Annex A-1

Guidance Note on Independent Assessment of Year 2000 Preparations of a Hong Kong Incorporated Authorised Institution

Introduction

This guidance note aims to provide some practical guidance to a Reviewer for conducting an independent assessment of the Year 2000 preparations of a Hong Kong incorporated authorized institution ("AI").

The main objective of the Reviewer is to assess whether the local management of the institution has taken or is taking the necessary measures to resolve the Year 2000 problem of the systems, particularly the critical systems, that would be used spanning the period prior to, during and after the Year 2000 by the institution and its local and overseas subsidiaries and branches. If the institution is part of a larger banking group, the Reviewer should take into account the extent to which its Year 2000 project is being directed by the parent bank in assessing the efforts of the local management. Where it is the case, the Reviewer should check, through discussion with the local management, whether the necessary steps are being taken by the parent bank to resolve the Year 2000 problem in respect of the Hong Kong incorporated institution and its subsidiaries and branches.

This guidance note contains eight sections, each of which provides a general description of the sound practices related to the various important aspects of the Year 2000 compliance work. It also includes a list of suggested questions which the Reviewer may ask pertaining to each important aspect of the Year 2000 compliance work. It should be noted that the questions suggested are not meant to be exhaustive. The Reviewer can ask additional questions and where appropriate obtain documentary evidence from the institution to ascertain the claims and responses made by the institution. For this particular purpose, the guidance note has also included suggested

documentary evidence that the Reviewer can ask for review of the matters under each section.

Section I - Establishing Strategic Objective And Management Oversight

Objective of assessment:

The Reviewer should assess and report on whether the senior management of the institution has been giving sufficient priority to, and maintaining adequate oversight of, the Year 2000 problem of the institution and its subsidiaries and branches.

General description of sound practices:

The institution should establish the resolution of the Year 2000 problem as a strategic objective of the institution including all its subsidiaries and branches. The Year 2000 problem should be taken into account when considering other strategic business initiatives (e.g., mergers, acquisitions, major system development, corporate alliances, or business expansions).

Regarding the management oversight of the Year 2000 problem, there should be a clear assignment of lines of responsibility and accountability. In particular, a senior executive should be assigned with explicit oversight responsibility and accountability for the overall Year 2000 preparation efforts of the institution and its subsidiaries and branches. The institution should also establish its Year 2000 project team (comprising the appropriate officers from various departments) to co-ordinate the Year 2000 readiness work of the institution as a whole including its subsidiaries and branches. It would also be useful to set up a Year 2000 project steering committee involving senior executives from relevant departments to provide steers to the Year 2000 project team. In addition, the institution's board of directors and senior management should be kept informed through regular reports on the status of Year 2000 preparations of the institution and its subsidiaries and branches.

There should also be explicit and proactive involvement of the internal audit, or possibly external audit, in monitoring the Year 2000 progress of the institution and its subsidiaries and branches. Exceptions identified should be followed-up promptly.

Suggested questions that the Reviewer may ask:

1. Have the senior management and board of directors clearly established the resolution of the Year 2000 issue as a strategic objective?
2. Has the institution taken Year 2000 into account when considering other strategic business initiatives (e.g., mergers, acquisitions, major system development, corporate alliances, or business expansions)? What due diligence and other measures would be taken in merger and acquisition transactions to protect against inheriting Year 2000 problems?
3. Has the institution clearly assigned the responsibilities for dealing with various aspects (technical, operational, business line) of the Year 2000 preparations?
4. Has a senior executive been assigned with explicit oversight responsibility and accountability for the overall Year 2000 preparation efforts of the institution and its subsidiaries and branches?
5. Has the institution established its Year 2000 project team (including the appropriate officers from various departments) to co-ordinate the preparations of the institution as a whole and its subsidiaries and branches?
6. Has a Year 2000 project steering committee been set up involving senior executives from relevant departments to provide policy steers to the Year 2000 project team?
7. Have the institution's board of directors and senior management been receiving regular reports, at least on a monthly basis, on the status of Year 2000 preparations of the institution and its subsidiaries and branches?
8. Has there been explicit and proactive involvement of the internal audit, or external audit, in regular monitoring of the Year 2000 progress of the institution and its subsidiaries and branches?
9. Does internal and/or external audit communicate the exceptions identified and findings to the senior management and even board of directors? Has the institution in general made timely follow-up actions in response to the findings?

