

Foreword

In view of an ever-evolving technology landscape and the potential risks associated with this, the "Hong Kong Monetary Authority (HKMA)" issued the new TM-E-1 Risk Management of e-Banking in September 2015 ("new TM-E-1") to cover a wider scope of electronic banking (e-banking) services. The new requirements cover phone banking, internet banking, mobile banking, self-service terminals, e-banking services in social media platforms and contactless mobile payments. Additionally, a supplementary document titled Additional Guidance for SPM TM-E-1 was issued to further elaborate on the technical requirements and controls pertaining to the provision of e-banking services. The Hong Kong Monetary Authority (HKMA) had previously issued Supervisory Policy Manual (SPM) TM-E-1 Supervision of E-banking in 2004, which set out the minimum control standards for e-banking platforms deployed by banks.

The implications of the new requirements for banks in Hong Kong include:

- (1) An extended scope of e-banking requirements for banks to assess their compliance: The new TM-E-1 covers many new risk management aspects that were not mentioned in previous regulations or guidance. Banks will need to perform a comprehensive review based on the new TM-E-1 to ensure compliance with the extended scope of requirements.
- (2) Increased regulatory focus on technology risk and cyber risk: The new TM-E-1 is a sign that regulators are adapting to the evolving technology risk and are actively issuing new directives to heighten the technology control standard of the industry. This also suggests that there will be more measures to come in the near future.
- (3) Opportunities for banks to gain business benefits by exploring new e-banking channels: The extended scope of the new TM-E-1 to cover emerging e-banking channels such as mobile banking, social media platforms and contactless mobile payments is an indication of e-banking industry trends. Banks should take this opportunity to assess the potential benefits brought by these emerging e-banking channels, and determine the upcoming technology strategy and road map.



Henry Shek Partner, Advisory



Kelvin Leung



Background

E-banking services, such as internet banking, mobile banking and phone banking services, have increasingly become the preferred way for customers to interact with banks. Many banks in Hong Kong have long offered e-banking services for customers to perform online balance enquiries and fund transfers. Due to the increasing use of mobile devices and social media platforms in recent years, many banks have been enhancing their existing e-banking platforms, including improving their e-banking mobile apps and leveraging the functions offered by various social media platforms. Although these advancements in e-banking technologies have improved convenience for banking customers, they have also presented a bigger security threat.

Is your bank ready to take advantage of the business benefits brought about by the latest e-banking technologies? In addition, does your bank have adequate controls over e-banking to ensure compliance with the new requirements?

The following are some of the key updates in the new TM-E-1 issued in 2015.



A Comprehensive Set of Requirements for e-Banking



Staffing Resources and Competence to Manage e-Banking



Penetration Testing and Source Code Reviews



Small Value Fund Transfer



Requirements for Online Submission of Information



Specific Controls for Mobile Banking







Self-service Terminals



Contactless Mobile Payments



Distributed Denial of Service (DDoS)



Capacity Planning,
Performance Monitoring and
System Resilience



Customer Notifications

Highlights - Key Updates

A Comprehensive Set of Requirements for e-Banking Services



TM-E-1 (2004 version)

The e-banking requirements consist of one SPM and a number of other HKMA circulars covering two-factor authentication, incident response, account aggregation services, etc.

New TM-E-1 (2015 version)

The new TM-E-1 includes all the requirements related to the provision of e-banking services, superseding nearly all the previous SPMs and circulars related to e-banking. Banks will only need to reference the new TM-E-1 for most of the compliance requirements related to e-banking services.

Staffing Resources, Accountability and Staff Competence to Manage e-Banking



The risk pertaining to e-banking systems, including staffing resources, should be overseen by the bank's board and senior management.

The new TM-E-1 further elaborates on the requirements for managing e-banking risk, including the need to have adequate staff resources and staff expertise, in addition to senior management oversight. Banks should clearly specify the management and staff accountability for managing e-banking risk, and banks should not launch e-banking services if they do not have the required resources and expertise.

Penetration Testing and Source Code Reviews on Internet Banking Systems



The independent assessor would consider the need to perform penetration testing during the independent assessment of internet banking systems.

Management should ensure that regular penetration testing is performed by qualified independent parties on internet banking systems. Additionally, the bank should perform periodic vulnerability assessments to detect security vulnerabilities in the internet infrastructure supporting the internet banking system. If a new internet banking system is launched or if there are system changes, a party independent of the system developer should perform an application source code review to identify noncompliance with their security coding standards.

