RESCINDED

Office of Thrift Supervision
Department of the Treasury
Acting Executive Director, Supervision
1700 G Street, N.W., Washington, DC 20552 • (202) 906-6853

March 29, 1998

Any attachments to this document are rescinded only as they relate to national banks and federal savings associations.

MEMORANDUM FOR: Chief Executive Officers

FROM: John E. Ryan
Acting Executive Director, Supervision

SUBJECT: FFIEC Guidance Concerning Due Diligence in Connection with Service Providers and Software Vendors, as well as Guidance Concerning the Year 2000 Impact on Customers

This memorandum transmits guidance prepared by the Office of Thrift Supervision (“OTS”) and the other Federal banking regulatory agencies represented on the Federal Financial Institutions Examination Council (“FFIEC”). These guidelines pertain to Year 2000 risks posed to financial institutions by their service providers, software vendors, and customers.

The purpose of the guidance pertaining to service providers and software vendors is to ensure that senior management and the boards of directors of financial institutions establish a due diligence process for determining the ability of these entities to become Year 2000 ready. This process includes: identifying mission critical services and products provided by these entities; monitoring procedures to verify that these entities are taking appropriate Year 2000 actions; establishing contingency plans; and testing those services and products.

This guidance stresses the need for well-defined objectives, testing approaches, and testing schedules. It also encourages management to join forces and coordinate group efforts to evaluate the performance and testing methodologies of service providers and software vendors, to participate in testing efforts to the extent possible, and to evaluate contingency plans. These joint efforts can help financial institutions, particularly smaller ones, more effectively solicit information and demand performance from service providers and software vendors. We want to stay informed of any difficulties or impediments you are experiencing with service providers or software vendors pertaining to the implementation of your ongoing Year 2000 project management plan. Please contact your OTS regional office should problems arise.

RESCINDED

The customer risk guidance will help your institution develop a process to identify customers that pose a material risk, evaluate their Year 2000 preparedness, assess them as credit risks, and implement controls to manage any risk exposure. The guidance recognizes that this process will vary on a case-by-case basis depending on the size of your institution and the size and technological sophistication of your customers. The guidance includes sample forms and questionnaires to assist your staff in evaluating and monitoring the Year 2000 preparedness of your customers.

We would be pleased to answer any questions you may have about this guidance. Please contact your OTS regional office; or Dorothy Van Cleave, National Year 2000 Coordinator at (202) 906-7380; or Jennifer Dickerson, Manager, Information Systems Examinations at (202) 906-5631. This guidance is also available on OTS' website: *www.ots.treas.gov*

Attachments

Federal Financial Institutions **Examination Council**

Board of Governors of the Federal Reserve System
Office of the Comptroller of the Currency
Federal Deposit Insurance Corporation
Office of Thrift Supervision
National Credit Union Administration

2100 Pennsylvania Avenue, NW, Suite 200 • Washington, DC 20037 • (202)634-6526 • FAX (202)634-6556

Press Release

For immediate release March, 1998

FFIEC Issues Guidance on Vendors and Customers' Year 2000 Risk

The Federal Financial Institutions Examination Council (FFIEC) today issued additional guidance for financial institutions on risks they face due to the Year 2000 date change -- risk from service providers and software vendors and from institutions' customers. Today's guidance follows previous FFIEC Year 2000 statements on project management and business risk.

"Regulators want to make sure senior management and boards of directors are fully aware of the wide range of risks that the Year 2000 date change poses for their institutions," said FFIEC Chairman Eugene A. Ludwig. "Regulators have made a major commitment to this challenge and all financial institutions are expected to do the same."

Vendor Due Diligence Guidance

Today's FFIEC guidance on Year 2000 risks from service providers and software vendors calls for financial institutions to develop a due diligence process that includes identifying mission-critical services and products provided by service providers and software vendors, monitoring procedures to verify that service providers and vendors are taking appropriate Year 2000 action, establishing contingency plans, and testing of these services and products within the environment of the financial institution to the extent possible.

The guidance encourages financial institutions to join other financial institutions through user groups to evaluate and test service providers and software vendors' Year 2000 efforts. These joint efforts may help financial institutions to solicit information and demand performance from service providers and software vendors that provide mission-critical products and services.

Financial institutions should develop contingency plans for all mission critical systems and ensure that they pursue alternative means of achieving Year 2000 readiness in the event the service provider or software vendor cannot complete critical efforts by "trigger dates."

As part of the FFIEC's efforts, the FFIEC agencies are conducting examinations of service providers and will provide the results of these examinations to the federally insured financial institution clients of these servicers. The FFIEC agencies also will inspect software vendors that agree to examinations and, where software vendors consent, the agencies will release the results of those examinations to serviced institutions. The agencies, however, will not certify service providers or software vendors as Year 2000 compliant as a result of these reviews.

Customer Risk Guidance

Today's customer risk guidance outlines a due diligence process that will help financial institutions identify material customers, evaluate their Year 2000 preparedness, assess their Year 2000 customer risk, and implement controls to manage the risk. A financial institution can face increased credit, liquidity, or counterparty trading risk when its customers encounter Year 2000-related problems. By June 30, 1998, senior management should implement the due diligence process. By September 30, 1998, Year 2000 assessments, based on this due diligence process, should be substantially completed. The customer risk guidance includes sample forms and questionnaires to assist financial institutions in evaluating the Year 2000 preparedness of their customers.

The guidance recognizes that the due diligence process will vary among financial institutions, depending on the size of an institution and the size and technological sophistication of its customers. The FFIEC identifies three major types of customers: funds takers, funds providers, and capital market/asset management counterparties. For funds takers, such as borrowers and bond issuers, the guidance focuses on assessing how the Year 2000 will affect their ability to meet the terms of contracts.

The guidance notes that Year 2000 problems in the second group of customers, funds providers, can increase an institution's liquidity risk. Year 2000 due diligence plans for this group should focus particular attention to funding concentrations, including concentrations from one provider or group of providers.

Steps to limit Year 2000 risk from a third source -- counterparties and capital markets -- may include requirements for additional collateral or netting arrangements on contracts. The guidance underscores that failure by a capital market customer to meet its obligations because of the Year 2000 problem could cause liquidity problems and, in some cases, total loss on financial contracts.

The FFIEC will issue shortly two additional Year 2000 policy statements on testing and contingency planning.