Suggested documentary evidence that the Reviewer can ask for review:

- Relevant board minutes and memos from senior management, minutes of Year 2000 project steering committee and project team, copies of management status reports on Year 2000 project of the institution;
- Correspondence with subsidiaries/branches/head office (if any); and
- Sample of audit plan of internal auditors, or external auditors, and findings and follow-up actions of the institution.

Section II - Organisational Awareness

Objective of assessment:

The Reviewer should assess and report on whether the institution has taken the necessary measures to promote the awareness of the Year 2000 problem within the institution including its subsidiaries and branches.

General description of sound practices:

The board of directors and senior management should have a clear understanding of the Year 2000 problem that it is a business survival issue and not just a technical issue. Directors and senior management should understand their fiduciary duties to ensure necessary measures would be taken to prepare for the Year 2000 problem. Senior management should communicate to the staff (including line management, technical staff, end users of systems, credit officers) of the institution and its subsidiaries and branches about the strategic implications of the Year 2000 problem, particularly the strategic objective to resolve the Year 2000 problem.

The staff (including line management, technical staff, end users of systems, credit officers) of the institution and its subsidiaries and branches must also realise how the millennium change may affect their activities. They should also understand that their activities depend on numerous other parties (for example, customers, correspondents, and service providers) that must also be ready for the millennium change.

The institution and its subsidiaries and branches must be aware of the various supervisory requirements for Year 2000 preparedness established in each of the jurisdictions in which they operate.

Suggested questions that the Reviewer may ask:

1. Do the board of directors and senior management have a clear understanding of the Year 2000 problem, that it is a business survival issue and not just a technical issue?
2. Do the directors and senior management understand their fiduciary duties to ensure necessary measures would be taken to prepare for the Year 2000 problem?
3. Has the senior management communicated to the staff (including line management, technical staff, end users of systems, credit officers) of the institution and its subsidiaries and branches about the strategic implications of the Year 2000 problem, particularly the strategic objective to resolve the Year 2000 problem?
4. Do the staff (including line management, technical staff, end users of systems, credit officers) of the institution and its subsidiaries and branches realise how the millennium change may affect the their activities? Do they understand that their activities would depend on numerous other parties (for example, customers, correspondents, and service providers) that must also be ready for the millennium change?
5. Are the institution and its subsidiaries and branches aware of relevant supervisory benchmarks, target dates, and other sound practices identified for Year 2000 compliance in each jurisdiction in which they operate? Do they understand the regulatory consequences of failures in preparing for the Year 2000 issues? If certain systems would be provided by the parent bank (if any), has the institution informed its parent bank about the local regulatory requirements so that the parent bank will take into account such requirements in modifying and testing the systems?

Suggested documentary evidence that the Reviewer can ask for review:

- Sample of internal awareness programme, training materials, circulars/ correspondents; and
- Correspondence with customers.

Section III - Assessment and detailed planning

Objective of assessment:

The Reviewer should assess and report on whether the institution has taken the necessary measures to assess the impact of the Year 2000 problem on the institution and its subsidiaries and branches, to formulate a sound and effective project plan to address the Year 2000 problem and to ensure that sufficient budget and resources have been allocated to the project.

General description of sound practices:

The institution must determine the size and complexity of the Year 2000 problem by developing detailed inventory of the systems that it would use, regardless of whether the systems are in-house developed or provided by the parent bank (if any), vendors or service providers (e.g., exchanges, clearing houses). The inventory should include centralised or decentralised computer hardware, software, networks, or equipment with embedded computer chips, and system interfaces. Equipment with embedded computer chips include security systems, vaults, telephones, faxes, heating/cooling systems, entrance systems, fire alarm, safe deposit box systems, network equipment, building services, escalators, elevators, air-conditioning systems, audio response systems, tape recording systems and dealing systems. The detailed inventory should identify which systems would be affected if the Year 2000 problem of the systems was not resolved and the risk analysis. Priority should be set on each system according to the risks assessed.

