Federal Financial Institutions Examination Council

YEAR 2000

WORKPROGRAM

PHASE II

VERSION 3.02

Number:

Institution/Organization Name:

City/State:

Date of Review:

Examiner In-Charge:

INTRODUCTION

The following examination procedures are for use in federally supervised financial institutions, service providers, and software vendors. The examination procedures will help the examiner to determine if the institution has addressed the Year 2000 problems inherent in many computer software, hardware, and environmental systems as well as indirect risks associated with external sources, customers, or fiduciary activities. The examination procedures are designed to focus on the adequacy of the institution's plans and processes for achieving Year 2000 readiness, with particular emphasis placed on the final phases of the Year 2000 project. These procedures apply to systems in domestic institutions and in their foreign branches and subsidiaries.

GENERAL INSTRUCTIONS

The workprogram is divided into six sections (General, Renovation, Validation, Implementation, Contingency Planning, and Examination Conclusions), each containing a series of work steps and related examination procedures. In most cases, related examination procedures are then subdivided in categories for general procedures, serviced institutions, turnkey institutions, and large or complex organizations. The subdivided categories are defined below.

General Procedures	These procedures should be performed, as applicable, during all reviews of financial institutions, service providers, or software vendors.
Serviced Institutions	Procedures detailed under the subheading of "Serviced Institutions" should be performed, as applicable, during reviews of institutions in which mission-critical data processing services are provided by an affiliated or nonaffiliated data processing service provider.
Turnkey Institutions	Procedures under this subheading should be performed, as applicable, during reviews of institutions which rely on outside vendors for mission-critical hardware and software.
Large or Complex Organizations	Procedures under the subheading of "Large or Complex Organizations" should be performed, as applicable, if the review is being conducted at any one of the following: an independent service provider, a financial institution or a subsidiary of a holding company which services other financial institutions, a software vendor, a financial institution which does in-house programming, a financial institution with total assets greater than $1 billion, and a financial institution whose systems are deemed complex.

For certain hybrid institutions, such as those which exhibit a blend of turnkey and serviced characteristics, examiners would use an appropriate blend of questions under the serviced institution and turnkey institution headings.

This workprogram provides a risk-focused approach to the Year 2000 on-site examination process. Therefore, an examination seldom will require every step in the workprogram to be performed. Examiners should complete those worksteps and examination procedures which are necessary to respond to the requirements in the Examination Conclusions Section. The scope of the examination

should be appropriate to the nature and sophistication of the entity under review; institution management's understanding of the Year 2000 issue and their ability to oversee the institution's Year 2000 correction process; and to the institution's current progress in completing its Year 2000 project phases. Examiners may leverage the efforts of internal/external audit when this work is deemed effective in evaluating the entity's Year 2000 readiness. Note that not all institutions, or all systems within an institution, may be in the same phase (awareness, assessment, renovation, validation, implementation) at the time of review. In instances where a question is not applicable, use N/A.

The FFIEC Year 2000 Examination Procedures, issued in May 1997, are supplemented by this workprogram. (Refer to guidance issued by each respective agency regarding effective dates.) However, examiners may reference and use any part of the original workprogram if additional guidance is sought. Portions of the FFIEC Year 2000 Examination Procedures workprogram may be particularly useful during first time Year 2000 reviews of newly chartered institutions.

OBJECTIVES

1. To determine if the institution is handling Year 2000-related issues in a safe and sound manner and if the project is meeting established timelines and FFIEC key milestone dates.
2. To follow up on results from previous Year 2000 reviews.
3. To determine whether the institution has implemented an effective plan for testing Year 2000 renovated products and implementing these products into its production environment.
4. To assess the adequacy of the institution's Year 2000 contingency plans.
5. To determine whether further corrective action is necessary to assure that Year 2000 readiness is achieved.

PRE-EXAMINATION PLANNING

1. Determine the institution's sources of information systems support for hardware (mainframe, mid-range, networks, personal computers) and related applications, operating system software, and environmental systems. Note whether mission-critical information systems processing is provided internally, externally, or both.

2. Review previous examination, audit, and/or consultant findings relative to Year 2000 issues, particularly results from the institution's last on-site Year 2000 examination/visitation noting significant findings and management responses.

3. Review the FFIEC Year 2000 Workprogram and related workpapers from the institution's last on-site review and any subsequent off-site reviews. Follow-up on any deficiencies noted.

4. Review institution specific information contained in your agency's Year 2000 tracking record/databases, including any information concerning new systems, services, or other changes that have occurred since the previous examination.

