



HONG KONG MONETARY AUTHORITY
香港金融管理局

Circulars

07 Oct 1998

Year 2000 Counterparty Assessment

All authorized institutions

7 October 1998

Year 2000 Counterparty Assessment

I am writing to require your institution, if it has not already done so, to develop and implement policy and procedures to assess and manage Year 2000 risks posed by counterparties.

An authorized institution ("AI") is subject to increased risks (e.g. credit risk, liquidity risk and counterparty trading risk) when its counterparties encounter Year 2000 problems. These problems may result from a counterparty's own failure to achieve Year 2000 compliance, or from problems that are not addressed by its service providers, clients or other external dependencies.

The Hong Kong Monetary Authority ("HKMA") expects all AIs to develop and implement a counterparty assessment framework to identify, assess and establish controls in relation to Year 2000 risks posed by counterparties. Your institution should aim to substantially complete the counterparty assessment process before 31 March 1999. This should also include establishing the overall potential impact of Year 2000 counterparty risks on your institution, and controls to be implemented to manage and mitigate these risks. Your institution should also incorporate counterparty risk assessment into the normal due diligence process on new counterparties as soon as possible.

It should be stressed that it is your responsibility to identify and manage any counterparty risks, whether or not Year 2000 related, in an effective manner. In fact, I am aware that many of you have put in place counterparty assessment policy and procedures. To assist those who have not yet done so, the attached [Guidance Note](#) sets out some suggestions. However, it should be noted that the guidance provided is neither exhaustive nor universally applicable. Each institution must tailor its risk management process having regard to factors such as its size, appetite for risk-taking, reliance of counterparties on IT systems and the level of its own Year 2000 risk exposure.

The process of developing and implementing a counterparty assessment framework is likely to take several months to complete. Hence, you are advised to give early attention to the matter and to draw up a realistic processing time-frame, having considered factors such as your institution's scale of operations, resource availability and the complexity of the assessment. You should also ensure that yourself and other members of the senior management are in a position to review and approve the counterparty assessment

framework before its implementation, and to monitor the progress and results of assessment on a regular basis.

Should you have any queries on the above, please contact Mr Vincent Lee at 2878-1384.

Guidance Note on Year 2000 Counterparty Assessment by Authorized Institutions

Introduction

1. The Hong Kong Monetary Authority ("HKMA") requires all authorized institutions ("AIs") to develop and implement a framework to identify, assess and establish controls in relation to Year 2000 risks posed by counterparties. It must be stressed that counterparty risks, whether or not caused by the Year 2000 problem, are part of institutions' business risks. It is the responsibility of the management of each institution to manage such risks in an effective manner. The purpose of this Guidance Note is to assist AIs in developing risk controls in this area. However, the guidance is neither exhaustive nor universally applicable. Each institution is expected to develop its own assessment framework having considered factors such as its size, appetite for risk-taking, reliance of counterparties on IT systems, and the level of its own Year 2000 risk exposure.

Background

2. The Year 2000 problem poses many challenges to risk control and management by AIs. Institutions can be subject to increased credit risk, liquidity risk and counterparty trading risk arising from their counterparties due to business disruption, losses and/or failure to fulfill obligations on their part. These problems may result from a counterparty's failure to achieve Year 2000 compliance, and from problems that are not addressed by its service providers, clients or other external dependencies. In this context, counterparties can be classified into three broad categories: fund takers, fund providers and capital market/asset management counterparties:

- **Fund takers** - including borrowers and debt issuers. AIs may face increased credit risk when their fund takers encounter Year 2000 problems resulting in their inability to meet payment obligations.
- **Fund providers** - AIs may be subject to liquidity risk when a fund provider is unable to provide funding or needs to withdraw funding because of Year 2000 problems.
- **Capital market/asset management counterparties** - trading and treasury operations will be affected when a capital market/asset management counterparty is unable to settle a transaction due to Year 2000 problems. Moreover, an AI can be prevented from fulfilling its fiduciary responsibilities to protect and manage assets for fiduciary beneficiaries when its counterparty encounters Year 2000 problems.

Development & Implementation of a Counterparty Assessment Framework

3. The process of developing and implementing a counterparty assessment framework is likely to take several months to complete. Hence, it is important for AIs to give early attention to the matter if they have not already done so, and to draw up a realistic

processing time-frame, having considered factors such as their scale of operations, resource availability and complexity of the assessment. Moreover, the senior management of AIs should be in a position to review and approve the counterparty assessment framework before its implementation and to monitor the progress and results of assessment on a regular basis.

