Deloitte.

德勤

Latest Developments in Monetary Authority of Macao (AMCM) Guidelines

An Overview of Revisions to the AMCM Guidelines on Technology and Operational Risk Management

MAKING AN IMPACT THAT MATTERS since 1845

General Overview

As the modern financial services industry evolves and adopts emerging technologies and new business models amid emerging challenges. the Monetary Authority of Macao (AMCM) has been optimising its supervision of financial technology.

To improve regulatory compliance and security requirements while promoting development, in 2023 the AMCM further enhanced its guidelines on technology and operational risk management, including:

- Guideline on Risk Management of Electronic Banking (Circular no. 005/B/2023-DSB/AMCM);
- Guideline on Technology and Cyber Risk Management (Circular no. 017/B/2023-DSB/AMCM);
- Guideline on Outsourcing (Circular no. 020/B/2023-DSB/AMCM);
- Industry Guidance on Cloud Outsourcing Controls (Circular no. 021/B/2023-DSB/AMCM).

Key Milestones of the Technology and Operational Risk Management Guidelines

2008
- Guideline on Risk Management of Electronic Banking [Revised in 2023]

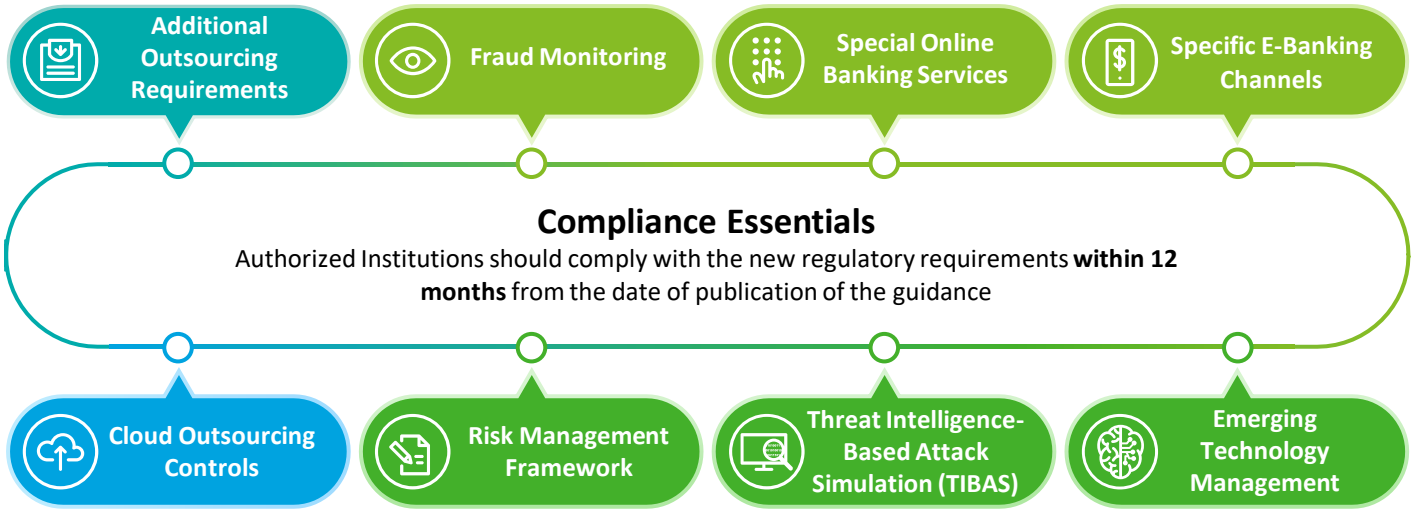
2009
- Guideline on Outsourcing [Revised in 2023]
- Guideline on Business Continuity Management

2019
- Guideline on Cyber Resilience [Revised in 2023]

2023
- Guideline on Risk Management of Electronic Banking
- Guideline on Technology and Cyber Risk Management *[Replaced Guideline on Cyber Resilience]*
- Guideline on Outsourcing
- Industry Guidance on Cloud Outsourcing Controls *[NEW]*

Key Points of the New Regulation Requirements by the AMCM

The following are the key topics of new control requirements of the new regulations. Authorized Institutions should conduct gap analysis on their existing control points as soon as possible to understand whether there are gaps or non-compliance issues, and complete related remediation measures within 12 months after the new guidelines come into effect. The AMCM will conduct on-site inspections and off-site reviews of authorized institutions to determine whether authorized institutions meet the regulatory requirements of relevant regulations.