The institution should contact those vendors and service providers as to their progress and plans for addressing the year 2000 issue. The development of effective communication channels with vendors and service providers is essential. Contracts may need to be reviewed and amended, as appropriate. Current and future purchases of hardware/software technology should require certification that it is Year 2000 compliant. If contract changes or modifications are

refused, then the institution should consider replacing the service or product.

The institution should develop a detailed project plan to detail what and how much efforts are necessary to address the Year 2000 problem of the institution and its subsidiaries and branches. The project plan should include breakdown of the project into manageable tasks with a concrete timetable for meeting each milestone. It should also establish trigger dates for making decisions on adopting alternatives should there be slippage on major dependencies on external factors.

The project plan should outline which systems will be modified and what the testing and implementation process will entail. It should recognise that testing will be the single most important resource intensive part of the project. The resource needs should be identified and secured, including appropriately skilled personnel, contractors, vendor support, budget allocations, and hardware capacity. Responsibilities and accountabilities need to be clearly defined and agreed upon for each step in the project plan.

Procedures for monitoring the progress against schedules and the utilised resources against budget should be devised with appropriate information flowing to the senior management and board of directors on a regular basis.

Suggested questions that the Reviewer may ask:

1. Has the institution determined the size and complexity of the Year 2000 problem by developing detailed inventory of the systems that it would use, regardless of whether the systems are in-house developed or provided by the parent bank (if any), vendors or service providers (e.g., exchanges, clearing houses)?
2. Does the inventory include centralised or decentralised computer hardware, software, networks, and system interfaces? Does the inventory include equipment with embedded computer chips such as security systems, vaults, telephones, faxes, heating/cooling systems, entrance systems, fire alarm, safe deposit box systems, network equipment, building services, escalators, elevators, air-conditioning

systems, audio response systems, tape recording systems and dealing systems?

3. Does the detailed inventory identify which systems would be affected if the Year 2000 problem of the systems was not resolved and the risk analysis? Has priority been placed on each system according to the risks assessed?
4. Has the institution contacted those vendors and service providers as to their progress and plans for addressing the year 2000 issue? Have effective communication channels with vendors and service providers been developed?
5. Have contracts and insurance policies been reviewed and amended, as appropriate? Do current and future purchases of hardware/software technology require certification that it is Year 2000 compliant? If contract changes or modifications are refused, would the institution and its subsidiaries and branches consider replacing the service or product?
6. Has the institution developed a detailed project plan to detail what and how much efforts are necessary to address the Year 2000 problem of the institution and its subsidiaries and branches? Does the project plan include breakdown of the project into manageable tasks with a concrete timetable for meeting each milestone? Have responsibilities and accountabilities been clearly defined and agreed upon for each step in the project plan? Does the project plan establish trigger dates for making decisions on adopting alternatives for major dependencies on external factors (e.g., delivery of Year 2000 compliant systems by vendors or service providers)?
7. Does the project plan outline which systems should be replaced, upgraded or otherwise modified and what the modification, testing and implementation process will entail? Does the project plan recognise that testing will be the single most important resource intensive part of the project (around 50 to 60% of the total time, funding, and personnel needed)?
8. Have the resource needs been identified and secured, including appropriately skilled personnel, contractors, vendor support, budget allocations, and hardware capacity? Has a reasonable basis been adopted to estimate these resource requirements? Have factors such as potential increasing wages and staffs turnover of information technology staff been taken into account in formulating the project plan and resource requirements?
9. Has the institution established strong monitoring of progress throughout the process to address the Year 2000 problem? Has a system been established for tracking utilised resources (expenses, internal and external personnel, and technological equipment)?