Internal nking Upda

Small Value Fund Transfer

\$

TM-E-1 (2004 version)

Fund transfers to unregistered third parties are considered high-risk transactions and should be subject to two-factor authentication.

New TM-E-1 (2015 version)

Small value fund transfers to unregistered third parties can be performed without two-factor authentication. Banks should refer to the requirement stated in the Additional Guidance for SPM TM-E-1, and also consider the banks' own risk appetite when determining the caps for small value fund transfers.

Internet Portal for Online Submission of Information



There are no specific requirements regarding the submission of information (e.g. application forms) online.

Banks are required to assess the risk and establish controls over the submission of information online. Some of the controls required by the new TM-E-1 include:

- The use of encryption to protect the confidentiality and integrity of the information submitted online
- Controls to detect malware attacks through the documents submitted
- Additional checks to validate the identity of the customer submitting the information.

Specific Controls for Mobile Banking



There are no specific requirements regarding the provision of mobile banking services.

Banks are required to assess the specific risk relevant to mobile banking, and formulate security measures to address those risks. The specific risks mentioned in the new TM-E-1 include: security vulnerabilities associated with mobile platforms; risk from malware and malicious mobile apps; risk of loss or theft of mobile devices; and customers' security awareness.

Social Media Platforms

TM-E-1 (2004 version)

New TM-E-1 (2015 version)



There are no specific requirements regarding the provision of e-banking services through social media platforms.

Banks are required to assess the specific risks relevant to providing e-banking services through social media platforms, and formulate security measures to address those risks. In particular, banks should ensure the following:

- (1) Legal due diligence has been undertaken on the social media platform to ascertain that any applicable local or overseas legal or regulatory requirements are being complied with.
- (2) Security controls are implemented to minimise the risk of intrusion in the bank's system and leakage of customer data through social media platforms.
- (3) Independent assessment over the risk of intrusion to the bank's systems and risk of data leakage.

Self-service Terminals



There are no specific requirements regarding the provision of banking services through self-service terminals (e.g. automatic teller machines (ATMs)).

Expanded requirements have been set out to mitigate risk related to self-service terminals. This includes requirements to use chip-based authentication for ATM cards, controls over overseas ATM cash withdrawals, the use of ATM keypad covers, the use of card antiskimming devices, controls to detect counterfeit banknotes, the use of closed-circuit television (CCTV), and the implementation of customer education programmes.

Contactless Mobile Payments



There are no specific requirements regarding contactless mobile payments.

Banks are required to assess the security risks related to contactless mobile payments and formulate measures to mitigate security risks. Such risks include (1) the leakage of credit card information through electronic pick-pocketing; and (2) fraudulent transactions due to loss or theft of mobile devices. Additionally, banks should ensure that contactless mobile payment services comply with security standards issued by banking industry associations.

TM-E-1 (2004 version)

New TM-E-1 (2015 version)

Distributed Denial of Service (DDoS)



The previous TM-E-1 required that banks implement measures to guard against different types of online attacks. However, there are no specific requirements regarding DDoS attacks.

DDoS attacks are specifically mentioned in the new TM-E-1, and banks are required to implement controls to promptly detect and respond to DDoS attacks. Banks are also required to regularly review the effectiveness of their controls to guard against emerging DDoS attack techniques.

Capacity Planning, Performance Monitoring and System Resilience



Requirements to consider the capacity of e-banking systems are included as part of the 'Business Continuity Considerations' for e-banking services. Apart from that, there are no specific requirements regarding capacity planning, performance monitoring and system resilience.

Expanded requirements related to system resilience, capacity planning and performance monitoring have been included in the new TM-E-1. Specifically, banks should implement automated performance monitoring and alert system that cover all e-banking-related systems and network infrastructure components.

In addition to the controls above. banks' IT functions should establish service level agreements with business lines regarding the agreed availability of the e-banking systems.

.....

Customer Notifications



Banks are required to notify customers immediately through alternative automated channels (e.g. SMS messages) after customers conduct high-risk transactions.