Guideline on Risk Management of Electronic Banking (Circular no. 005/B/2023-DSB/AMCM)	Guideline on Technology and Cyber Risk Management (Circular no. 017/B/2023-DSB/AMCM)	Guideline on Outsourcing (Circular no. 020/B/2023-DSB/AMCM)	Industry Guidance on Cloud Outsourcing Controls (Circular no. 021/B/2023-DSB/AMCM)

Guideline on Risk Management of Electronic Banking (Circular no. 005/B/2023-DSB/AMCM)

Background

The AMCM issued this revised "Guideline on Risk Management of Electronic Banking" (Circular no. 005/B/2023-DSB/AMCM) on 26 June 2023. This Guideline sets forth the key principles and provides guidance for authorized institutions to identify, assess and manage the risks associated with electronic banking from technology and operations perspectives. These revisions enhance the required security measures for financial products and services provided to customers via internet banking, self-service terminals and phone banking channels, and establish a fraud monitoring mechanism to identify, mitigate and reduce the risk of fraud.

Obligation

#1 Comply with the Revised Guidance
Authorized Institutions should comply with the guideline by June 2024

#2 Independent Assessment
Independent assessment should be performed before the launch of the e-banking systems or major enhancements to existing services

#3 Risk Assessment
After completing #2, risk assessment should be performed at least every two years or in the event of substantial changes

#4 Technical Assessment
Penetration testing and vulnerability scanning should be performed at least annually. Assessment results should be submitted to the AMCM upon request

#5 Report Submission to the AMCM
#2 Independent assessment report should be submitted to the AMCM. The reports will be used as reference during on-site examinations and off-site reviews

Applicable to

Locally incorporated authorized credit institutions or branches of overseas banks in Macao

All such credit institutions that are engaging or going to engage in electronic banking activities

The following institutions that adopt/will adopt the use of electronic communication channels in the delivery of their services:

(a) finance companies licensed under Decree-law no. 15/83/M;
(b) institutions licensed under Decree-Law no. 25/99/M to carry out assets management activities;
(c) investment fund management companies licensed under Decree-Law no. 83/99/M;
(d) financial intermediaries and other financial institutions licensed under the Financial System Act.

Details on the Major Updates

Security Domain

Board and Management Oversight | **Security Controls** | **Fraud Monitoring**

Business Continuity Planning | **Outsourcing Management** | **Management of Cross-border Activities**

Fraud Monitoring	Establish fraud monitoring mechanism	Establish fraud handling process and procedure	Designated staff with relevant expertise on fraud monitoring and response	Provide continuous training for designated staff
Business Continuity Planning	Conduct regular capacity planning exercise	Establish business continuity and contingency plans, incident response and management	Conduct regular drills of the incident response plan	Implement automated performance monitoring and alert mechanisms, perform end-to-end performance tests
Security controls & other domains	Enhance authentication and authorization controls requirements	Enhance encryption algorithm requirements for confidentiality of sensitive information	Establish mobile banking (including mobile payment) security requirements	Conduct technical security assessment requirements on a regular basis (at least annually for vulnerability scanning and penetration test)
	Establish specific internet banking services requirements (e.g., funds transfers, online submission of information, remote on-boarding service, account aggregation services, and open API)	Establish specific electronic banking channels requirements (e.g., social media platforms, self-service terminals, and phone banking)	Establish customer security requirements (e.g., customer awareness program, timely notification and risk disclosure etc.)	

Guideline on Technology and Cyber Risk Management (Circular no. 017/B/2023-DSB/AMCM)

Background

The technology and cyber risk landscape of the financial sector has been transforming rapidly, with many financial institutions pursuing digitalisation to enhance operational efficiency and provide better services to customers.

To improve authorized institutions' resilience to technology and cyber risk, the AMCM issued this revised "Guideline on Technology and Cyber Risk Management" (Circular no. 017/B/2023-DSB/AMCM) on 11 December 2023, to replace the "Guideline on Cyber Resilience" (Circular No. 016/B/2019-DSB/AMCM). The new Guideline includes requirements related to the management of emerging technologies and the improvement of information technology development and operations, providing authorized institutions with a set of technology and cyber risk management principles and best practices.