10. Have there been any significant changes to established target dates? Do such changes materially affect the ability of the institution and its subsidiaries and branches to be ready in a timely manner?
11. Have there been any missed milestones? If so, what were the reasons for the missed milestones and the effect on the overall plan?

Suggested documentary evidence that the Reviewer can ask for review:

- Detailed inventory of systems of the institution and its subsidiaries and branches, with risk analysis and priorities assigned;
- Year 2000 detailed project plan for the institution and its subsidiaries and branches;
- Resource requirements (including appropriately skilled personnel, contractors, vendor support, budget allocations, and hardware capacity) for the Year 2000 project;
- Procedures for monitoring the progress against schedules and the utilised resources against budget; and
- Sign off procedures for key milestones.

Section IV - Modification

Objective of assessment:

The Reviewer should assess and report on whether the institution has taken the necessary measures to ensure the systems that would be used by the institution and its subsidiaries and branches, especially critical systems, have been or would be properly modified.

General description of sound practices:

The additional resources needed for the project (e.g., additional hardware equipment/capacity for modification and testing) should be acquired or contracted. Systems needing fixing should be modified, upgraded, replaced, outsourced or discontinued. For those systems that would not be modified, upgraded, replaced, outsourced or discontinued, procedures should be developed to handle the Year 2000 problem for such systems. Execution should be done systematically with priorities set in accordance with risk and critical systems should be modified first.

A clear understanding of what the vendor or service provider means by being year 2000 compliant should be obtained. While a warranty or certification may be sought or offered, the institution must recognise the need for rigorous testing is not obviated by such a warranty or certification.

There should be adequate controls over the modification (including upgrade, replacement, outsourcing or discard) of systems. If third-party contractors perform certain modification work, the institution should maintain close monitoring of the quality and progress of the work of the contractors.

Suggested questions that the Reviewer may ask:

1. Have additional resources needed for the project been acquired or contracted?
2. Has the institution communicated date format changes with external entities with which they exchange data?
3. Have procedures been developed to handle the Year 2000 problem for those systems that cannot be modified, upgraded, replaced, outsourced or discontinued?
4. Are modifications being done systematically with priorities set in accordance with risk? Are critical systems being modified first?
5. Have clear understandings of what the vendor or service provider means by being year 2000 compliant been obtained? Does the institution recognise that the need for rigorous testing is not obviated by a warranty or certification?
6. Are there adequate controls over the modification (including upgrade, replacement, outsourcing or discard) of systems? In particular, are there change control procedures in place to ensure modifications to systems are properly documented and managed? If vendor technicians and outside consultants are engaged, would they be subject to similar controls?
7. If third-party contractors perform certain modification work, has the institution maintained close monitoring of the quality and progress of the work of the contractors? Are there formal engagement letters with the third-party contractors?
8. What are the natures of problems or issues that have arisen during the course of modifications (for example, resource shortages, backlogs, bottlenecks, and failures)? How have these issues been addressed?

Suggested documentary evidence that the Reviewer can ask for review:

- Sample of correspondence with vendors and service providers;
- Engagement letters with third-party contractors;
- Control procedures related to modification work performed by third-party contractors, if applicable; and
- Progress report related to the modifications of systems.

Section V - Testing

Objective of assessment:

The Reviewer should assess and report on whether the institution has taken the necessary measures to ensure the systems that would be used by the institution and its subsidiaries and branches, especially critical systems, have been or would be properly tested for Year 2000 readiness.

General description of sound practices:

Systems should be tested according to priorities. In addition to testing of individual modified systems including upgraded components, the interaction of such systems with the institution's other systems with which they interface directly should also be tested. The institution should also conduct external testing with external entities with whom it exchanges data electronically. As far as possible, "end-to-end" testing should be conducted to verify the ability of the institution to originate a transaction to transmit test data to a receiving entity or system through an intermediary (e.g., financial systems provided by exchanges or clearing houses).