Interagency Statements

Guidance Concerning Institution Due Diligence in Connection with Service Provider and Software Vendor Year 2000 Readiness

Guidance Concerning the Year 2000 Impact on Customers

OTS Year 2000 Page | OTS home | Other OTS Press Releases

Federal Financial Institutions **Examination Council**

Board of Governors of the Federal Reserve System
Office of the Comptroller of the Currency
Federal Deposit Insurance Corporation
Office of Thrift Supervision
National Credit Union Administration

2100 Pennsylvania Avenue, NW, Suite 200 • Washington, DC 20037 • (202)634-6526 • FAX (202)634-6556

Interagency Statement

March 17, 1998 statement

Guidance Concerning Institution Due Diligence in Connection with Service Provider and Software Vendor Year 2000 Readiness

To: The Board of Directors and Chief Executive Officer of all federally supervised financial institutions, service providers, software vendors, senior management of each FFIEC agency, and all examining personnel.

Background:

The Federal Financial Institutions Examination Council (FFIEC) has issued several statements on the Year 2000 problem. These interagency statements address key phases of the Year 2000 project management process and the specific responsibilities of senior management and the board of directors to address business risks associated with the Year 2000 problem. Nearly all financial institutions in the United States rely on service providers and software vendors to operate mission-critical systems, and thus nearly all should work closely to ensure services and products are Year 2000 ready.

Purpose:

The purpose of this guidance is to ensure that senior management and the boards of directors of financial institutions establish a due diligence process for determining the ability of its service providers and software vendors to become Year 2000 ready, establishing appropriate and effective remediation programs, establishing testing to the extent possible, and developing effective contingency plans in the event service providers and software vendors are not Year 2000 ready.

Summary:

Management of financial institutions should establish a comprehensive Year 2000 due diligence process with its service providers and software vendors. The due diligence process should enable management to:

- Identify and assess the mission-critical services and products provided by service providers and software vendors;
- Identify and articulate the obligations of the service provider or software vendor and the institution for achieving Year 2000 readiness;
- Establish a process for testing remediated services and products in the institution's own environment to the extent possible;
- Adopt contingency plans for each mission-critical service and product; and
- Establish monitoring procedures to verify that the service provider or software vendor is taking appropriate action to achieve Year 2000 readiness.

FFIEC Expectations and Efforts

In the May 1997 Interagency Statement, the FFIEC advised all financial institutions to identify service provider or software vendor interdependencies as part of its assessment phase. The FFIEC recommended that a Year 2000 readiness team and oversight committee, formed by the board of directors in consultation with senior management, be assigned the responsibility for identifying all systems, application software, and supporting equipment that are date dependent. Institutions should have completed their assessments by September 30, 1997. The Interagency Statement also addressed the importance of assessing mission-critical systems first because the failure of mission-critical services and products could have a significant adverse impact on the institution's operations and financial condition. Each system and application should be assessed based on the importance of the system and application to the institution's continuing operation and the costs and time required to implement alternative solutions.

The FFIEC recognizes that service providers and software vendors may not be able or may be unwilling to correct Year 2000-related problems for a variety of reasons. Developers of software and equipment may no longer be in business or they may no longer support the application or operating system. Source code may not be available for remediation and the systems and hardware equipment may have components that are no longer manufactured. In addition, a software provider that sells a large variety and volume of programs might provide only general instructions for reconfiguring a product to the user because of the high cost associated with changing each product. Alternately, a service provider may assume total responsibility for the renovation of its operating systems, software applications, and hardware because its systems are maintained internally. However, the FFIEC believes it is important that financial institutions obtain sufficient information to determine if their mission-critical service providers and software vendors will be able to successfully deliver Year 2000 ready products and services. This guidance assists financial institutions with managing their relationship with service providers and software vendors as their Year 2000 project management plan is implemented.

The FFIEC will support financial institutions in their efforts to meet the expectations addressed in this guidance. The FFIEC agencies will provide to the serviced institutions information on the level of preparedness of their service providers that the agencies inspect. In addition, the FFIEC agencies are encouraging software vendors to provide as much information as possible on their remediation and testing efforts to their client financial institutions. The FFIEC also plans to participate in industry-sponsored events to exchange information on software vendors and the due diligence process and post information on its Internet web site (www.ffiec.gov).

Due to the pivotal role played by service providers and software vendors in an institution's operations, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration have augmented their examination of service providers to include focused Year 2000 reviews. **Although the agencies will not certify service providers or software vendors as Year 2000 compliant as a result of these reviews, the agencies will forward the results of service provider Year 2000 readiness examinations to the serviced institutions that use these service providers.** The agencies also will examine software vendors that agree to periodic inspections. In those cases where the software vendor consents, the results of Year 2000 readiness examinations will be forwarded to client institutions.

The examination reports of service providers and software vendors should not be viewed as a substitute for independent due diligence of your service provider's and software vendor's Year 2000 readiness. The examination reports should not limit a financial institution's efforts to obtain information directly from the service provider and software vendors. The information contained in an examination report reflects the Year 2000 readiness of a service provider and software vendor as of a particular point in time. When reviewing these reports, institutions should be aware that circumstances may have changed since the review was conducted and follow up with the service provider and software vendor may be necessary.

Financial institutions may find it beneficial to join forces with other financial institutions in similar circumstances and coordinate group efforts to evaluate the performance and testing methodologies of service providers and software vendors, to participate in testing efforts to the extent possible, and to evaluate contingency plans. By working through user groups, financial institutions can gather and disseminate information on the efforts of service providers and software vendors, testing methodologies, contingency plans and monitoring techniques. User groups also can be useful to encourage uncooperative service providers and software vendors to provide more prompt and effective service to client institutions.

Responsibilities of Financial Institutions with Respect to Service Providers and Software Vendors

The management of a financial institution is responsible for determining the ability of its service providers and software vendors to address Year 2000 readiness, for establishing appropriate and effective testing and remediation programs, and for developing effective contingency plans in the event providers are not Year 2000 ready. Financial institutions should contact service providers and software vendors to determine what is needed to make the product or service Year 2000 ready. Management also should assess whether the service provider or software vendor has the capacity and expertise to complete the task. Service providers and software vendors should make full and accurate disclosures to their client financial institutions concerning the state of their remediation efforts.

Management should request the following information for all mission-critical products provided by service providers and software vendors:

- Information on Year 2000 project plans, including the scope of the effort, a summary of resource commitments, dates when remediation and testing will begin and end, and dates when Year 2000 products and services will be delivered to the financial institution.
- Plans to discontinue or extensively modify existing services and products.
- Ongoing updates on the service providers' and software vendors' progress in meeting timetables of their Year 2000 project plans.
- Estimates of product and support costs to be incurred by the financial institutions required for remediation and testing.
- Contingency plans of service providers or software vendors in the event their project plans fail.