Obligation

#1 Comply with the Revised Guidance
Authorized Institutions should comply with the guideline by December 2024

#2 Independent Assessments
Independent assessment should be performed at least every two years or upon notification from the AMCM

#3 Report Submission to the AMCM
Independent assessment report should be submitted to the AMCM upon request

Applicable to

- Credit institutions that are either locally incorporated or are branches of overseas banks in Macao
- Financial companies
- Cash remittance companies
- Assets management companies
- Investment fund management companies
- Other financial institutions

Details on the Major Updates

Security Domain

Technology and Cyber Risk Management Framework | Governance and Strategy | IT Project Management and System Development

IT Service Operations | Cybersecurity | Response And Recovery | Emerging Technology

Technology and Cyber Risk Management Framework	Establish Risk Management Framework & Risk Management Process	Governance And Strategy	**Enhance The Situational Awareness of Authorized Institutions & Staff** • Should include newly developed technology • Should include industry threat intelligence & information sharing forums and subscribe to threat information sources			
IT Project Management and System Development	Establish IT project Management Framework to Manage Project that Used Technology	IT Service Operations	Enhance Remote Access Management	Response and Recovery	Establish IT Problem Management	
Cybersecurity	**Cryptograph** • Adopt international standards for encryption algorithm & encryption key length	**Data Disposal and Destruction** • Establish secure process to manage data disposal and destruction	**Threat Intelligence-Based Attack Simulation (TIBAS)** • Create tailored, end-to-end cyber attack testing scenarios • Perform in a production environment to mimic real-life attack scenarios or consider to conduct tests on a simulated component that closely resembles the production component • TIBAS should be conducted by qualified tester			
Emerging Technology	**Emerging Technology Management Principle** • Establish governance framework and risk management measures	**Internet of Things (IoT)** • Maintain an inventory of all its IoT devices that can be connected to authorized institution's network/internet (e.g., multi-function printers, security cameras and smart televisions) • Implement appropriate security measures (e.g., access control, monitoring, etc.)	**Artificial Intelligence (AI)** • Governance of AI • Logging of AI application • Data security of AI application • Cybersecurity measures • Contingency measures	**Distributed Ledger Technology (DLT)** • E.g., Blockchain • Identify & assess the potential risk • Reference other governance framework / international standards / best practice		

Guideline on Outsourcing (Circular no. 020/B/2023-DSB/AMCM)

Background

With an increasing number of companies outsourcing their services, business operations, maintenance, and business activities or functions to vendor services, associated risks have come to the fore.

To ensure that all outsourcing arrangements of authorized institutions, particularly those involving material business activities or functions, are subject to appropriate due diligence, approval and on-going monitoring; the AMCM issued this revised "Guidelines on Outsourcing " (Circular no. 020/B/2023-DSB/AMCM) on 28 December 2023. The Guideline outlines the AMCM's supervisory approach to outsourcing arrangements by authorized institutions and major prudential issues to be considered when they enter outsourcing arrangements.

Outsourcing Definition

"Outsourcing" occurs when an authorized institution enters into an arrangement to transfer, generally for a fixed period, the day-to-day running of some part of its business to another party (including a related entity).

Obligation

#1 Comply with the Revised Guidance

Authorized institutions should comply with the guideline by December 2024

#2 Proposal Submission to the AMCM If Involve

- Outsourcing material business activities / functions
- Material changes/ amending existing outsourcing scope

#3 On-going Monitoring

Continually monitor the performance, financial condition and risk profile of the service provider and managing the risk associated with the outsourced activity / function

Applicable to

Locally incorporated authorized credit institutions or branches of overseas banks in Macao

Other financial institutions that are under the supervision of the AMCM

Details on the Major Updates

Risk assessment

Conduct risk assessment prior to entering into/ changing scope of existing outsourcing arrangements

Exit strategy

Establish exit strategy; manage data removal / transfer, intellectual property and information rights, termination controls and transition to other service providers etc.

Concentration Risks

Embed concentration risk into risk management framework and outsourcing policy, including:

a) Evaluate the concentration risk
b) Implement risk remediation for any concentration risk identified

Confidentiality

More in-depth requirements, such as data protection assessment related security controls, responsibilities, regular review and monitoring

Subcontracting

Conduct due diligence to manage the associated risks of subcontracting and consider below controls:

a) Included subcontractors' liability clause
b) Retained contractual rights on termination
c) Notification requirements
d) Ongoing monitoring

Material Cloud Outsourcing

(Ref to Industry Guidance on Cloud Outsourcing Controls)

Industry Guidance on Cloud Outsourcing Controls (Circular no. 021/B/2023-DSB/AMCM)

Background

With the rise of cloud computing technology, authorized institutions in Macao are increasingly taking initiatives to explore the use of cloud computing services to enhance their operations. Although the adoption of cloud computing services provides advantages such as business agility, scalability and cost savings, it creates corresponding risks.