5. Review any existing informal or formal regulatory actions as well as resulting correspondence for Year 2000 provisions.

6. For turnkey and serviced institutions, obtain and review a copy of the latest report of examination, Year 2000 visitation report, or shared application software review for the mission-critical service provider or software vendor used by the institution.

SECTION 1 - GENERAL

This section is designed to provide general examination procedures for following up on progress made during the awareness and assessment phases, provide guidance on miscellaneous areas of Year 2000 risk, allow for the evaluation of the involvement and effectiveness of internal/external audit, and provide for an assessment of the institution's indirect Year 2000 risks associated with external sources, customers, and fiduciary activities. For further guidance, examiners should refer to the Interagency Statements on Year 2000 Impact on Customers, Guidance on Year 2000 Customer Awareness Programs and Year 2000 Business Risk.

WORK STEPS

1.1 Obtain a copy of the institution's Year 2000 project plan.

1.2 Obtain and review board minutes, Year 2000-related committee minutes, if applicable, and copies of management status reports on Year 2000-related activities.

1.3 Obtain and review internal/external audit or other qualified sources' plans for, and reports of review of, Year 2000 activities.

1.4 Obtain and review the institution's Year 2000 inventory of hardware, software, and environmental systems.

1.5 Obtain and review the institution's Year 2000 budget.

1.6 Obtain and review any customer awareness pamphlets/letters being distributed by the institution.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL - AWARENESS	
1.7 Determine if the institution has a reasonable overall Year 2000 strategic plan that, at a minimum, discusses its Year 2000 program management structure, reporting requirements (when and to whom), timeframes and sequencing of Year 2000 efforts, and on an institution-wide basis, what solutions will be used to achieve Year 2000 compliance.	
1.8 Determine if management provides the board of directors, on at least a quarterly basis, status reports detailing the institution's Year 2000 efforts, particularly internal corrective efforts and the ability of the institution's major vendors or servicers to provide Year 2000-ready products and services.	
1.9 Determine if the institution established a committee or other mechanism to ensure Year 2000 efforts are communicated and coordinated among departments institution-wide.	
GENERAL - ASSESSMENT	
1.10 Determine if management has conducted an assessment of all software, hardware, and environmental systems and other computer-controlled systems including:	
a. Prioritizing the inventoried items and identifying those items deemed to be mission-critical.	
b. Describing the method it plans or has used to renovate non-compliant systems.	

SECTION 1 - GENERAL

1.11 Determine if management has a process established to periodically evaluate prioritized inventory to ensure previously assigned priorities remain accurate.

1.12 Assess if the institution has identified and retained enough qualified staff who can assist the institution in becoming Year 2000 compliant.

GENERAL - AUDIT

1.13 Determine the effectiveness of internal/external audit or other qualified sources' involvement in the Year 2000 process by reviewing whether they have:

a. Evaluated the institution's validation and contingency planning processes for service providers, turnkey systems, end-user applications, in-house developed software, and environmental systems, as applicable.

b. Reviewed and assessed controls over the Year 2000 process, particularly emphasizing the validation and contingency planning processes.

c. Determined if those involved in the Year 2000 process have the knowledge and skills to understand and effectively manage Year 2000 efforts.

d. Independently evaluated the Year 2000 project status and the process for reporting to senior management.

e. Assessed the adequacy of business line management and user involvement.

f. Adequately reported their efforts and findings to the board of directors.

GENERAL - MISCELLANEOUS

1.14 Determine if the institution's legal counsel has performed a legal audit that includes a review of insurance policies, public documents, and new and existing contracts or warranties to ensure that they contain appropriate Year 2000 language.

1.15 Determine if management is aware of or contemplates any litigation related to Year 2000. If litigation is anticipated, note the estimated contingency loss and any reserves established for potential losses.

1.16 Assess the reasonableness of the annual budget established for renovation and testing of mission-critical systems (both hardware and software) to make them Year 2000 compliant. Note the amount budgeted for the Year 2000 effort.

1.17 Determine if documentation relating to the institution's Year 2000 compliance efforts has been retained.

1.18 Review the institution's due diligence process for any merger or acquisition plans that may impact the institution's Year 2000 readiness.

SECTION 1 - GENERAL

1.19 Determine if the institution has mission-critical software package(s) or applications that are supported by non-U.S. domiciled companies.

a. If so, note whether a supervisory authority in the company's home country reviewed, or is scheduled to review, the applications or software packages for Year 2000 compliance. If a review has been conducted, note the results.