Financial institutions should thoroughly investigate the legal ramifications of renovating software vendor code because there is considerable legal risk in renovating software vendor-supplied code. For example, code modifications could render warranties and maintenance agreements null and void. However, financial institutions may need to make critical decisions that balance the consequences of these legal risks with business necessity. Financial institutions may also need to determine whether they can terminate their current service contracts and at what cost.

The failure of service providers and software vendors to meet these expectations could pose a risk to the safety and soundness of an institution and in such circumstances, institutions may need to terminate their relationship with the service provider or software vendor.

Testing

Testing for changes to the services and products will play a critical role in the Year 2000 process. Financial institutions should test, to the extent possible, service provider and software vendor provided products and services in the institution's own environment. The FFIEC expects service providers and software vendors to fully cooperate with financial institutions in testing. Management should not rely solely on the stated commitment of a service provider or software vendor to test but request that the scope be defined, objectives listed, and testing approaches and scenarios be developed. Testing schedules should be supplied by service providers and software vendors. In addition, the institution's testing strategy should include a testing scenario to simulate and measure the impact of a Year 2000-related disaster on normal operations.

The FFIEC will provide guidance on testing in an upcoming release.

Contingency Plans

Financial institutions should develop contingency plans for each mission-critical service and product. Contingency plans should describe how the financial institution will resume normal business operations if remediated systems do not perform as planned either before or after the century date change. They should establish "trigger dates" for changing service providers and software vendors to allow sufficient time to achieve Year 2000 readiness. Management of financial institutions, in consultation with the institution's legal counsel, should identify any legal remedies or resolutions available to the institution in the event products are not able to handle Year 2000 date processing. Institutions should consult with business partners that have interconnected systems, user groups, and third-party service providers.

If service providers and software vendors refuse or are unable to participate in Year 2000 readiness efforts or if commitments to migrate software or replace or repair equipment cannot be made by the "trigger date," the institution should pursue an alternate means of achieving Year 2000 readiness. In either of these cases, the institution should consider contracting with other service providers and software vendors to provide either remediation or replacement of a product or service. Difficulties of this nature should be reported to the financial institution's primary federal regulatory agency.

The FFIEC will provide detailed guidance on contingency planning in an upcoming release. However, that portion of a financial institution's Year 2000 contingency plan pertaining to service providers and software vendors should be tailored to the needs and complexity of the institution and should incorporate the following components:

- A risk assessment that identifies potential disruptions and the effects such disruptions will have on business operations should a service provider or software vendor be unable to operate in a Year 2000 compliant environment. The plan should determine the probability of occurrence and define controls to minimize, eliminate or respond to disruptions.
- An analysis of strategies and resources available to restore system or business operations.
- A recovery program that identifies participants (both external and internal) and the processes and equipment needed for the institution to function at an adequate level. The program should ensure that all participants are aware of their roles and are adequately trained.
- A comprehensive schedule of the remediation program of the service provider or software vendor that includes a trigger date. Institutions should assure themselves that adequate time is available should their internal test results require additional remediation efforts.

The development and implementation of contingency plans should be subject to the scrutiny of senior management and the board of directors. Institution management should periodically review both its contingency and remediation plans. These reviews should address the impact that any changes made to a renovation plan might have on contingency plans. Additionally, the institution should ensure that an independent party review these plans. Finally, the institution's senior management and the board of directors should review and approve all material changes to their plans.

Monitor Service Provider and Software Vendor Performance

Management of financial institutions should monitor the efforts of service providers and software vendors. The monitoring process should include frequent communication and documentation of all communication. Since the institution cannot rely solely on the proposed actions of service providers and software vendors, management should contact each mission-critical service provider and software vendor quarterly, at a minimum, to monitor its progress during the remediation and testing phases. The institution should maintain documentation for all of its communications.

Many service providers and software vendors maintain web sites on the Internet with information about the Year 2000 readiness of their services and products. In addition, the FFIEC Year 2000 web site (www.ffiec.gov/Y2K/) includes links to other federal government web sites in which listings of various service provider and software vendor statements are maintained. To the extent that a financial institution relies on information from a web site, a paper copy of the information should be kept on file, and the web site periodically checked to determine if information has been updated.

Conclusion

The FFIEC expects management and the boards of directors of financial institutions to establish a comprehensive Year 2000 due diligence process with its service providers and software vendors. Management of each financial institution is responsible for ensuring that its service providers and software vendors take adequate steps to address Year 2000 problems. Financial institutions should establish contingency plans to ensure that management has alternative options for all mission-critical systems in the event service providers and software vendors are not able to meet key target dates. Management should test services and products in the institution's own environment to the extent possible.

OTS Year 2000 Page | OTS home | Other OTS Press Releases

Last Updated: March 17, 1998

Federal Financial Institutions **Examination Council**

Board of Governors of the Federal Reserve System
Office of the Comptroller of the Currency
Federal Deposit Insurance Corporation
Office of Thrift Supervision
National Credit Union Administration

2100 Pennsylvania Avenue, NW, Suite 200 • Washington, DC 20037 • (202)634-6526 • FAX (202)634-6556

Interagency Statement

March 17, 1998 statement

Guidance Concerning the Year 2000 Impact on Customers

To: The Boards of Directors and Chief Executive Officers of all federally supervised financial institutions, Department and Division Heads of each FFIEC agency, and all Examining Personnel.

Background:

The Federal Financial Institutions Examination Council (FFIEC) has issued three statements providing guidance on the Year 2000 problem. Two interagency statements were issued in June 1996 and May 1997 to address the key phases of the Year 2000 project management process. The most recent guidance, published in December 1997, outlined the specific responsibilities of senior management and the board of directors to address risks associated with the Year 2000 problem.

Purpose:

The purpose of this guidance is to assist financial institutions in developing prudent risk controls to manage the Year 2000-related risks posed by their customers. This guidance describes a variety of approaches for a financial institution's senior management and board of directors to assess the risks arising from the failure or inability of the institution's customers to address their Year 2000 vulnerabilities. This guidance outlines the due diligence process that financial institutions should adopt to manage their Year 2000-related risks arising from relationships with three broad categories of customers: funds takers, funds providers, and capital market/asset management counterparties.

