to varying degrees and some in great detail, while a few AIs demonstrated over-reliance on the vendor and were only able to provide a more simplistic response, without being able to provide clear reasons why specific settings had been adopted.

1.2 Where a group-wide policy is in place, AIs must understand and be able to justify, in line with compliance policies and risk appetite, any variations in system settings or configuration adopted locally which impacts performance of the system.   This applies to the lists and data which are entered into systems and against which screening is conducted and also the algorithms / rules utilised (referred to as "system filters").   Some variations were observed in the thematic review while a few AIs were unable to adequately demonstrate how any deviation from the group-wide policy would affect the effectiveness and efficiency of its screening system, such as accuracy and number of alerts generated.

1.3 While not included in the review, as additional guidance, Management Information (MI) should provide senior management with adequate information to understand the financial crime risks to which the AI may be exposed.   In the context of sanctions risk management, this may include an overview of the sanctions risks to which the AI is exposed, the effectiveness of certain aspects of system performance, such as screening and relevant information regarding volume of alerts, details of false positives, genuine sanctions hits, etc.

<table>
<tr>
<td>**2.**</td>
<td>**New systems, or upgrades to existing systems need to be thoroughly tested and tuned prior to deployment, with sufficient levels of reporting and oversight**</td>
</tr>
</table>

2.1 A few AIs were not able to demonstrate that adequate testing had taken place before system deployment.   As a good practice, AIs should take steps to satisfy themselves the system is appropriate and operating as expected before relying on automated screening systems.   If an AI is upgrading an existing screening system, testing should be conducted prior to deployment to check that all system filters work properly and that the new system is an improvement over the old one.   AIs should document that testing and analysis have been duly conducted.

<table>
<tr>
<td>**3.**</td>
<td>**Ongoing monitoring, tuning and testing should be conducted on all aspects of sanctions screening systems, lists and processes on a regular and frequent basis**</td>
</tr>
</table>

3.1 AIs are expected to have an adequate understanding of their obligations under the sanctions regime in Hong Kong and, as applicable, in other jurisdictions in relation to AI's international operations.   Generally, most of the AIs examined in the thematic review had an adequate understanding of the above obligations.

3.2 Most AIs carried out quality assurance work on the effectiveness of their sanctions systems, although frequency and intensity varied.   Many AIs had systems validated by external vendors and where this was the case, there was generally a better understanding of system / filter performance and the various factors underpinning such performance.   Most AIs in the review exercise expressed that system effectiveness was one of the more challenging areas to test, since it required dummy data to validate the end result.   It should be noted that regardless of how testing is performed, the testing process should be independent and provide the level of validation required.

3.3 With regards to frequency of testing, running a test once a year or every few years will not provide sufficient ongoing comfort that best efforts are being made to meet obligations.   Testing must be performed frequently to maintain a system which is both effective and efficient, ensuring that latest sanctions list changes are tested and that system filters are operating within expectations[3].

---

[3] The database of AIs' designated parties should be updated in a timely manner in accordance with Chapter 6 of the AML Guideline.

As revealed in the thematic review, a few AIs which did not carry out frequent testing and tuning internally were unable to demonstrate an adequate understanding of system filter performance and had not collated the necessary information and data to make correct decisions with regards to system settings.

4.	**AIs are expected to have a clear and demonstrable understanding of the system filters utilised in their screening technology, and to employ / equip staff with the right skills and knowledge to support the deployment of effective sanctions screening systems**

4.1 Many AIs as examined in the review had developed appropriate internal training programmes for staff in key roles. During the post-test interviews, these AIs with training programmes and relevant subject matter expertise demonstrated a more thorough understanding of system filter performance. It was apparent in a few other interviews, however, that staff had not been provided with the right skills to support effective system deployment.

4.2 Most AIs in the review exercise were able to clearly describe specific decisions around the lists their system operated and the filters employed. Explanations for each setting within the system should be properly documented. The review also revealed a few AIs that had limited knowledge of system filter performance or whether certain sanctions lists were in scope of the screening system or not.

4.3 There should also be clarity around ownership and accountability of the risk and which functions, compliance or information technology units, should contribute to managing that risk, for example, by ensuring that sanctions lists are kept up to date.

4.4 Suppression (or good guy/false hit) lists should be subject to particularly robust oversight. The reason for the inclusion of each entry should be documented properly, and these lists should be subject to regular maintenance and reviews. Appropriate approval should also be sought with respect to these regular reviews, as well as prior to the inclusion of any entry into these lists.

5. **AIs are expected to conduct ongoing tuning of system filters to reduce the level of false positives without compromising effectiveness**

5.1 AIs should understand their required level of effectiveness based on risk appetite, but should at the same time tune the system for greater efficiency where possible. Most AIs in the review understood the competing relationship between effectiveness and efficiency of the system and could evidence this understanding through actions such as monitoring levels of false positives. In those AIs where there was proactive and ongoing fine tuning to achieve greater efficiency, there was also a more comprehensive understanding of how the system, and the filters employed, operated. In a few AIs we noted high volumes of alerts, and where there were great dependency on vendor support and a general lack of awareness of the need for system optimization in one or two cases.