1.20 Determine if management has assessed the financial and operational capabilities of its hardware and software vendors to provide Year 2000 processing capabilities.

GENERAL - YEAR 2000 EXTERNAL COUNTERPARTY, CUSTOMER RISK, AND FIDUCIARY ACTIVITIES

1.21 Determine if systems used to conduct trust activities are included in the institution's Year 2000 project.

1.22 Determine if the institution has adequately evaluated and addressed risks associated with:

a. Holding or managing commercial real estate.

b. Holding or managing closely held firms.

c. Fiduciary and transactional counter parties.

d. Disclosure requirements within the Investment Company Act of 1940 and the Investment Advisors Act of 1940.

1.23 Determine if senior management implemented by June 30, 1998, a due diligence process which identifies, assesses, and establishes controls for Year 2000 risk posed by customers such as funds takers, funds providers, and capital market/asset management counter parties and whether this process includes:

a. Identifying material customers.

b. Evaluating their Year 2000 readiness.

c. Assessing their Year 2000 risk to the institution.

d. Implementing appropriate controls to manage and mitigate their Year 2000-related risk to the institution.

1.24 Determine if management will have an assessment of individual customers' Year 2000 preparedness and the impact on the institution substantially complete by September 30, 1998.

1.25 Determine if management's review of the adequacy of the loan and lease loss allowance includes Year 2000 customer risk.

1.26 Assess whether the institution has taken measures to mitigate liquidity risk associated with potential customer withdrawal of funds before or after the century rollover. If so, describe.

SECTION 1 - GENERAL

GENERAL - YEAR 2000 CUSTOMER AWARENESS	
1.27 Describe what the institution has done to inform its customers of its Year 2000 readiness.	

SECTION 2 - RENOVATION

This section is designed to determine whether the institution will complete Year 2000 renovations using methods consistent with safe and sound practices. The renovation phase evaluates Year 2000 code enhancements, hardware and software upgrades, system replacements, and other associated changes. For institutions relying on outside service providers or software vendors, ongoing discussions and monitoring of vendor progress will be necessary.

WORK STEPS

2.1 Review the renovation section of the institution's Year 2000 project plan.

2.2 Review correspondence to/from the institution's service provider/software vendor.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL	
2.3 Determine if an adequate process has been established to track renovation efforts of internal mission-critical systems and external systems which interface with mission-critical systems.	
2.4 Determine if the institution has ensured that any replacement products (hardware and software) are Year 2000 compliant or will be Year 2000 compliant within acceptable timelines.	
2.5 Determine if the institution has communicated date format changes with external entities with which it exchanges data.	
LARGE OR COMPLEX ORGANIZATIONS	
2.6 Verify that the institution has implemented change control procedures to ensure all modifications to information systems and their components are properly documented and managed.	
2.7 Determine if the organization has a systems-development life cycle that provides adequate controls over the renovation phase of the Year 2000 process.	
2.8 If vendor technicians and outside consultants are being used, determine if they are subject to the same policies and controls as in-house staff.	

SECTION 3 - VALIDATION

This section is intended to determine the adequacy of the institutions' compliance with guidance and accepted procedures for validating mission-critical hardware, software, and environmental systems for Year 2000 readiness. It is the responsibility of the board of directors and senior management to ensure that Year 2000 risks are effectively evaluated and managed. The most critical phase of the Year 2000 readiness process is validation. For further guidance, refer to the FFIEC Guidance Concerning Year 2000 Readiness.

WORK STEPS

3.1 Obtain and review a list of mission-critical systems (e.g., hardware, software, networks, and environmental) noting if systems are developed in-house, or obtained from a turnkey software vendor or service provider.

3.2 Obtain and review the Year 2000 validation policies, practices, or procedures.

3.3 Obtain and review a copy of the validation strategies and plans for the various information processing environments.

3.4 Obtain and review the definition the institution is using for Year 2000 compliance.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL	
3.5 Determine if the institution has met or will meet the following key milestones in the Year 2000 validation process:	
a. June 30, 1998 - complete the development of their written validation strategies and plans.	
b. September 1, 1998 - commence validation of internal mission-critical systems, including those programmed in-house and those purchased from software vendors.	
c. December 31, 1998 - validation of internal mission-critical systems should be substantially complete. Service providers should be ready to test with customers.	
d. March 31, 1999 - validation by institutions relying on service providers for mission-critical systems should be substantially complete. External testing with material third-parties should have begun.	
e. June 30, 1999 - validation of mission-critical systems should be complete and implementation should be substantially complete.	
3.6 Determine if the written validation strategy and plan for internal and external systems includes:	
a. A description of the testing environment.	
b. Testing methodology (e.g., test scripts, development of test data, proxy testing).	
c. Testing schedules.	
d. The allocation of human and financial resources.	
e. Testing of relevant critical dates.	
f. Documentation of test results.	
g. Testing hardware and software deemed compliant during the assessment phase.	

