Comment on CPMI-IOSCO Guidance on Cyber Resilience for FMIs made by the Hong Kong Monetary Authority (HKMA)

1. With respect to the category on "**Detection**", the HKMA would like to suggest making certain changes to the section 5.2 "Detecting an attack" as follows:

   - Consideration can be given to moving the section of "**Vulnerability Assessment (VA)**" from the section 7, under the category of "Testing", to the category of "Detection". Based on our discussions with some global banks, VA is conducted on an on-going basis now given the rapidly changing cyber environment and the growing risk of cyber attacks. VA is more a day-to-day activity under the cyber security operation and monitoring function rather than a testing requirement as in the past. VA is also conducted before significant system changes.

   - Consideration can be given to including the following points:

     (i) In the section 5.2.1 "**Continuous Monitoring**" –
     "To facilitate the detection of anomalous activities and events prior to occurrence of disruptions, it is suggested that an FMI should first define the normal patterns of activities at the network level and system level so that anomalous activities and events can be easily identified during the continuous monitoring process."

     (ii) In the section 5.2.3 "**Layered detection**" –
     "An FMI should review, and revise if necessary, the detection process before significant system changes. Also, the revised detection process should be adequately tested to ensure that it is functioning as expected and does not cause any undesirable impact on other system processes."

2. Under the section 6.2.2 "**Resumption within two hours**", consideration can be given to replacing the term "critical operations" by "time-critical operations".

The Hong Kong Monetary Authority

December 2015