The new TM-E-1 has reinforced the need for prompt customer notification after performing high-risk transactions. In addition to high-risk transactions, banks are also required to promptly notify customers for a number of other transactions including card-notpresent (CNP) credit card transactions and small-value fund transfers. The details of the customer notification requirements are stated in the "Additional Guidance for SPM TM-E-1."

Leading Practices for the Provision of e-Banking Services

One of the key risks pertaining to e-banking systems using the internet is cybersecurity risks. In recent years, a number of high-profile cyberattacks on e-banking systems have led to massive service disruptions and data leakages. With the increased frequency and sophistication of cyberattacks, many organisations are performing in-depth reviews to understand the capabilities of the IT function with regard to mitigating cyber risks. The following 6 domains are the key areas that organisations should look into when addressing cyber risks.



Based on our experience, the following are some of the leading areas that you should begin to assess maturity on cyber / Internet risks:

Leadership and Governance

Clear Roles and Responsibilities for the Three Lines of Defence

E-banking risk management and governance should be supported by clear responsibilities and accountability from the three lines of defence. In general, the first line of defence refers to the technology/IT department responsible for the development and maintenance of the e-banking systems. It is the responsibility of the first line of defence to ensure that the e-banking system is designed, developed and maintained according to the established policies and procedures. Any non-conformance with the established policies and procedures due to practical reasons should be escalated to obtain management approval.

The second line of defence usually refers to the risk management and compliance departments. In general, the second line of defence is responsible for monitoring the changes in risk landscape and compliance requirements, assisting in the formulation of policies and procedures, and performing periodic checks to ensure that the established policies and procedures are duly adhered to by the first line of defence. The second line of defence should regularly evaluate the adequacy of controls implemented by the first line of defence, and enhance existing controls if necessary.

The third line of defence usually refers to the internal audit department or similar functions that are independent of the bank's day-to-day operations. The roles and expectations of the HKMA for the internal audit department are clearly stipulated in SPM IC-2 Internal Audit Function issued in 2009. The third line of defence should perform regular reviews and audits from an independent point of view to ensure that the controls implemented and performed by the first and second lines of defence can effectively mitigate the risk arising from e-banking systems.

Human Factors

Strong Information Security Organisation to Tackle Cyber Risk

Banks' senior management should be responsible for defining an organisation's e-banking and cybersecurity strategy, and for ensuring roles and responsibilities are appropriately assigned. Although cyber defence often starts with IT, it is actually a risk for the bank as a whole and should be addressed at the organisation level, and not left with IT to handle alone. C-suite management should work closely with IT and other relevant security divisions to help them understand the real risk beyond technology.

In addition to senior management oversight, training your staff on e-banking and cybersecurity issues is an effective way to counter cyber threats. Raising security awareness helps to improve the weakest link in cybersecurity people. A lot of recently identified cyberattacks were initiated through penetrating the 'people' layer by using various social engineering techniques (e.g. phishing emails).

12 | Internet Banking Updates

Information Risk Governance

Comprehensive Policies for e-Banking

With the continuous evolution of regulatory requirements pertaining to the risk management of e-banking systems, banks should regularly review and update existing policies and procedures to ensure alignment with the latest regulatory requirements and industry best practices. From experience some of the common pitfalls we have identified are:

- There are no established policies regarding the need to perform regular risk assessments of e-banking systems. Requirements relating to the risk assessment of e-banking services should be formally documented and the results of the risk assessment should be used to analyse and determine whether regular independent assessments should be performed across all e-banking platforms.
- Policies and procedures regarding the monitoring of unusual or suspicious activities performed by e-banking users are inadequate. For example, there are no implemented controls to detect the initiation of high-risk transactions through the internet using an internet protocol (IP) address different from the one usually used by the customer.
- Incident response policies do not clearly state the criteria to determine
 whether an e-banking incident should be escalated to the local regulators
 such as the HKMA, the Securities and Futures Commission (SFC) or the
 Hong Kong Police Force (HKPF).
- Policies and procedures regarding system capacity planning and capacity management for e-banking systems are not formally documented.
- There are inadequate policies to identify training that keeps IT staff abreast of the latest technologies and evolving cyberattacks.

With the increased adoption of different e-banking platforms, it is good practice for banks to review their e-banking policies and procedures from time to time to ensure alignment with regulatory requirements and industry best practices.