The AMCM issued the "Industry Guidance on Cloud Outsourcing Controls" (Circular no. 021/B/2023-DSB/AMCM) on 28 December 2023. The Industry Guidance outlines the AMCM's requirements on cloud outsourcing arrangements and major prudential issues to be considered when entering cloud outsourcing arrangements.

Obligation

#1 Comply with the Industry Guidance
Authorized institutions should comply with this Industry Guidance by December 2024

#2 Consult with the AMCM for Applying New Cloud Services
Before entering into agreements of any material cloud arrangements, authorized institutions should consult and discuss their plans with the AMCM.

Applicable to

All authorized institutions incorporated in Macao and to the Macao branches of authorized institutions incorporated overseas

Other financial institutions that are under the supervision of the AMCM

The guideline applies to all cloud outsourcing arrangements ("Cloud Arrangements"), either outsource to a cloud service provider ("CSP") offering services or rely on a CSP for delivering services.

All types of material Cloud Arrangements:

Service models:
- Software as a Service ("SaaS")
- Platform as a Service ("PaaS")
- Infrastructure as a Service ("IaaS")

Deployment models:
- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

Details on the Major Updates

Security Domain

Governance | Data Location and Transfer | Audit / Review Arrangements | Outsourcing Agreements | Additional Key Controls

(A) Architectural design	(B) Virtualization containerization	(C) Data security and encryption	(D) Application security	(E) Identity and access management	(F) Change and configuration management
(G) Event and security incident management	(H) Business continuity management	(I) Training	Depending on the service models deployed, authorized institutions may share the responsibilities with CSPs over the management and operation of security controls, including (A) to (I)		

How Can Deloitte Help?

Deloitte offers a **tailored service and approach** based on our understanding of your business needs and project characteristics as well as our experience, rather than providing a standardized set of services. You can choose the most suitable assessment and advisory service according to the characteristics, type and regulatory requirements of your needs. Deloitte aims to provide a professional, continuous and flexible service model to help you save time and labor costs.

Independent Assessment

- Bank-wide compliance assessment
- E-Banking Service Launch Independent Assessment
- Third-Party Assessment
- Cloud Assessment
- Swift CSP Assessment
- Other Independent Assessment

Technical Assessment

- Vulnerability Scan
- Mobile and Web Penetration Testing
- Configuration Review
- Red Teaming
- Threat Intelligence-Based Attack Simulation (TIBAS)

Advisory

- Establish/Enhance Policies and Procedures to Achieve the Implementation of Secure and Compliant Processes
- Design and develop the client's Technology and Cyber Risk Management Framework which suitable for client's environment
- Provide Cybersecurity Awareness Training to enhance to ensure employees are well-informed and equipped to protect against cyber threats

Why Deloitte?

Know the Banking Industry and the Challenges You Face

We have **extensive knowledge in banking industry and fruitful experience in delivering projects** with similar clients, size and scope for **Macao, Hong Kong and China clients.** Such experiences provide us with knowledge of the key risks and issues that our clients are likely to face, helping our work to remain practical and effective.

Strong Professional Team

Our Engagement Partner has **over 18 years of professional experience, our assessment and technical team has many years of experience in cybersecurity advisory.** Our specialists possess **CISSP, CISA, OSCP, CREST** qualifications with the right fit of knowledge and expertise to bring value to the project.

Familiar with the Development and Trends of Cyber Security

We are well versed in the current state of cybersecurity, regulatory requirements and best practices in the financial industry in Macao. **We understand the legal and regulatory developments in cybersecurity and data privacy in various places, as well as the latest threat intelligence.** We are committed to helping our clients to interpret the regulatory requirements, improve the cybersecurity environment, and share with them the latest trends in the industry.

Start the conversation

If you are interested in learning more about our service, please contact:

Sidney Cheng
Macao Office Managing Partner

Tel: +853 8898 8898
Email: sidcheng@deloitte.com.mo

Eileen Cheng
Partner, Risk Advisory

Tel: +852 2238 7119
Email: eicheng@deloitte.com.hk

Carmen Lei
Director, Central Business Development

Tel: +853 8898 8833
Email: carlei@deloitte.com.mo

Becca Leong
Associate Director, Risk Advisory

Tel: +852 2258 6266
Email: beleong@deloitte.com.hk

MAKING AN IMPACT THAT MATTERS since 1845

Designed by CoRe Creative Services. RITM1655224