SECTION 3 - VALIDATION

	h. Integration testing between the institution's internal systems and interfaces with external entities (foreign and domestic service providers, software vendors or other third-parties) as applicable.
	i. Requirements for user participation.
3.7	Assess the adequacy of the institution's Year 2000 testing policies, practices, or procedures including, but not limited to:
	a. Reporting the status of Year 2000 efforts to the board of directors on at least a quarterly basis.
	b. Routine management reporting (e.g., metrics) to assess the status of testing efforts.
	c. Testing mission-critical systems first for business continuity purposes.
	d. Maintenance of sound internal controls over the testing process.
	e. Requirements for comprehensive testing (baseline, future date, user acceptance, point-to-point, and end-to-end) and system-level reporting to management of significant deviations from the testing methodology as applicable.
3.8	Determine if the institution has:
	a. Retained management and staff with appropriate technical knowledge and skills to manage the Year 2000 testing process.
	b. Identified staffing and training needs for those involved in Year 2000 testing.
	c. Allocated resources (hired, trained, or engaged employees) to perform and analyze tests.
3.9	Review management's process for scoping testing activities and determine whether the process involves or considers:
	a. Reviewing the inventory of mission-critical applications and identifying the method used to renovate these applications, such as windowing (including pivot years), date expansion, etc.
	b. Compiling a list of the delivery dates for compliant versions of all software developed in-house or obtained from third-parties.
	c. Identifying any custom code or features in third-party software.
	d. Documenting the network connections and telecommunications dependencies and determining their effect on testing.
	e. Documenting the functions, commands, features, transactions, user interfaces, internal/external interfaces, and data files associated with each mission-critical application.
	f. Reviewing each mission-critical application to document the application's business or calendar rules.
3.10	Determine the adequacy of the institution's definition of Year 2000 compliance.

SECTION 3 - VALIDATION

3.11	Determine if management's scoping process included testing procedures designed to test all provisions of the organization's Year 2000 compliance definition.
3.12	Verify management reviewed the FRB century date change bulletins and determined testing strategies for programs which interface with a Federal Reserve Bank, if applicable.
3.13	Determine if the testing scope includes testing equipment and hardware with embedded microchips.
3.14	Determine if the institution has taken steps to prevent contamination or corruption of operational systems and related databases during and after the testing process.
3.15	Review the Year 2000 validation process the institution has/will perform for its mission-critical systems and determine if the following types of tests, defined in the Interagency Guidance Concerning Testing for Year 2000 Readiness, are conducted as applicable:
	a. Baseline.
	b. Future date.
	c. User acceptance.
	d. Point-to-point.
	e. End-to-end.
3.16	Has the institution determined and tested the relevant critical dates necessary to ensure Year 2000 readiness of its mission-critical systems?
3.17	Determine if the institution tests internal and external interfaces.
3.18	Select a sample of test documentation for mission-critical systems and determine if an adequate audit trail exists to support the institution's Year 2000 testing process. Documentation should include:
	a. Year 2000 readiness criteria.
	b. Types of tests performed (e.g., baseline, user acceptance).
	c. Description of the tests noted above.
	d. Results of tests.
	e. Individuals responsible for acceptance testing.
3.19	Determine whether the institution has or plans to conduct point-to-point testing of mission-critical applications with third-parties with whom it does business, including:
	a. Business partners.
	b. Other institutions.
	c. Payment systems providers.

SECTION 3 - VALIDATION

	d. Clearinghouses.
	e. Customers.
	f. Telecommunications vendors.
3.20	Determine if the institution has or plans to participate in end-to-end testing for transactions of mission-critical systems such as electronic payments.
3.21	Determine whether the evaluation of the testing process included participation by:
	a. Project managers.
	b. System owner/end users.
	c. Independent third-parties (internal/external auditors or other qualified sources).
3.22	Discuss procedures management has in place to ensure test data and test input is retained for testing future releases of the software.
3.23	Evaluate the institution's processes to test that its systems remain Year 2000 compliant following enhancements or modifications. (Clean Management)
SERVICED INSTITUTIONS	
3.24	Determine if the institution is coordinating Year 2000 testing with its service providers.
3.25	Evaluate whether the institution has obtained sufficient information to determine if its mission-critical service providers have successfully tested products and services to ensure Year 2000 readiness.
3.26	If the institutions is using proxy testing, determine if management has analyzed the applicability of proxy testing to their institution.
3.27	If proxy testing is used, determine if the institution reviewed and/or provided input to the test scripts used by the user group.
3.28	Evaluate the institution's process for assessing the testing results provided by the party conducting a proxy test.
3.29	Assess the effectiveness of the institution's testing of internal and external interfaces unique to its technology environment and any custom code.
TURNKEY INSTITUTIONS	
3.30	Determine how the institution is coordinating Year 2000 testing with its software vendor.
3.31	Assess whether the institution has determined that mission-critical software vendors have successfully tested their products and services to ensure Year 2000 readiness.

