HONG KONG MONETARY AUTHORITY
香港金融管理局

Circulars

07 Jan 2008

Examinations on Controls over Information Technology (IT) Problem and System Change Management

Our Ref. : B1/15C
B9/29/2C

7 January 2008

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Examinations on Controls over Information Technology (IT) Problem and System Change Management

The Hong Kong Monetary Authority (HKMA) has recently completed a round of on-site examinations of selected authorized institutions (AIs) on their controls over IT problem and system change management. The examination results indicate that there are rooms for improvement in respect of certain aspects of the controls over IT incident management and implementation of emergency system changes by the examined AIs.

Specifically, our examinations found inadequacy in the process of reporting, risk assessment, escalation and rectification of IT problems. For instance, some AIs have underestimated the risk implications or incorrectly categorised the severity of certain reported IT incidents. As a consequence, lower priority and insufficient resources have been assigned for identifying and rectifying the root cause of these IT incidents, which is intended for preventing the incidents from recurring or evolving into a major system disruption incident. In addition, control weaknesses are identified in relation to the implementation of emergency changes to production systems and IT infrastructure. Some emergency system changes are not supported by formal documentation, and access to and use of high-privilege user and system IDs are not adequately controlled. These control weaknesses will obviously increase the risk of unauthorised access to the production system environment and thus the chance of system disruptions.

To help the banking sector improve the controls over IT problem and system change management, I set out in Annex 1 and Annex 2 respectively for your reference a list of major common issues and some good practices adopted by the examined AIs. I would also like to take this opportunity to remind your institution of the need to regularly assess the adequacy of the IT problem and system change controls within your operating environment.

Should you have any questions about the content of this circular, please contact Mr. Shu-pui Li at 2878-1826 or Mr. Nelson Chow at 2878-1470.

Yours faithfully,

Arthur Yuen
Executive Director
(Banking Supervision)

Annex 1 - Common Controls Issues Identified

Reporting, risk assessment, escalation and management of IT problems

Delays in IT problem resolution and recurring of incidents

- Delays in replacing a faulty system component have finally caused a major system disruption incident.
- Although some reported IT incidents are found to have affected the customer services such as outages of the ATM and phone banking services, these incidents are only assigned with a low severity level. It resulted in delays of problem resolution.
- A number of recurring IT incidents are believed to be caused by insufficient testing before system implementation.

Misleading problem trend analysis reports

- Misclassification of problem severity of (e.g. lower severity level assigned to severe incidents), and wrong root causes being identified for, IT problems resulting in possible misleading outcome of problem trend analysis.
- Some AIs do not adopt automated tools for IT problem reporting and management. In some cases, the problem records are manually maintained and resulted in incomplete records.

System change requests and implementation

Inappropriate timing for scheduled changes to critical systems

- A few AIs sometimes implement scheduled changes to critical systems and infrastructure close to the commencement of business hours. Such arrangements increase the risk of system disruptions to the production environment during business hours.

Handling of high-privilege IDs for change implementation

- A few AIs do not monitor and review the usage of high-privilege user and/or system IDs, particularly after change implementation. In addition, access attempts to firewalls performed by IT support staff have not been reviewed. As a result, unauthorised changes and/or errors made during routine maintenance work to critical network infrastructure might not be detected promptly.

Inadequate emergency change request process

- A number of AIs have implemented emergency changes to the production systems without the support of any valid and/or approved problem tickets.

Annex 2 - Good practices adopted by certain AIs

Senior management oversight

- Several AIs produce regular and good quality problem statistics and trend analysis reports (including categorisation and detailed root cause analysis of the incidents) for review by the senior management.
- A number of AIs have established a dedicated change management committee or function to review and prioritise system and infrastructure change requests. Such dedicated functions help ensure that scheduled changes are properly managed, prioritised and approved, and sufficient resources are allocated to the change requests.

Reporting, escalation and management of IT problems

- All AIs examined have established a designated incident response team and structure to oversee the problem management process.
- A few AIs have developed a set of comprehensive procedures for problem reporting and escalation, including a mechanism for assessing the need to report the incidents to relevant authorities.

Scheduled system change requests and implementation

- A few AIs have established "Change Windows" (i.e. the periods of time that changes to production systems are allowed to be made) for individual systems which are mutually agreed between the IT department and business users. The "Change Windows" for high-risk changes are required to be allocated to non-business days (e.g. weekends / long weekends) and long before commencement of business hours to allow sufficient time for fallback implementation if required.
- Some AIs have implemented an effective network monitoring and management system to record and monitor user activities and system changes to network equipment to ensure timely detection of unauthorised changes.
- A few AIs have implemented a remote console system that enables IT support staff to have direct logical access to the production system and infrastructure to facilitate problem troubleshooting, and implementation of emergency changes. The remote console system avoids the need of IT support staff to enter the data centre physically. The system is installed in a secured room and access to the system is restricted to authorized staff only. Audit trails of access to the production systems and infrastructure are also maintained.

Emergency change requests and implementation

- Some AIs have established a stringent emergency system change policy that requires all emergency changes be substantiated with a valid problem ticket and proper approval. The AIs concerned also conduct regular post-implementation reviews to facilitate timely detection of unauthorised changes and to identify any policy non-compliance issues.

Others

- A number of AIs have implemented automated systems for problem and change management (e.g. problem assignment, approval process and status monitoring).
- A few AIs have implemented automated systems for managing password assignment and reset of high-privilege users' and systems' passwords to facilitate monitoring of their usages in particular for problem troubleshooting or change implementation.

Last revision date : 01 August 2011