Summary:

Key points addressed in this guidance include:

A financial institution can face increased credit, liquidity, or counterparty trading risk when its customers encounter Year 2000-related problems. These problems may result from the failure of a customer to properly remediate its own systems and from Year 2000 problems that are not addressed by the customer's suppliers and clients. By June 30, 1998, senior management should have implemented a due diligence process which identifies, assesses and establishes controls for the Year 2000 risk posed by customers. By September 30, 1998, the assessment of individual customers' Year 2000 preparedness and the impact on an institution should be substantially completed.

The due diligence process outlined in this guidance focuses on assessing and evaluating the efforts of an institution's customers to remediate their Year 2000 problems. Year 2000 issues related to the institution exchanging data with its customers should be addressed as a part of the institution's internal Year 2000 project management program.

The guidance recognizes that each institution must tailor its risk management process to its size, its culture and risk appetite, the complexity of its customers, and its overall Year 2000 risk exposure. The FFIEC understands that these differences will affect the risk management programs developed by financial institutions. However, financial institutions must evaluate, monitor, and control Year 2000-related risks posed by funds providers, funds takers, and capital market/asset management counterparties.

The institution's due diligence process should identify all customers representing material Year 2000-related risk, evaluate their Year 2000 preparedness, assess the aggregate Year 2000 customer risk to the institution, and develop appropriate risk controls to manage and mitigate Year 2000 customer risk.

Risk management procedures will differ based on a variety of factors, including the institution's size, risk appetite and culture, the complexity of customers' information and operating systems, and the level of its own Year 2000 risk exposure. The Year 2000 due diligence processes used by smaller institutions may not be as extensive or formal as those in larger institutions where customers may be more dependent upon information technology.

The attached appendices provide examples of processes used by financial institutions to manage Year 2000-related customer risk.

An institution's management should provide quarterly reports to the board of directors that identify material customers who are not effectively addressing Year 2000 problems. The reports should summarize the action taken to manage the resulting risk.

Overview

The Year 2000 problem presents many challenges for financial institutions and their customers. The FFIEC recognizes that risk management procedures will vary depending on the institution's size, its risk appetite and culture, the complexity of customers' information and operating systems, and the level of its own Year 2000 risk exposure. For example, customers of small community financial institutions may not depend on computer-based information systems to the same extent as large business customers of large financial institutions. As a result, Year 2000 due diligence processes used by these institutions may not be as extensive or formal as those in institutions whose customers may be more dependent upon information technology. Senior management should oversee the development and implementation of a due diligence process which is tailored to reflect the Year 2000 risk in their institution's customer base.

Three major types of customers may expose a financial institution to Year 2000-related risks. They include funds takers, funds providers, and capital market/asset management counterparties.

Fund Takers
Funds takers include borrowers and bond issuers that borrow or use bank funds. Failure of fund takers to address Year 2000 problems may increase credit risk to a financial institution through the inability of fund takers to repay their obligations.

Funds Providers
Funds providers provide deposits or other sources of funds to a financial institution. Liquidity risk may result if a funds provider experiences a Year 2000-related business disruption or operational failure and is unable to provide funds or fulfill funding commitments to an institution.

Capital Market/Asset Management Counterparties
Capital market and asset management counterparties include customers who are active in domestic and global financial markets. Market trading, treasury operations, and fiduciary activities may be adversely affected if a financial institution's capital market and asset management counterparties are unable to settle transactions due to operational problems caused by the Year 2000 date change.

General Risk Control Guidelines

By June 30, 1998, financial institutions should establish a process to manage the Year 2000 risks posed by its customers. The process should: (1) identify material customers; (2) evaluate their Year 2000 preparedness; (3) assess their Year 2000 risk to the institution; and (4) implement appropriate controls to manage and mitigate their Year 2000-related risk to the institution. The assessment of individual customers' Year 2000 risk and their impact on an institution should be substantially completed by September 30, 1998. Year 2000 issues related to data exchanges between the institution and customers should be addressed as a part of an institution's internal Year 2000 project management program.

Identify Material Customers
Management should identify customers that represent material risk exposure to the institution, including international customers. Material risk exposure may depend on:

- Size of the overall relationship;
- Risk rating of the borrower;

Complexity of the borrower's operating and information technology systems;
Customer's reliance on technology for successful business operations;
Collateral exposure for borrowers;
Funding volume or credit sensitivity of funds providers; and
Customer's dependence on third party providers of data processing services or products.

Assess Preparedness of Material Customers
The impact of Year 2000 issues on customers will differ widely. Smaller financial institutions may find that most of their material borrowers use either manual systems or depend on commercial software products and services. The evaluation of Year 2000 preparedness for these customers will be less involved and may not require additional risk management oversight. To ensure consistent information and a basis for comparisons among customers, management should address the following.

Train account officers to perform a basic assessment of Year 2000 risk of customers.
Develop a standard set of questions to assess the extent of a customer's Year 2000 efforts. Appendices A - D contain samples of forms some financial institutions use to evaluate customer Year 2000 preparedness. Financial Institutions are not required to use these forms, although they provide useful examples of methods to evaluate customer preparedness.
Update the status of a customer's Year 2000 efforts periodically, but at least semi-annually. For customers that represent significant Year 2000 exposure to the institution, quarterly updates may be necessary.
Document Year 2000 assessment conclusions, subsequent discussions, and status updates in the institution's customer files.

Evaluate Year 2000 Risk to the Institution
After identifying all customers representing material Year 2000 risk and evaluating the adequacy of their Year 2000 programs, management should assess the Year 2000 risk posed to the institution by these customers, individually and collectively. Management should determine whether the level of risk exposure is high, medium, or low. Management also should provide quarterly updates to the board of directors on customers that are not addressing Year 2000 problems effectively and discuss the actions taken by the institution to control the risk.

Develop Appropriate Risk Controls
Once the institution has evaluated the magnitude of Year 2000 risk from its customers, management must develop and implement appropriate controls to manage and mitigate the risk. Senior management should be active in developing risk mitigating strategies and ensure that effective procedures are implemented on a timely basis to control risk.

Specific Risk Control Guidelines

The specific risk controls an institution implements will vary depending on the size of the institution, its risk appetite and culture, the complexity of customers' information and operating systems, and its own level of Year 2000 risk exposure. Different risk management controls may be needed to address unique and material Year 2000 issues that arise from business dealings with different categories of customer.

