HONG KONG MONETARY AUTHORITY
香港金融管理局

Banking Supervision Department

Our Ref: B1/15C
B9/29C

12 August 2014

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Disruptions of critical banking services

In the light of some significant disruptions of critical banking services (e.g., online banking, phone banking, ATM, branch services, etc.) in recent months, I am writing to reiterate the importance of sufficient management oversight exercised by authorized institutions (AIs) to ensure effective incident management capability and a high level of system availability of their critical systems, in line with the sound practices set out in this circular.

Incident management capability

Given that the risk of service interruptions cannot be completely eliminated, AIs are reminded to observe the circular issued by the HKMA on "Incident response and management procedures" of 22 June 2010 to ensure, among others:

(i) timely handling of significant incidents involving disruptions of critical banking services. For instance, an AI's top priority should be to protect the interests of customers who have been or may be affected by a disruption. The AI should also assess whether the disruption is likely to affect other customers or the customers of other AIs (e.g., where the incident relates to the use of shared ATM networks); and

(ii) prompt notification of the affected customers. AIs should proactively notify the customers affected or likely to be affected through the most effective means and inform them of the precautionary steps required, any estimated service resumption time and, where applicable, how customers can apply for compensation for any losses incurred by the disruption. Where the disruption may last for a prolonged period of time or it may affect many customers, AIs should consider making a public announcement where the situation so warrants, such as if it is one of the faster or more effective communication

means than individual notifications[1]. Taking into account our observations of how relevant AIs were handling service disruptions in the past months, we generally expect an AI to issue a public announcement (or a similarly effective notification) shortly after any disruption of its critical service that could affect many customers if the AI does not have a reasonable confidence that the service would be resumed in the near future.

AIs should ensure that they have the capacity of handling incidents and notifying affected customers promptly, in line with the above practices, at all times even for service disruptions during weekends or non-office hours.

Disaster recovery and preventive controls of system disruptions

In line with the relevant HKMA's guidance[2], AIs' IT function should formulate a service level agreement with business lines covering system availability. Against this system availability benchmark, AIs should ensure the continued availability of their critical systems by maintaining and servicing IT facilities and equipment in accordance with industry practices and suppliers' recommended service intervals and specifications. Moreover, AIs should continuously monitor the performance of their critical systems, and formulate and drill regularly an IT disaster recovery plan to ensure that critical systems can be resumed in accordance with the business recovery requirements.

According to the information provided by relevant AIs, some system disruptions of critical services in recent months were caused by (i) problems in the actual implementation of some conventional IT controls such as poor change management process and inadequate testing on system changes (see **Annex** for examples); (ii) deficiencies in the resilience design and setup; or (iii) a lack of proper system monitoring and maintenance. Therefore, AIs should also take appropriate measures having regard to these lessons learnt from recent system disruptions. As some system disruptions happened during, or caused by, scheduled system maintenance or drill exercises conducted over weekends or office hours, AIs should implement proper precautionary measures (see **Annex** for examples) before and during scheduled maintenance or drills.

Regular reviews commissioned by AIs' management

To protect AIs' reputation and reduce the impact on customers that may be caused by disruptions of critical services, we expect AIs' management to commission regular reviews on the above-mentioned areas and address any inadequacies identified. The HKMA would assess the effectiveness of AIs' management oversight including the outcome and follow-up actions of such regular reviews, especially when an AI experiences a significant disruption of its critical service(s).

---

1 These may include, for instance, calling the affected customers or sending SMS messages to the affected customers.

2 For example, these include the Supervisory Policy Manual module "TM-G-1 General Principles for Technology Risk Management" and the circular on "Examinations on Controls over Information Technology (IT) Problem and System Change Management (Jan 2008)".

Should you have any questions on the content of this letter, please feel free to contact Mr George Chou at 2878 1599 or Mr Michael Chan at 2878 1531.

Yours faithfully,

Sunny Yung
Acting Executive Director (Banking Supervision)

Encl.

Annex

Common control weaknesses observed in testing and change management processes that led to recent system disruptions

- Lack of end-to-end testing which simulated the production environment and the actual transaction volume before launching system changes into the IT production environment;

- Inadequate testing of exceptional scenarios and the implication of holidays for the system behavior;

- Incorrect instructions leading to changes for testing environment mistakenly applied to the production environment;

- Absence of dual control to prevent human errors during implementation of system changes;

- Inappropriate scheduling of changes to fall on business hours; and

- Failure of applying system/configuration changes to all the areas required (e.g., changes were made only to the primary system/equipment but not the backup system/equipment), causing problems in disaster recovery or system resilience.

Precautionary measures before and during scheduled system maintenance or drills

- Management oversight and monitoring over the scheduled system maintenance/drills and related preparation/follow-up actions;

- Proper preparation (e.g., proper maintenance/recovery procedures, testing on the changes with satisfactory results, well-tested fall-back procedures to cater for any exceptional and unexpected situations) before the maintenance/drills;

- Live test after the scheduled system maintenance/drills to ensure the healthiness of the relevant services;

- Adequate upfront notifications to relevant customers about the service outage (e.g., the services that would be affected and the duration of the impact);

- Arrangements that ensure prompt responses to customer and media enquiries that may arise during or after the affected period; and

- Procedures on proper and timely escalation to senior management and public communication plan to cater for exceptional and unexpected situations (e.g., the scheduled system maintenance/drills could not be completed in time and the services could not be resumed as scheduled).