If certain user groups test certain systems provided by vendors or service providers, the institution should evaluate the applicability of the user group test results to it before relying on the user groups' testing. Measures should be taken to manage the residual risks if the test results of the user groups cannot be fully applicable to the institution. For those systems that will not be tested, the institution

should have evaluated and determined that the relevant vendors and service providers have successfully tested their systems. For those systems that will not be modified, the procedures developed to handle the Year 2000 problem of such systems should be tested.

Written test plans should be developed to describe how the testing will be conducted. In general, test plans should include, at minimum, the following elements: a description of testing environment, testing methodology (e.g., test scripts, development of test data), testing schedules, testing of relevant critical dates, documentation of test results, the allocation of human and financial resources and requirements for user participation.

End users of the systems should be involved in defining what should be tested and the expected results, validating the actual testing results against the expected results and signing off the systems. Appropriate training on how the testing would be conducted should be provided to personnel participating in the testing.

Proper control procedures should be established over the testing process. In particular, there should be "clean management" procedures to prevent contamination or corruption of operational systems and related databases during and after testing process. Moreover, the status of any problems identified during testing should be tracked closely to ensure such problems will be fixed and re-tested accordingly. If third-party consultants are engaged to conduct the testing, they should be subject to similar controls. Moreover, their quality of work and progress should be carefully monitored.

Suggested questions that the Reviewer may ask:

1. Is testing for systems conducted according to priorities?
2. Does the testing include the validation of the interaction of modified systems with the institution's other systems with which they interface directly?
3. Does the institution have plans to conduct external testing with external entities (e.g., exchanges, clearing houses) with whom it exchanges data electronically? Does it have plans to conduct "end-

to-end" testing with service providers (e.g., financial systems provided by exchanges or clearing houses) as far as possible?
4. Would the applicability of the user groups' test results be evaluated before such results are relied upon? Would there be measures to manage the residual risks if the test results of the user groups cannot be fully applicable to the institution?
5. For those systems that would not be tested, how would the institution evaluate and determine that the relevant vendors and service providers have successfully tested their systems? For those systems that would not be modified, have the procedures developed to handle the Year 2000 problem of such systems been tested?
6. Have written test plans been developed to describe how the testing would be conducted? Do the test plans include, at minimum, the following elements: a description of testing environment, testing methodology (e.g., test scripts, development of test data), testing schedules, testing of relevant critical dates, documentation of test results, the allocation of human and financial resources and requirements for user participation?
7. Would the following critical dates, and the rollover or progression before and after these dates, be generally tested? If automated tools would be used to simulate these dates, has the adequacy of the testing of the operating system been assessed?

Date	**Reason**
April 9, 1999	9999 on the Julian Calendar. The 99th day of the year 1999. 9999 denotes the "end of input" in many computer programs.
September 9, 1999	9999 on the Gregorian Calendar. 9999 denotes the "end of input" in many computer programs.
December 31, 1999	Last day in 1999 year.
January 1, 2000	Beginning of the Year 2000.
January 3, 2000	First business day in the Year 2000.
January 10, 2000	First date to require a 7-digit date field (1/10/2000).

January 31, 2000	End of the first month of the year 2000.
February 29, 2000	Leap year day.
March 31, 2000	End of first quarter of 2000.
October 10, 2000	First date to require an 8-digit date field (10/10/2000).
December 31, 2000	End of Year 2000.
January 1, 2001	Beginning of the Year 2001.
December 31, 2001	Check that year has 365 days.

8. Have end users of the systems been involved in defining what should be tested and the expected results, validating the actual testing results against the expected results and signing off the systems? Has appropriate training on how the testing would be conducted been provided to personnel participating in the testing?

9. Have proper control procedures been established over the testing process? In particular, are there "clean management" procedures to prevent contamination or corruption of operational systems and related databases during and after testing process? Are there procedures in place to closely track status of any problems identified during testing to ensure all problems identified during testing would be fixed and re-tested accordingly? If third-party consultants are engaged to conduct the testing, would they be subject to similar controls? Moreover, would their quality of work and progress be carefully monitored?

