

# HKMA Cybersecurity Risk Management Circular 2015

September 2015

## Why is this important?

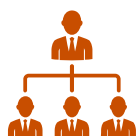
In response to the recent increase in cyberattacks, the Hong Kong Monetary Authority (HKMA) issued a circular, *Cybersecurity Risk Management*, on 15 September 2015 to emphasise the importance of robust cybersecurity risk management. In particular, the HKMA highlighted how authorised institutions (AIs) should prepare themselves and play a proactive role in mitigating cybersecurity risk.

AIs' senior management is responsible for understanding the requirements of the *Cybersecurity Risk Management Circular* and for strengthening cybersecurity controls to safeguard AIs' critical assets.

The *Cybersecurity Risk Management* circular can be downloaded below:

<http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2015/20150915e1.pdf>

## What are the focus areas?



### Cybersecurity risk ownership

Clear ownership and accountability of cyber risk should be established. AIs should establish effective cybersecurity risk management measures across all business lines, contractors, service providers, and overseas offices of their banking group.



### Periodic cyber control benchmarking and reporting

The HKMA expects AIs to perform periodic assessments of cybersecurity controls against credible industrial benchmarks (e.g. SANS Top 20 Critical Security Controls) to determine whether the existing cybersecurity controls should be strengthened. AIs' boards should review the results of these periodic assessments and take the appropriate action to strengthen the organisations' cybersecurity position.



### Incident reporting and industrial collaboration

AIs should designate relevant functions to collaborate with other institutions and the police by enforcing an effective incident reporting mechanism and sharing cyber threat intelligence.



### Proactive cyberattack contingency planning

AIs' business continuity plans (BCPs) should include measures to address cyberattack scenarios. Drills for cyberattacks should be carried out regularly so that management is trained to deal with cyberattacks.




### Regular independent assessments

AIs are encouraged to engage parties with cybersecurity expertise to perform independent assessments and penetration tests to ensure the ongoing effectiveness of cybersecurity controls.


## Assessing your readiness

In *Cybersecurity Risk Management*, the HKMA explains that it expects Als' boards and senior management to begin strengthening their oversight so that **concrete progress can be seen in the remaining board meetings in 2015**.


The following are some of the key questions to assess your readiness level:




Do current risk management processes adequately highlight cyber risk for the board?




Is the corporate value of information assets clearly understood?




Does the organisation's risk appetite account for cyber risk?



What future steps are being planned by management to mitigate cyber risk in a cost-effective manner?



Is there an appreciation of the business benefits of proactively managing cyber risk?



Is the corporate impact clearly understood if information assets are stolen, corrupted or destroyed?

### KEY QUESTIONS

to assess your readiness

## How can KPMG help?

KPMG can help you assess your cybersecurity exposure by identifying gaps where immediate focus will be required. The KPMG approach to cybersecurity focuses on people, process and technology. We can help you assess your current cybersecurity position and provide scorecard reporting together with assistance to help you implement industry practices on cybersecurity management as below:



## Contact us

If you would like further information or recommendations on cybersecurity risk management, please contact one of our Cyber team leaders:

**Henry Shek**  
Partner, Advisory  
KPMG China  
T: +852 2143 8799  
E: henry.shek@kpmg.com

**Paul McSheaffrey**  
Partner, Advisory  
KPMG China  
T: +852 2978 8236  
E: paul.mcsheaffrey@kpmg.com

**Kelvin Leung**  
Director, Advisory  
KPMG China  
T: +852 2847 5052  
E: kk.leung@kpmg.com

**Alvin Li**  
Associate Director, Advisory  
KPMG China  
T: +852 2978 8233  
E: alvin.li@kpmg.com