Funds Takers
An institution's Year 2000 risk management controls for funds takers should focus on limiting potential credit risk by ensuring that Year 2000 problems do not prevent a borrower or bond issuer from meeting the terms of its agreements with the institution. Controls to manage an institution's exposure to its funds takers should address underwriting, documentation, credit administration, and the allowance for loan and lease losses (ALLL). These same factors also should be considered, where appropriate, when evaluating risk posed by an institution's capital market and asset management counterparties.

Underwriting
During any underwriting process, management should evaluate the extent of the borrower's Year 2000 risk. Specifically, management should:

Ensure that underwriters are properly trained and have sufficient knowledge to perform a basic assessment of Year 2000 customer risk. There are a number of resource materials available that will assist in informing lenders of Year 2000 issues. State and national trade associations have prepared materials to assist lenders in understanding customer risk created by the Year 2000. Additional information is available on the Internet and can be located by searching on the words "Year 2000".

Evaluate whether Year 2000 issues will materially affect the customer's cash flows, balance sheet, or supporting collateral values. As a part of the assessment and based on materiality, management should consider the complexity of the customer's operations; their dependence on service providers or software vendors; the extent of management oversight of the Year 2000 project; the resources the customer has committed to the project; and the date the customer expects to complete Year 2000 efforts.

Control credit maturities or obtain additional collateral, as appropriate, if credit funding is to be continued for high-risk customers.

Documentation

Proper loan documentation provides an effective means to monitor and manage the Year 2000 risk posed by borrowers. Loan documents should reflect the degree of risk posed by customers. Institutions should consider incorporating some or all of the following into loan agreements:

Representations by borrowers that Year 2000 programs are in place;

Representations that borrowers will disclose Year 2000 plans to the lender, provide periodic updates on the borrower's progress of the Year 2000 program, and provide any assessment of the borrower's Year 2000 efforts conducted by a third party;

Audits that address Year 2000 issues;

Warranties that the borrower will complete the plan;

Covenants ensuring that adequate resources are committed to complete the Year 2000 plan; and

Default provisions allowing the lender to accelerate the maturity of the debt for non-compliance with Year 2000 covenants;

Credit Administration

After the initial assessment, ongoing credit administration provides the best opportunity for an institution to manage Year 2000-related customer risk. Periodic credit analyses, which should include an update of the customer's Year 2000 efforts, can help to monitor a borrower's Year 2000 efforts. When performing credit analyses, loan officers should determine whether a customer's Year 2000-related risk merits an adjustment to its internal risk rating.

ALLL Analysis

Management's review of the adequacy of loan and lease loss allowances should include Year 2000 customer risk. When Year 2000 issues adversely impact a customer's creditworthiness, the allowance for loan and lease losses should be adjusted to reflect adequately the increased credit risk. Additionally, management's analysis of loss inherent in the entire portfolio should reflect Year 2000 risk.

Funds Providers

Management should consider the potential effect on an institution's liquidity by assessing the potential for unplanned reductions in the availability of funds from significant funding sources that have not taken appropriate measure to manage their own Year 2000 problems. Management should develop appropriate strategies and contingency plans to deal with this potential problem.

Risk Assessment of Funds Providers

As with funds takers, management should discuss Year 2000 issues with significant funds providers, evaluate their Year 2000 readiness to the extent possible, and assess the Year 2000-related risks posed by the providers. Management should be aware of concentrations -- including concentrations in any single currency -- from an individual provider or group of providers that may not be Year 2000 ready.

Contingency Planning

The risk assessment of major funds providers' Year 2000 readiness should be incorporated into an institution's liquidity contingency plans. As with other contingency planning processes, management should evaluate its exposure and potential funds needs under several scenarios that incorporate different assumptions about the timing or magnitude of funds providers' Year 2000-related problems. Institutions with significant funds flows in different currencies may needs separate contingency plans for each major currency.

Although the liquidity risks from funds providers' Year 2000-related problems are similar to other "event risks" that institutions address in their liquidity contingency plans, Year 2000-related liquidity risks differ because the date of this event is known in advance. As a result, institutions may be better able to plan for and mitigate potential liquidity risks. For example, institutions may be able to reduce potential liquidity risks by extending the maturity of their advances under funding lines sufficiently past January 1, 2000, to provide time to assess and evaluate the effect of the Year 2000 on its funds providers. Maintaining close contact with funding sources throughout this potentially difficult period can provide management with timely, market sensitive information and thus allow for more effective liquidity planning.

Capital Market and Asset Management Counterparties

The focus of the controls for an institution's exposure to Year 2000-related problems in capital markets and among counterparties mirror those needed for funds takers and funds providers. Potential Year 2000-related problems with capital market participants range from a counterparty's failure to complete a securities transaction or derivatives contract settlement to, in extreme cases, the failure of the counterparty itself. A counterparty failure could lead to the total loss of the value of the payment or contract. A counterparty's failure to settle a transaction could cause the institution unexpected liquidity problems, which in turn could result in the failure of a financial institution to deliver dollars or foreign currencies to its counterparties.

In addition, Year 2000-related problems among fiduciary counterparties could prevent a financial institution from fulfilling its fiduciary responsibilities to protect and manage assets for fiduciary beneficiaries. A counterparty's failure to remit bond payments, fund employer pension contributions or settle securities transactions could increase the institution's fiduciary risk.

Risk Assessment of Counterparties

As part of a sound due diligence process, management should identify and discuss Year 2000 compliance issues with those counterparties which represent large exposures to the bank itself and to fiduciary account beneficiaries. Financial institutions should evaluate counterparty exposure and develop risk reducing action plans to help manage and control that risk.

Risk Reduction Plans

In cases where institutions are not fully satisfied that their counterparties will be Year 2000 ready, management should establish mitigating controls such as early termination agreements, additional collateral, netting arrangements, and third-party payment arrangements or guarantees. In cases where management has a high degree of uncertainty regarding a counterparty's ability to address its Year 2000 problems, the institution should consider avoiding transactions with settlement risk after January 1, 2000. As noted earlier, the interest rate effect of material mismatches of funding, or maturity, should be evaluated as maturity and settlement risk is adjusted. The financial institution should not resume normal transaction activities until the counterparty has demonstrated that it will be prepared for the Year 2000.

Conclusion

Financial institutions face significant internal and external challenges from Year 2000-related risks posed by their customers. The concepts and guidance in this interagency statement are designed to assist institutions in developing appropriate risk controls. The FFIEC recognizes that risk management procedures may vary depending on the institution's size, its risk appetite and culture, the complexity of its customers' information systems, and its own Year 2000 risk exposure. While these differences will affect the risk management practices developed by management, it is essential that financial institutions identify, measure, monitor and control Year 2000-related risks posed by funds providers, funds takers, and capital market/asset management counterparties.

