HONG KONG MONETARY AUTHORITY 香港金融管理局		
Supervisory Policy Manual		
SA-2	**Outsourcing**	V.1 – 28.12.01

This module should be read in conjunction with the Introduction and with the Glossary, which contains an explanation of abbreviations and other terms used in this Manual. If reading on-line, click on blue underlined headings to activate hyperlinks to the relevant module.

Purpose

To set out the HKMA's supervisory approach to outsourcing and the major points which the HKMA recommends AIs to address when outsourcing their activities

Classification

A non-statutory guideline issued by the MA as a guidance note

Previous guidelines superseded

Guideline No. 3.8 "Outsourcing of Data Processing Operations" dated 03.07.96; Circular "Outsourcing" dated 08.12.98

Application

To all AIs

Structure

---

1. Introduction

1.1 Background

1.1.1 The term "outsourcing" used in this module refers to an arrangement under which another party (i.e. the service provider) undertakes to provide to an AI a service previously carried out by the AI itself or a new service to be launched by the AI. Outsourcing can be to a service provider in Hong Kong or overseas and the service provider may be a unit of the same AI (e.g. head office or an overseas branch), an affiliated company of the AI's group or an independent third party.

1.1.2 With globalisation and technological advancement, outsourcing has become increasingly common both internationally and in Hong Kong. Typical functions outsourced by AIs in Hong Kong include data processing, customer-related services (e.g., call centres) and back office-related activities.

1.1.3 AIs choose to outsource their functions or activities for various reasons. These include:

- saving costs or exploiting economies of scale;
- allowing AIs to concentrate on their core business;
- making use of specialised expertise available to the service provider, e.g. the latest technology; or

- centralising such services at the head office or another branch to improve services and to improve controls and risk management.

1.2 Legal obligations under the Seventh Schedule

1.2.1 AIs should be aware of their legal obligations to meet the minimum authorization criteria stipulated under the Seventh Schedule to the Banking Ordinance in relation to their outsourcing plans.

1.2.2 Specifically, para. 10 of the Seventh Schedule requires AIs to have adequate accounting systems and systems of control and para. 12 requires them to conduct their business with integrity, competence and in a manner not detrimental to the interest of depositors and potential depositors. AIs should not enter into, or continue, any outsourcing arrangements if this may result in their internal control systems or business conduct being compromised or weakened after the activity has been outsourced.

1.3 Supervisory approach

1.3.1 As outsourcing can bring significant benefits to AIs and their customers, the HKMA will not stand in the way of AIs using outsourcing arrangements to achieve their business objectives, provided that such arrangements are well-structured and properly managed and the interests of customers will not be compromised.

1.3.2 As outsourcing arrangements differ from case to case, AIs which intend to begin outsourcing in respect of a banking-related business area (including back office activities) or to make changes to or amend the scope of their outsourcing of such areas should discuss their plans with the HKMA in advance and satisfy the HKMA that all the major issues set out in section 2 below are properly addressed before they implement the plans. If in doubt as to whether an activity would fall within the scope of discussion with the HKMA, AIs should seek advice from the HKMA.

1.3.3 For outsourcing to overseas jurisdictions, the HKMA may also communicate directly with the AI's home or host

regulators, as the case may be, to seek confirmation on various matters.

1.3.4 Once AIs implement an outsourcing plan, the HKMA expects them to continue to review the effectiveness and adequacy of their controls in monitoring the performance of the service provider and managing the risks associated with the outsourced activity.

1.3.5 Where there are deficiencies identified in any outsourcing arrangements, AIs should take appropriate action to rectify them, failing which the HKMA reserves the right, in extreme cases, to require the AI to take steps to make alternative arrangements for the outsourced activity.

1.3.6 The HKMA will, in the course of its on-site examinations, off-site reviews or prudential interviews with AIs, establish whether they have adequately addressed the concerns mentioned in section 2 below and rectified deficiencies.