Business Management and Crisis Management E-banking System Resilience and Contingency Plans

For e-banking systems that are critical to the bank's operations, it is important to have robust system resilience plans and contingency plans to safeguard the risk of unplanned service disruptions. The network and application infrastructure supporting the e-banking platforms should be analysed to identify areas that are susceptible to the risk of a single point of failure. System resilience measures such as high-availability configuration and backup devices should be implemented to safeguard the risk of a single point of failure. Disaster recovery plans should also be established to handle disastrous events such as the total failure of a data centre due to power outages or other technical issues.

In addition to system resilience and disaster recovery measures, business continuity plans (BCPs) should be updated to handle e-banking disruptions. For example, business departments and customer-facing staff should be aware of the response plans and customer communication plans in the event of e-banking channel disruptions. A contingency plan for a major e-banking disruption or security breach should be formulated so that senior management and the team responsible for crisis management can follow the contingency plan to strategise the response in such an event.



Operations and Technology

Comprehensive Risk Assessment on New e-Banking Services or e-Banking System Changes

With the rapid adoption of internet technologies, a lot of banks are looking to adopt new e-banking platforms including mobile banking, social media banking and online form submission portals. Since different e-banking platforms will pose different risks to banks, it is important that they conduct a comprehensive risk assessment to holistically assess the associated risk during the design phase of an e-banking platform. With the introduction of the new TM-E-1, banks should also revisit their risk assessment approach to cover the broader scope of e-banking as defined in the new TM-E-1.

One of the common observations regarding e-banking system risk assessments is the lack of cross-channel risk assessments. If a bank has provided more than one e-banking service to customers, it is important to assess the cross-channel risks to understand whether a compromise on one e-banking system may impact the security of other systems. For example, if the bank allows customers to view their own personal information in the online banking system, it should consider that if this system is compromised, such personal information may be used to gain unauthorised access to other banking channels or e-banking platforms such as teller or phone banking services. Therefore, it is important for banks to conduct comprehensive risk assessments on different e-banking systems to determine the extent of the impact arising from a compromised e-banking system.



Legal and Compliance

Regular Audit and Independent Assessment

The new TM-E-1 requires banks to perform regular risk assessments on existing e-banking systems to determine whether an independent assessment is necessary. In fact, with the various technology-related regulatory requirements that have been published in the past 12 months (e.g. requirements for cloud computing, customer data protection and bringyour-own-device), banks have been engaging independent parties such as the internal audit department or external consultants to holistically review their risk and compliance status with these new requirements. With the implementation of the new TM-E-1, and the various changes in the HKMA's Risk Assessment requirements, banks will need to assess their compliance status against the new e-banking requirements in order to obtain approvals or 'no-objection' from the HKMA for their new technology-related initiatives.





How can KPMG help?

KPMG has assisted numerous banks in Hong Kong to assess and define controls to comply with the HKMA requirements. Our dedicated compliance subject matter team combines industry knowledge and regulatory experience to provide wide-ranging support in regulatory compliance.

What is the compliance status at your bank? KPMG can help you assess your cybersecurity & compliance status, while taking into consideration the following new regulatory requirements:

- 1. Mitigating Cybersecurity Risks (issued by the Securities and Futures Commission (SFC) in 2014)
- 2. TM-E-1: Risk Management of E-banking (issued by the HKMA in September 2015)
- 3. Outsourcing to the public cloud
- 4. Customer Data Protection (issued by the HKMA in October 2014)
- 5. Bring-Your-Own-Device (issued by the Hong Kong Association of Banks in October 2014)

KPMG can help you navigate through the complex regulatory requirements by helping identify gaps which require immediate focus. In addition to the above new regulatory requirements, our team has in-depth experience assisting banks with their new technology-related initiatives by performing independent assessments as required by the HKMA Risk Assessment Forms, including e-banking, cloud computing, outsourcing and contactless retail payment initiatives. During the course of our independent assessments, we provide valuable insights regarding the regulatory focus areas and common industry practices so that you can position yourself to obtain regulatory approvals.

Our approach to compliance assessment focuses on people, process and technology. We can help filter your complex requirements, build them into your everyday operational processes, conduct user awareness training, and implement the technical tools required to enable the required regulatory controls.