Appendix A: Year 2000 Questionnaire (9 KB PDF)

Appendix B: Year 2000 Worksheet (14 KB PDF)

Appendix C: Millenium Risk Evaluation (13 KB PDF)

Appendix D: Year 2000: Credit Risk Assessment Worksheet (26 KB PDF)

Appendix A

YEAR 2000 QUESTIONNAIRE

FOR CUSTOMERS OF ______________________________ BANK

Customer Name: ______________________________ Date: _______________________

Relationship Manager: _________________________

Please complete the questionnaire based on responses from the customer. If necessary, comment in the space provided or attach additional information to this form. Any "No" answers require appropriate follow-up with the customer on a periodic basis. Please retain a copy of this form in the credit file.

	Yes	**No**	**N/A**
1. Has the company developed a comprehensive plan for Year 2000 compliance?			
2. Is someone in the company specifically responsible for managing the Year 2000 plan?			
3. Has senior management and the board of directors reviewed and approved the plan?			
4. Has the company completely inventoried its software, hardware, and telecommunications?			
5. Has the company identified all equipment with date-sensitive operating controls such as elevators, HVAC, security systems, manufacturing equipment, etc.?			
6. Has the company verified that vendor-supplied systems will be Year 2000 compliant?			
7. Has the company verified Year 2000 compliance of outside data-processing companies and established a testing time frame?			
8. Has the company budgeted sufficient resources (both financial and personnel) to accomplish its Year 2000 mission?			

9. Has the plan been reviewed by the company's outside auditors?			
10. Does the company's plan call for remediation and preliminary testing of critical systems to be largely completed by 12/31/98?			
11. Will the company have contingency plans for mission critical systems in place by 12/31/98?			
12. Does the company have any ongoing or long-term contracts that could subject it to liability if it failed to perform as a result of Year 2000 compliance failure?			
13. Has the company discussed potential legal ramifications or expenses with its attorney?			
14.Has the company discussed potential losses from Year 2000 problems with insurers to determine coverage of any losses?			

Comments:

____

____

____

____

Appendix B

YEAR 2000 WORKSHEET

The following are issues surrounding Year 2000 that your relationship manager will be discussing with you in the near future. Please note that this worksheet should not be used and is not intended to be used by you to determine whether your company needs to enlist assistance in assessing and addressing your company's Year 2000 preparedness and/or exposure. For answers and assistance regarding Year 2000 questions, you should contact qualified professionals of your choice.

Circle Response	**ISSUE IDENTIFICATION**
Y N N/A	
	• Has your company begun its assessment of the scope of being Year 2000 compliant?
Y N N/A	• Are your following systems capable and ready to handle Year 2000 processing?
Y N N/A	• Information processing (hardware and software)
Y N N/A	• Delivery (telecommunication and transportation)
Y N N/A	• Manufacturing (robotics, lighting, heat, water supplies)
Y N N/A	• Real estate (HVAC, security, card access, elevators)
	• Support (insurance, license, automatic inventory control)
	• For each "No" answer to the last question, which systems need to be modified to handle year
Y	2000 processing?
Y	• Information processing
Y	• Delivery
Y	• Manufacturing
Y	• Real estate
Y N N/A	• Support
	• Has any vendor of any of the above advised that they will not make their system Year 2000
Y N N/A	compliant? Please specify.
	• If outside data processing service bureaus are used, have they been verified for Year 2000
Y N N/A	compliance and a testing time frame established?
	• Do you have any ongoing or long term contracts that could subject you to liability if you failed
	to perform as a result of a Year 2000 compliance failure?
	SPONSORSHIP/MONITORING
Y N N/A	
	• Has your company assigned overall responsibility for the Year 2000 effort to a senior manager?
Y N N/A	• Does the process include regular reporting to and monitoring by senior management?
Y N N/A	• Does the process include regular reporting to and monitoring by the Board?

OVERALL PLAN

	• Does your company have a Year 2000 problem resolution process that includes:	•Has your company discussed a Year 2000 problem resolution process that includes (Awareness, assessment, renovation, etc.): With Key Suppliers	With Key Customers
Y N N/A	• Awareness of the problem	Yes No N/A	Yes No N/A
Y N N/A	• Inventory check list*	Yes No N/A	Yes No N/A
Y N N/A	• Assessment of complexity	Yes No N/A	Yes No N/A
Y N N/A	• Remediation	Yes No N/A	Yes No N/A
Y N N/A	• Validation/Testing	Yes No N/A	Yes No N/A
Y N N/A	• Implementation	Yes No N/A	Yes No N/A

*Complete list of equipment, software, etc., that may be affected by the Year 2000 issue

Y N N/A • Has your company discussed the Year 2000 issue with its major suppliers, service providers or customers in terms of any system interfaces that may exist between them?

RESOURCE ISSUES

Y N N/A • Has your company established a budget for the Year 2000 effort (determined how much and how the expenditures will be financed)?

Y N N/A • Has your company assigned adequate personnel resources to the project?

Y N N/A • Has your company discussed potential legal ramifications or expenses with its attorney?

Y N N/A • Will your company's CPA firm help in this task?

Y N N/A • Has your company hired a consultant to assist with Year 2000 issues?

TIMING

Y N N/A • Has your company established project target dates and deliverables for the Year 2000 effort?

• By what date does your company's Year 2000 plan call for the renovation and testing of all mission critical systems to be largely completed? Date _______________

• By what date will contingency plans for mission critical systems be in place?
Date _____________

Year 2000
Customer Evaluation

Customer Name: ______________________ **Rel Mgr/Mail Code:** __________________________
Obligor #: ___________________________ **Date:** _____________________________________

Instructions: Complete the evaluation based on responses to the Customer Questionnaire, Customers rated "High" or "Medium" require quarterly follow-up until their "Status" is rated "l". Forward a copy of completed forms to Loan Administration. Retain a copy of this form in the Credit File.

---

1. Rate the company's sensitivity to Year 2000 risk based on the following information about the company's operations:

High Medium Low (circle one)

High	**Medium**	**Low**
a. Could not conduct its business If it did not have computers, or	**a. Computers only used in financial, accounting, and recordkeeping functions, or**	**a. Minimal reliance on computers to conduct its business**
b. Operates in computer-related industry, or	**b. Has customers or suppliers that are systems impacted**	
c. Has major customers, suppliers, or vendors which meet (a) or (b) above.		

