



HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C

27 September 2024

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Risk Associated with Third-party IT Solutions

In the light of the recent global IT incident arising from the faulty update of a cybersecurity solution provider, the HKMA would like to share insights gathered from its industry engagement and remind your institution to ensure that adequate measures are put in place to effectively manage third-party dependencies and enhance the operational resilience against the failure of third-party IT solutions.

The widespread impact of the global incident may be attributed to the service provider's testing issues before product update, the concerned solution's ability to push automatic update without users' controls, and inadequate risk management around third-party software.

Following the incident, the HKMA has reached out to major Authorized Institutions (AIs) to gather insights on risk management measures aimed at preventing similar incidents in the future. In addition to the principles and guidance provided in the HKMA's Supervisory Policy Manual modules, Cyber Risk Assessment Framework (C-RAF), and circulars on third-party risk management, the HKMA expects the senior management of AIs to ensure that their institutions take into account the good industry practices (see Annex) in reviewing and enhancing their risk management controls.

Should you have any questions, please contact us via e-mail at opr_incident@hkma.iclnet.hk with provision of your institution's contact information.

Yours faithfully,

Carmen Chu
Executive Director (Banking Supervision)

Encl