10. What are the natures of problems or issues that have arisen during the course of testing (for example, resource shortages, backlogs, bottlenecks, and failures)? How have these issues been addressed?

Suggested documentary evidence that the Reviewer can ask for review:

- Control policies and procedures over the Year 2000 testing process;
- Sample of Year 2000 test plan for critical systems, including internal integration testing and external testing (if applicable);
- Sample of documentation of Year 2000 test results and user sign-off for critical systems, in particular internal integration testing and external testing (if applicable); and
- Progress report related to testing.

Section VI - Implementing Tested, Compliant Systems

Objective of assessment:

The Reviewer should assess and report on whether the institution has taken the necessary measures to ensure the systems that would be used by the institution and its subsidiaries and branches, especially critical systems, have been or would be properly implemented in production.

General description of sound practices:

Putting tested, compliant systems into production (including data conversion) well before the end of 1999 should be an objective for the institution because it allows counterparties and customers to interact with the systems during normal day-to-day activities. Additionally, once back in production, normal maintenance of the application using standard change-control procedures becomes possible.

In some instances, the institution may choose to implement modified systems after rigorous testing of functionality but before completing Year 2000 testing, especially external testing. While this approach has the advantage of minimising the length of time a particular application is "frozen" from normal maintenance and change-control

procedures, it does not lessen the need for thorough Year 2000 testing.

Appropriate re-testing of systems in production should be addressed when other Year 2000 applications are introduced. Frequently, compliant systems become non-compliant because file formats or other components change in another application with which there is interaction.

Procedure manuals should be written or rewritten and disseminated. Training programs should be provided, and help desks established or retrained.

Suggested questions that the Reviewer may ask:

1. Are tested systems put into production (including data conversion) as soon as practical to allow counterparties and customers to identify and resolve any difficulties they may have in interacting with the application?
2. Does the institution have sound procedures in place to control version changes in applications? Are these procedures followed rigorously with respect to Year 2000 implementation?
3. After a tested application has been put into production, are there adequate plans in place to re-test the application when other applications with which it interacts are changed?
4. Has the institution implemented revised operation procedures for the new or corrected applications and tested them?
5. Has the institution trained all users and operators for the new or corrected applications, as well as latest releases of third-party software?
6. Has the institution established help desks to provide support to users on using the implemented systems?

Suggested documentary evidence that the Reviewer can ask for review:

- Implementation schedule of all modified systems;
- Sample of implementation (including data conversion) plans of critical systems;
- Sample of documentation of implementation (including data conversion) results;

- Operating procedures manuals;
- Training plan and material; and
- Progress report related to implementation.

Section VII - Contingency Planning

Objective of assessment:

The Reviewer should assess and report on whether the institution has taken the necessary measures to ensure contingency plans have been or would be properly developed and tested to ensure business continuity of the institution and its subsidiaries and branches and to deal with other Year 2000 problems that may arise.

General description of sound practices:

The need to develop contingency plans to assure business continuity is an integral part of the Year 2000 project. Some elements of contingency plans, such as the identification of alternatives for external dependencies and specific dates for making decisions on whether to change vendors, should be done as part of the assessment phase as inventories are developed.

Other elements such as specific plans for business resumption can be done more effectively when the likelihood of particular events occurring is better understood. Because this understanding is developed most effectively as testing begins, especially external testing, efficient use of resources suggests that contingency planning in this area will be a priority during the testing process. In particular, it might be necessary to develop contingency plans to ensure that customers' assets are protected and that their instructions can be effected after the 1 January 2000.

Some contingency plans can be developed only in cooperation with counterparties, customers, and the public sector. In particular, areas of systemic concern need to have coordinated planning efforts

because developing sound approaches will require knowing what approaches others are using.

Finally, the institution should also develop contingency plans related to its general functioning. This would include, *inter alia*, anticipating expected losses caused by the Year 2000, planning for counterparties being unable to perform, anticipating above average use of credit lines or cash withdrawals, and planning limitations on business activities that are highly dependent on technology (for example, trading activities).