---

2. Rate the status of the company's Year 2000 implementation on the following scale (1-6, with 1 representing most progress to 6 representing least progress):

1 2 3 4 5 6
(circle one)

1. **Has Year 2000 plan with budget, implementation dates in place**
   - **Plan has senior management (and Board) support and regular reporting on status.**
   - **Plan is evidenced by material progress toward testing and implementation**
   - **Year 2000 issues have been discussed with information system vendors, key customers, and suppliers**
2. **Has Year 2000 plan with budget, implementation dates in place**
   - **Limited action taken on plan implementation to date**
3. **Has preliminary Year 2000 plan and budget drafted but not finalized and approved**
   - **Very limited or no action taken to date**
4. **Aware of Year 2000 issue and intends to draft a plan but has not begun**
5. **Not fully aware of Year 2000 issue**
6. **No intention of completing a Year 2000 plan**

Millennium Risk Evaluation

Yes No

I. Awareness

A. Is the customer realistically aware of and does the customer understand the Year 2000 or Millennium problem and the potential business and financial risks to which he or she is exposed? ☐ ☐

B. Has the customer identified an individual and/or a working group responsible for all functions impacted by Year 2000? ☐ ☐

Name: ______________________________

C. Is the customer relying on:
☐ internal ☐ external resources?

A. Does the customer fully understand how their industry, business, customers and key partners can be affected? Different industries are impacted in very different ways. A casual explanation is probably a warning that the issue has not been explored in depth. A quick glance at the millennium matrix can guide you to complexity levels.

B. If an individual has not been selected to lead the program, then a program does not exist. Identify the person. Is this a full time job? Are their skill sets consistent with the task?

C. Reliance on third parties is not uncommon, but heavy use of external resources can increase the risk by not having full control at all times.

II. Vulnerability and Dependency

A. Are mainframe or minicomputer applications critical to core business operation, whether in-house or outsourced? ☐ ☐

B Does the core business operation depend on automated processes, whether delivered on desktop computers or mainframes, whether in-house or outsourced? ☐ ☐

C. Do critical dependencies exist (suppliers, customers) that are vulnerable to Year 2000 disruptions? ☐ ☐

A.B.C. It is hard to imagine industries where computers are not critical, functions/operation are not automated, or where critical dependencies do not exist; we are seeking high levels of criticality where alternatives are few and the business functionality is at risk. These questions could be answered through a relationship manager's own knowledge of the business/industry.

III. Assessment

A. Has the customer performed an assessment of the Year 2000 impact on its system and business operations? ☐ ☐

B. Has the customer developed a complete inventory of all hardware (including mainframes, minicomputers, local and wide area networks and personal computers), firmware, and software (including systems and applications) components for all EDP systems? ☐ ☐

C. Has the customer had to provide certifications or disclose millennium status to third parties? ☐ ☐

A. An assessment is the foundation of serious planning and budgeting. The discussion should cover major business segments; for example, inquiring how major balance sheet categories could be negatively impacted by incorrect date calculations could form the basis of determining how deeply the customer has analyzed its condition. Lack of an assessment is a red flag.

B. The inventory of hardware, firmware, and software falls out of the assessment and vice versa. If the inventory has not been taken, than a plan and budget cannot be completed. The entire program is suspect.

C. Ask about the nature and frequency of inquiries being directed at the borrower, which will mirror the nature of their issues and industry challenges. Can you see a few? Do they keep a log?

Millennium Risk Evaluation

IV. Current Status

	Yes	No
A. At what stage is the customer in his or her Year 2000 project:		
☐ Has not started		
☐ Up to 1/4 complete		
☐ Up to 1/2 complete		
☐ Up to 3/4 complete		
☐ More than 3/4 complete		
B. Does the customer report that he or she is on schedule?	☐	☐
C. Does the customer report that the project will be completed before Year 2000?	☐	☐
D. Will there be time for testing?	☐	☐

A. B. C. Keep in mind that there is a date certain by which this work must be done; it cannot be moved. In discussing the date of completion and the status thereof, determine how much reliance has been placed on third party delivery dates, which are outside of company control.

D. Testing is critical to ensure trouble-free operations.

V. Budget, Planning and Impact

A. Has the customer developed a credible plan and budget for the Year 2000 project that is properly funded?

1. What is the estimated cost? $ ________
2. Millennium cost as a % of Technology budget? $ ________
3. Expended to date? $ ________
4. Over how many years spent? $ ________

B. What is the impact to the customer if Year 2000 issues and programs are not successfully completed?

No downgrade, or downgrade within pass categories	Green	☐
Downgrade to problem loan status	Yellow	☐
Risk of loss	Red	☐

C. In your opinion, will this customer meet significant Year 2000 timetables?

Highly likely	Green	☐
Tight schedule - not sure	Yellow	☐
Unlikely	Red	☐

A. After some discussion on resources, inventory, pervasiveness of technology; etc., you should be developing an opinion on whether the plan and budget, if they exist, are indeed appropriate and credible. We do not expect you to be technology experts, but reasonably informed on your customers' efforts to remediate their systems.

B. We are asking you to consider the impact of failure to remediate systems. Is capacity to pay impacted in a way that will affect a risk rating?

C. Consider this question in the light of the specificity of the plan, the complexity of the operations, the resources and funds dedicated to the project, and the track record of management in overcoming similar challenges. In situations where risk of loss or downgrade to problem loan status is the outcome of failure, we need to be very certain of the answer.

Appendix D

Year 2000: Credit Risk Assessment Worksheet

Information

The purpose of this worksheet is to help credit officers assess the level of a business borrower's risk associated with the Year 2000 (Y2K) problem and to ensure consistency of Y2K risk assessment approach.

The worksheet is multidimensional, assessing (1) the borrower's overall vulnerability to the Y2K problem, (2) the borrower's resources to manage the problem, and (3) the adequacy of the borrower's Y2K plan.

Although designed in a "check-the-box" format, the worksheet does not replace thoughtful and informed analysis.

Add to this worksheet issues that are specific to the business that you are assessing. Record and support appropriate conclusions driven by your information and analysis, whether or not derived directly from the worksheet logic.