Contact us

For inquiries related to this update, please contact us:



Henry Shek
Partner, Advisory
+852 2143 8799
henry.shek@kpmg.com

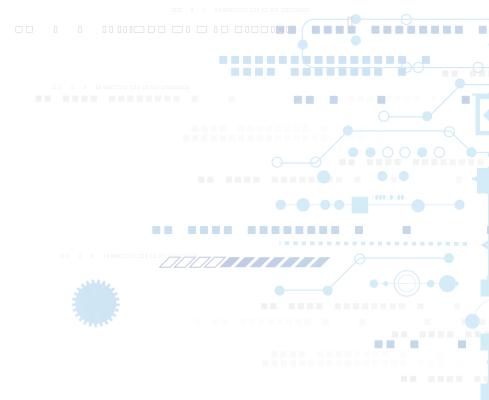


Paul McSheaffrey
Partner, Advisory
+852 2978 8236
paul.mcsheaffrey@kpmg.com



Kelvin LeungDirector, Advisory
+852 2847 5052
kk.leung@kpmg.com

Notes



Mainland China

Beijing

8th Floor, Tower E2, Oriental Plaza 1 East Chang An Avenue Beijing 100738, China

Tel: +86 (10) 8508 5000 Fax: +86 (10) 8518 5111

Foshan

8th Floor, One AIA Financial Center 1 East Denghu Road Foshan 528200, China

Tel: +86 (757) 8163 0163 Fax: +86 (757) 8163 0168

Hangzhou

8th Floor, West Tower, Julong Building 9 Hangda Road

Hangzhou 310007, China Tel: +86 (571) 2803 8000 Fax: +86 (571) 2803 8111

Shanghai

50th Floor, Plaza 66 1266 Nanjing West Road Shanghai 200040, China

Tel: +86 (21) 2212 2888 Fax: +86 (21) 6288 1889

Tianjin

Unit 15, 47th Floor, Office Tower Tianjin World Financial Center 2 Dagu North Road Tianjin 300020, China

Tel: +86 (22) 2329 6238 Fax: +86 (22) 2329 6233

Chengdu

17th Floor, Office Tower 1, IFS No. 1, Section 3 Hongxing Road Chengdu, 610021, China

Tel: +86 (28) 8673 3888 Fax: +86 (28) 8673 3838

Fuzhou

25th Floor, Fujian BOC Building 136 Wu Si Road Fuzhou 350003, China

Tel: +86 (591) 8833 1000 Fax: +86 (591) 8833 1188

Nanjing

46th Floor, Zhujiang No.1 Plaza 1 Zhujiang Road Nanjing 210008, China

Tel: +86 (25) 8691 2888 Fax: +86 (25) 8691 2828

Shenyang

27th Floor, Tower E, Fortune Plaza 59 Beizhan Road Shenyang 110013, China

Tel: +86 (24) 3128 3888 Fax: +86 (24) 3128 3899

Xiamen

12th Floor, International Plaza 8 Lujiang Road Xiamen 361001, China

Tel: +86 (592) 2150 888 Fax: +86 (592) 2150 999

Chongqing

Unit 1507, 15th Floor, Metropolitan Tower 68 Zourong Road Chongqing 400010, China

Tel: +86 (23) 6383 6318 Fax: +86 (23) 6383 6313

Guangzhou

38th Floor, Teem Tower 208 Tianhe Road Guangzhou 510620, China Tel: +86 (20) 3813 8000

Tel: +86 (20) 3813 8000 Fax: +86 (20) 3813 7000

Qingdao

4th Floor, Inter Royal Building 15 Donghai West Road Qingdao 266071, China

Tel: +86 (532) 8907 1688 Fax: +86 (532) 8907 1689

Shenzhen

9th Floor, China Resources Building 5001 Shennan East Road Shenzhen 518001, China

Tel: +86 (755) 2547 1000 Fax: +86 (755) 8266 8930

Hong Kong SAR and Macau SAR

Hong Kong

8th Floor, Prince's Building 10 Chater Road Central, Hong Kong 23rd Floor, Hysan Place 500 Hennessy Road Causeway Bay, Hong Kong

Tel: +852 2522 6022 Fax: +852 2845 2588

Macau

24th Floor, B&C, Bank of China Building Avenida Doutor Mario Soares Macau

Tel: +853 2878 1092 Fax: +853 2878 1096

kpmg.com/cn

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2015 KPMG, a Hong Kong partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in Hong Kong.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.

Publication number: HK-MC15-0002 Publication date: September 2015