2. Major supervisory concerns

2.1 Accountability

2.1.1 In any outsourcing arrangement, the Board of Directors and management of AIs should retain ultimate accountability for the outsourced activity. Outsourcing can only allow them to transfer their day-to-day managerial responsibility, but not accountability, for an activity or a function to a service provider. AIs should therefore continue to retain ultimate control of the outsourced activity.

2.2 Risk assessment

2.2.1 The Board of Directors and management of AIs should ensure that the proposed outsourcing arrangement has been subject to a comprehensive risk assessment (in respect of operational, legal and reputation risks) and that all the risks identified have been adequately addressed before launch. Specifically, the risk assessment should cover inter alia the following:

- the importance and criticality of the services to be outsourced;

- reasons for the outsourcing (e.g. cost and benefit analysis); and
- the impact on AIs' risk profile (in respect of operational, legal and reputation risks) of the outsourcing.

2.2.2 After AIs implement an outsourcing plan, they should regularly re-perform this assessment.

2.3 Ability of service providers

2.3.1 Before selecting a service provider AIs should perform appropriate due diligence. In assessing a provider, apart from the cost factor and quality of services AIs should take into account the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity, compatibility with the AI's corporate culture and future development strategies, familiarity with the banking industry and capacity to keep pace with innovation in the market.

2.3.2 AIs should have controls in place (e.g. comparison with target service level) to monitor the performance of service providers on a continuous basis.

2.4 Outsourcing agreement

2.4.1 The type and level of services to be provided and the contractual liabilities and obligations of the service provider should be clearly set out in a service agreement between AIs and their service provider.

2.4.2 AIs should regularly (e.g. annually) review their outsourcing agreements. They should assess whether the agreements should be renegotiated and renewed to bring them in line with current market standards and to cope with changes in their business strategies.

2.4.3 Where the service provider is a wholly-owned subsidiary of an AI or the head office or another branch of a foreign AI, a memorandum of understanding may be acceptable.

2.5 Customer data confidentiality

2.5.1 AIs should ensure that the proposed outsourcing arrangement complies with relevant statutory requirements (e.g. the Personal Data (Privacy) Ordinance - PDPO) and common law customer confidentiality[1]. This will generally involve seeking legal advice.

2.5.2 AIs should have controls in place to ensure that the requirements of customer data confidentiality are observed and proper safeguards are established to protect the integrity and confidentiality of customer information. Typical safeguards include, among other things:

- undertakings by the service provider that the company and its staff will abide by confidentiality rules, including taking account of the data protection principles set out in PDPO;
- AIs' contractual rights to take action against the service provider in the event of a breach of confidentiality;
- segregation or compartmentalisation of AIs' customer data from those of the service provider and its other clients; and
- access rights to AIs' data delegated to authorized employees of the service provider on a need basis.

2.5.3 AIs should notify their customers in general terms of the possibility that their data may be outsourced. They should also give specific notice to customers of significant outsourcing initiatives, particularly where the outsourcing is to an overseas jurisdiction.

2.5.4 In the event of a termination of outsourcing agreement, for whatever reason, AIs should ensure that all customer data is either retrieved from the service provider or destroyed.

2.6 Control over outsourced activities

[1] In addition to restrictions under the PDPO, AIs in Hong Kong are subject to a common law duty of confidentiality to their customers. No distinction is made between individual or corporate customers, while the PDPO only protects the data of individuals. The general principle under common law is that AIs should keep customer data confidential and not divulge such information to any person without the customer's consent.

2.6.1 In any outsourcing arrangement, AIs should ensure that they have effective procedures for monitoring the performance of, and managing the relationship with, the service provider and the risks associated with the outsourced activity.

2.6.2 Such monitoring should cover, inter alia:

- contract performance;
- material problems encountered by the service provider;
- regular review of the service provider's financial condition and risk profile; and
- the service provider's contingency plan, the results of testing thereof and the scope for improving it.