Suggested questions that the Reviewer may ask:

1. Does the institution have contingency plans to deal with slippage in the Year 2000 modification, testing or implementation phases, and with a situation where the delivery date of any critical system cannot be met or, if the modified systems do not perform as planned?
2. Does the institution have a contingency planning process in place to ensure that operations can continue if some systems do not function properly as of 1 January 2000? Does this process take into account both the risks associated with a particular activity and the likelihood of particular events occurring?
3. Does the institution have estimates of how long they can operate under various contingency plans?
4. Are there any significant critical systems that will not meet the deadline for Year 2000 compliance? Is senior management addressing these problems?
5. Do the contingency plans deal with equipment with embedded chips (e.g., security systems, vault, fire systems) and infrastructure issues (e.g., telecommunications, electrical power and water)?
6. Do the contingency plans identify adequate levels of responsibility and readily available resources (internal and external) to deal with any problems encountered with the millennium date change? Has the institution prepared disaster recovery teams to deal with multiple system failures and tested the use of manual record keeping?
7. Has the institution considered the impact on customers of various contingencies and how negative consequences can be mitigated? Are mechanisms in place for a fair and expeditious resolution of disputes with customers that may arise?
8. Has the institution developed contingency plans related to its general functioning? Do the contingency plans deal with potential liquidity, market, credit, and legal risk issues? Has the institution planned for

higher than normal cash withdrawals by customers ahead of 31 December 1999?

9. Have the contingency plans and their revisions been tested? Are the contingency plans being updated with issues / problems encountered?

Suggested documentary evidence that the Reviewer can ask for review:

- Contingency plans; and
- Progress report related to development and testing of contingency plans.

Section VIII - assessing and managing Counterparty risks

Objective of assessment:

The Reviewer should assess and report on whether the institution has taken the necessary measures to ensure the Year 2000 issue-related risks arising from the business counterparties of the institution and its subsidiaries and branches have been or would be properly assessed and managed.

General description of sound practices:

Because business counterparties (e.g., correspondents and customers) are also subject to the Year 2000 issue, they too must make the necessary changes to conduct business normally. Testing normal connectivity and message transfers with business counterparties is essential but not enough. If they have not also made the necessary adjustments to their own systems, they could pose credit and liquidity risks to the bank.

The institution and its subsidiaries and branches should develop a due diligence process to assess and manage their Year 2000 issue-related risks arising from business counterparties. Credit officers need to understand the Year 2000 risks faced by their business counterparties and how well their business counterparties are managing these risks. Current financial performance will not be an

indication of future performance for organisations that have not developed sound plans and provided for appropriate resources to carry them out.

Suggested questions that the Reviewer may ask:

1. Is there any arrangement to assess the Year 2000 preparedness of business counterparties? Has the institution discussed the Year 2000 problem with its major customers and business counterparties and assessed whether they will be able to meet their financial and informational obligations to the institution?
2. Has Year 2000 readiness been incorporated into the list of criteria for assessing the suitability of customers and business counterparties? Has Year 2000 preparedness been incorporated as one of the standing items in their credit proposal and ongoing credit monitoring process for their customers?
3. Has the institution amended policies and business procedures (such as credit, mergers/acquisitions, and investment banking) to incorporate consideration of Year 2000 risk in dealing with business counterparties?

Suggested documentary evidence that the Reviewer can ask for review:

- Revised policies and procedures for assessing and managing Year 2000 issue-related risks arising from business counterparties.

Section IX - overall assessment

The Reviewer should also assess and report on whether the progress of Year 2000 preparations of the institution and its subsidiaries and overseas branches is behind, ahead or on schedule according to the project plan.

The Reviewer should report on whether he has identified any major concerns or weaknesses in the institution's Year 2000 preparations in the course of the assessment, including those which might affect the ability of the institution to meet the deadlines established by the HKMA.

The Reviewer should recommend additional actions that may assist the senior management of the institution to address the problem areas.