The worksheet is divided into four parts:

- Part 1 is an overall Y2K *credit risk* conclusion, based on the assessments in Parts 2, 3, and 4.
- Part 2 is a *vulnerability* assessment, which helps to determine whether the business because of its reliance on technology, supplier, and or customer concentrations, and other considerations is at high, medium, or low risk to the Y2K problem.
- Part 3 is a *financial, management, and technology resource* assessment, which helps to determine whether the business is at high, medium, or low risk in relation to the depth and stability of resources available to address its Y2K problem.
- Part 4 is a Y2K *plan* assessment, which helps to determine whether the business is at high, medium, or low risk based on the adequacy of its Y2K plan.

Borrower Name ______________________________ Risk Rating ___________
Borrower Industry _____________________________ SIC __________
Binding Commitments ($000) ___________________

Worksheet Prepared by ________________________ Telephone ____________
Unit Name __________________________________ Unit # ________________
Date Prepared ______________________________

Part 1: Year 2000 Credit Risk Summary and Conclusion
Complete Part 1 after completing Parts 2, 3, and 4 on the following pages. Section C is provided for updating conclusions at intervals as required by managers or as new information is obtained from the borrower.

A: Summary of Conclusions from Parts 2, 3, and 4	
Part 2. Y2K Vulnerability Risk	☐ **Low** ☐ **Medium** ☐ **High**
Part 3. Y2K Resource Risk	☐ **Low** ☐ **Medium** ☐ **High**
Part 4. Y2K Plan Risk	☐ **Low** ☐ **Medium** ☐ **High**

B: Conclusion: Overall Y2K Credit Risk Assessment

Based on the above and other considerations as applicable, determine an overall Y2K credit risk conclusion for the borrower. Generally, if both resource and vulnerability risk assessments are low, the conclusion should be low overall risk regardless of the adequacy of the Y2K plan.

☐ Low Y2K credit risk ☐ Medium Y2K credit risk ☐ High Y2K credit risk

Comments:

C: Update

Date: ________________ Name (if differs from above): _______________________ BANet: _____________

Based on information in the comments below, provide an updated Y2K credit risk conclusion.

☐ Low Y2K credit risk ☐ Medium Y2K credit risk ☐ High Y2K credit risk

Comments:

Part 2. Year 2000 Vulnerability Assessment			
A. Overall technological and business vulnerability to the year 2000 problem			
	Yes	**No**	**Comments**
Are mainframe or mini-computer applications critical to core business operation, whether in-house or outsourced?			
Does core business operation depend on one or more automated processes (e.g., inventory, assembly line, shipping, customer orders, etc.), whether delivered on desktop computers or mainframes, whether in-house or outsourced?			
Does the business depend on any one supplier for 25% or more of inventory, is there a single mission critical supplier, and/or is the supply chain generally vulnerable to Y2K disruption?			
Does the business depend on any one customer for 25% or more of revenue and/or is the customer base generally vulnerable to Y2K disruption?			
Are there other key Y2K vulnerabilities? If you check yes, explain your assessment in the comment section.			
B. Vulnerability Risk Conclusion			
♦ If all boxes in Section A. Above are checked **No**, it is likely that business vulnerability risk is low; if this is your conclusion, stop here and indicate low vulnerability risk below. ♦ If one or more boxes above have been checked **Yes**, vulnerability to the Y2K problem is medium to high. Continue Part 2 by checking *yes* or *no* to the following (substantiate all *yes* responses).			
	Yes	**No**	Comment/Substantiation of "Yes" Response
Is the business by its nature generally not vulnerable to technology failure (e.g., some personal service businesses)?			
If there is a business interruption caused by a Y2K problem, could the business recover rapidly because of ready accessibility of viable alternatives, or other reasons particular to this business operation?			
♦ If one or more of the section B boxes above are checked **Yes**, it is likely that Y2K vulnerability is medium; if this is your conclusion, indicate medium vulnerability risk below. ♦ If both boxes are checked **No**, it is likely that Y2K vulnerability is high; if this is your conclusion, indicate high vulnerability risk below.			
Overall Year 2000 Vulnerability Conclusion			
Technological and business vulnerability risk is: ☐ **Low** ☐ **Medium** ☐ **High**		Comments:	

Part 3. Year 2000 Resource Risk: Financial, Management, and Technological Assessment Consider the adequacy of financial, management, and technology resources in relation to the extent of the technological vulnerability risk identified in Part 1.
☐ **Low Resource Risk** Financial, management, and technology resources (whether in-house or outsourced) available to address Y2K are superior to exceptional and business is not facing other unavoidable internal or external challenges likely to divert necessary resources.
☐ **Medium Resource Risk** Financial resources available to address Y2K are ample, management quality is good, technological expertise is readily available (in-house or outsourced) and business is not facing other unavoidable internal or external challenges likely to divert necessary resources.
☐ **High Resource Risk** Financial resources available to address Y2K are marginal to inadequate, management depth is thin, technological expertise is marginal to inadequate or not readily available, and/or business is facing other unavoidable claims on cash flow or business stability that threaten the adequacy of resources available for Y2K.
Comments:

Part 4. Year 2000 Plan Assessment (based on discussions with management).

	Yes	**No**	**N/A**	**Comments**
Does the business have a comprehensive Y2K plan that effectively prioritizes mission-critical systems?				
Does the Y2K plan have the endorsement and involvement of executive management?				
Has management clearly established that implementation of the Y2K plan has first priority?				
Does the Y2K plan include vendor compliance?				
Does the Y2K plan include contingencies for the impact of Y2K business interruptions affecting key vendors, suppliers, or customers?				

Part 4. Year 2000 Plan Assessment Continued

	Yes	No	N/A	Comments
Does the Y2K plan include computer controlled systems such as telecommunications, security systems, elevators, and climate control?				
Has a Y2K budget been established? (Enter budget totals in Comments.)				($000) 1997 $ __________ 1998 $ __________ 1999 $ __________ 2000 and beyond $ __________
Has the business incorporated the effect of Y2K into its financial planning?				
Has the business taken any steps to ensure key staff do not leave prior to project completion?				
Is the business generally meeting its plan deliverables at the dates specified in the plan?				Target completion date ___________
Is the business developing contingency plans to mitigate risk if the Y2K project is not completed on time?				
Other key considerations:				

Overall Plan Assessment

☐ Low Risk: Good Overall Plan All questions above are answered yes or not applicable	☐ Medium Risk: Adequate Plan Most questions above are answered yes or not applicable; those that are answered no are not critical to success.	☐ High Risk: Inadequate Plan Most questions above are answered no, or one or more answered no are critical to success.