4. A counterparty assessment framework should include measures to identify, assess and establish controls to manage or mitigate Year 2000 risks posed by counterparties. In the development of an assessment framework the following should be considered:

(a) Identify material counterparties

The assessment framework should help identify counterparties that pose material risk exposure to the AI. It is for the AI to judge what constitutes material risk exposure to the institution which may depend on any one or more of the following factors:

- i. size of the overall relationship;
- ii. potential losses if the counterparty fails or its business is disrupted;
- iii. reliance of the counterparty on IT systems and their complexity; and
- iv. dependence of the counterparty on external service providers and IT support.

Institutions should note that while the risks posed by an individual counterparty may not be material, the risks posed by a group of counterparties may be if they have common dependencies, e.g. a sizable agent to which a large group of counterparties might have outsourced their computer operations. In such cases, the assessment should be carried out on the dependencies concerned, instead of the counterparties themselves. Another example where assessment may have to go beyond institutions' counterparties is the potential exposure due to diminution in the value of the collateral, e.g. where shares of a Year 2000 non-compliant company are being used as collateral. In material cases, an assessment should be carried out on the company concerned.

(b) Assess Year 2000 efforts of material counterparties

The next step is for AIs to assess whether a material counterparty has the necessary commitment and resources to achieve Year 2000 compliance. Needless to say, staff should be trained to assess Year 2000 efforts of material counterparties. If institutions consider that outside assistance is necessary, many reputable firms have training courses available for this purpose. To ensure that the information received is consistent and provides a basis for comparison, it would be useful for AIs to develop standard sets of assessment form to assess the Year 2000 efforts of material counterparties. Some counterparties may be reluctant to disclose their Year 2000 compliance efforts. AIs should ensure that these cases are followed up. If the responses are insufficient after repeated requests, the risk assessment should reflect this. (It is worth noting that in certain cases, a face-to-face interview can be more effective in getting responses than by sending around standard questionnaire). Institutions should document any findings from the assessment, follow-up actions and status updates on material counterparties.

(c) Evaluate Year 2000 risks on the institution

After the assessment, the Year 2000 risks posed by material counterparties should be evaluated both on an individual and aggregate basis. Institutions may find it useful to adopt a risk rating system. A simple system, e.g. low, medium and high risks, may be sufficient. The management should determine follow-up actions in respect of each category of risk rating. The rating should also be factored into the overall credit assessment of the counterparty. Compliance progress of counterparties should be monitored on a regular basis. Those with a higher risk rating or higher potential impact should be monitored more frequently e.g. on a bi-monthly basis. The risk exposure of the Al's cash flows, balance sheet, etc. should be evaluated and reported to the senior management on a regular basis.

(d) Develop appropriate risk controls

Following the evaluation of Year 2000 risks posed by counterparties, Als should consider appropriate measures to manage and mitigate these risks. Different risk management controls may be needed to address unique and material Year 2000 issues that may arise from different categories of counterparties. However, in general, the following considerations should be given:

- i. For those counterparties having a higher risk rating, consideration should be given to reducing risk exposure such as establishing netting arrangements, seeking third-party guarantees, controlling credit maturities, obtaining additional collateral or even early termination of agreements;
- ii. Provision for loan loss and contingency planning should take into account Year 2000 counterparty risks;
- iii. Als should maintain close contact with material counterparties to ensure that they receive up-to-date information with respect to their Year 2000 efforts;
- iv. Als should establish proper loan documentation policy to provide an effective means to monitor and manage Year 2000 risk posed by customers e.g. incorporating into loan agreements provisions requiring borrowers to disclose Year 2000 plans and provide periodic updates on Year 2000 progress; and
- v. Als should avoid taking unnecessary risks, e.g. institutions may wish to reduce potential liquidity risks by extending maturity of funding obtained sufficiently past 3 January 2000, the first business day in the year 2000, and 29 February 2000. This will reduce the liquidity requirement on the critical dates and provide time to assess and evaluate the effect of the Year 2000 on the relevant fund providers. Also, Als should consider avoiding transactions with settlement risk on 3 January 2000 and 29 February 2000. They may wish to advise their customers to do the same so as to minimize the risks to which the latter are exposed.

Further Reference

5. [The Annex](#) provides a sample of assessment forms which some institutions use to evaluate customer Year 2000 preparedness and their Year 2000 risks to the institution. Als are not required to use these forms, although they provide useful reference of methods to evaluate customer preparedness.

6. Further information on counterparty risks assessment can be obtained from inter alia the website of the US Federal Financial Institutions Examination Council at <http://www.ffiec.gov> and the Federal Deposit Insurance Corporation at <http://www.fdic.gov>.

Hong Kong Monetary Authority
7 October 1998

Last revision date : 01 August 2011