2.6.3 Responsibility for monitoring the service provider and the outsourced activity should be assigned to staff with appropriate expertise.

2.6.4 AIs should establish reporting procedures which can promptly escalate problems relating to the outsourced activity to the attention of the management of the AI and their service providers.

2.6.5 The control procedures over the outsourcing arrangement should be subject to regular reviews by the Internal Audit.

2.7 Contingency planning

2.7.1 Contingency plans should be maintained and regularly tested by AIs and their service providers to ensure business continuity, e.g. in the event of a breakdown in the systems of the service provider or telecommunication problems with the host country.

2.7.2 Contingency arrangements in respect of daily operational and systems problems would normally be covered in the service provider's own contingency plan. AIs should ensure that they have an adequate understanding of their service provider's contingency plan and consider the implications for their own contingency planning in the event that an

outsourced service is interrupted due to failure of the service provider's system.

2.7.3 In establishing a viable contingency plan, AIs should consider, among other things, the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, time and resources that would be involved.

2.8 Access to outsourced data

2.8.1 AIs should ensure that appropriate up-to-date records are maintained in their premises and kept available for inspection by the HKMA in accordance with §§55 and 56 of the Banking Ordinance and that data retrieved from the service providers are accurate and available in Hong Kong on a timely basis.

2.8.2 Access to data by the HKMA's examiners and the AI's internal and external auditors should not be impeded by the outsourcing. AIs should ensure that the outsourcing agreement with the service provider contains a clause which allows for supervisory inspection or review of the operations and controls of the service provider as they relate to the outsourced activity.

2.9 Additional concerns in relation to overseas outsourcing

2.9.1 In addition to the issues mentioned from subsections 2.1 to 2.8 above, there are further concerns that need to be addressed in relation to overseas outsourcing:

- implications of the overseas outsourcing for AIs' risk profile - AIs should understand the risks arising from overseas outsourcing, taking into account relevant aspects of an overseas country (e.g. legal system, regulatory regime, sophistication of technology, infrastructure);
- right of access to customers' data by overseas authorities such as the police and tax authorities - AIs should generally obtain a legal opinion from an international or other reputable legal firm in the relevant jurisdiction on this matter. This will enable

them to be informed of the extent and the authorities to which they are legally bound to provide information. Right of access by such parties may be unavoidable due to compulsion of law. AIs should therefore conduct a risk assessment to evaluate the extent and possibility of such access taking place. AIs should notify the HKMA if overseas authorities seek access to their customers' data. If such access seems unwarranted the HKMA reserves the right to require the AI to take steps to make alternative arrangements for the outsourced activity;

- notification to customers - AIs should generally notify their customers of the country in which the service provider is located (and of any subsequent changes) and the right of access, if any, available to the overseas authorities;
- right of access to customers' data for examination by the HKMA after outsourcing - AIs should not outsource to a jurisdiction which is inadequately regulated or which has secrecy laws that may hamper access to data by the HKMA or AIs' external auditors. They should ensure that the HKMA has right of access to data. Such right of access should be confirmed in writing by both AIs and their home or host authorities, as the case may be;
- §33 of the PDPO in respect of transfer of personal data outside Hong Kong – although §33 has not yet come into operation, AIs are advised to take account of the provisions therein and the potential impact on their plans in respect of overseas outsourcing; and
- governing law of the outsourcing agreement - the agreement should preferably be governed by Hong Kong law.

2.9.2 In case of a locally incorporated AI, a principal concern is the ability of the HKMA to exercise its legal powers under the Banking Ordinance effectively if there is limited cooperation by the service provider. Accordingly, where a local AI is planning to outsource, for example, a major part

of its data processing function to outside Hong Kong, the HKMA will expect the AI to have a robust back-up system and contingency plan in an acceptable jurisdiction. The back-up system should be properly documented and regularly tested (see also subsection 2.7 above). It may be appropriate for an independent opinion on its effectiveness to be sought.

Contents	Glossary	Home	Introduction