3.32	Determine if the institution has joined forces with other institutions using products from the same software vendor, by participating in or relying on user group testing.
3.33	If user group testing is used, determine if the institution has evaluated the applicability of the user group test environment to the institution's production environment.
3.34	If user group testing is used, determine if the user group test has independence from the software vendor.
3.35	If user group testing is used, has management reviewed the scope of the test to ensure the factors in examination procedure 3.9 are adequately addressed. If these factors are not addressed, determine whether management has plans in place to address the remaining risks.
3.36	Evaluate the institution's process for assessing the testing results provided by the user group.
3.37	Determine if the institution has developed its own independent test plan incorporating results of the software vendor's Year 2000 testing efforts.
3.38	Verify that a Year 2000-compliant version of the operating system has been installed in the testing environment.
3.39	Review management's plans for using either a date simulation tool or IPL (booting) the system to advance the system clock to future dates. Assess whether these plans allow for an adequate test of the operating system.
3.40	Review management's plans or procedures for establishing a future date testing environment. Determine if these plans or procedures address the following issues:
	a. User password expiration.
	b. Data file and database expiration.
	c. Software license expiration.
	d. System authorizations/protections expiration.
	e. Aging test data files.
	f. The job scheduling function.
	g. Archived data.
	h. Automated housekeeping functions.
	i. Internal logging and diagnostic functions.
	j Other devices attached to the system.
3.41	Review management's procedures for returning the system from a post-dated environment.
LARGE OR COMPLEX ORGANIZATIONS	

SECTION 3 - VALIDATION

3.42	Describe the organization's process for evaluating and selecting automated testing tools.
3.43	Discuss the organization's program for training employees on validation techniques and the use of testing tools.
3.44	Review the testing plan to determine the methods the organization will use to validate that Year 2000 remediations have not adversely affected the application's structural integrity including:
	a. Stress-testing the application to determine if there are any changes to the minimum system configuration requirements.
	b. Testing the application's ability to recover from error conditions or system crashes.
3.45	Review the testing plan to determine the methods the organization will use to validate that Year 2000 remediations have not adversely effected the application's functional integrity, and determine if the plan includes:
	a. Baseline testing.
	b. Unit testing.
	c. Integration testing.
	d. Regression testing.
	e. Point-to-point testing.
	f. End-to-end testing.
	g. User acceptance testing.
	h. Consumer compliance testing.
3.46	Review the testing plan to determine the methods the organization will use to validate that applications will operate in a post-Year 2000 environment.
3.47	Determine if the compliant version of the operating system has been installed in the testing environment.
3.48	Review management's plans for using either a date simulation tool or IPL (booting) the system to advance the system clock to future dates. Assess whether these plans allow for an adequate test of the operating system.
3.49	Review management's plans or procedures for establishing a future date testing environment. Determine whether these plans or procedures address the following issues:
	a. User password expiration.
	b. Data file and database expiration.
	c. Software license expiration.
	d. System authorizations/protections expiration.

SECTION 3 - VALIDATION	
e. Aging test data files.	
f. The job scheduling function.	
g. Archived data.	
h. Automated housekeeping functions.	
i. Internal logging and diagnostic functions.	
j Other devices attached to the network.	
3.50 Review management's procedures for returning the system from a post-dated environment.	
3.51 Describe the organization's procedures for selecting contractors, and managing contractors and projects contracted to third-parties.	
3.52 Review the organization's procedures for ensuring program changes initiated concurrently with the renovation and testing phases are adequately tested and synchronized into the compliant versions of the programs.	
3.53 If the organization acts as a servicer or vendor, determine whether they will (have) share(d) the information generated in the test scoping process with the client institutions.	

SECTION 4 - IMPLEMENTATION

During a review of the implementation phase, examiners should focus on the adequacy of management's implementation plan and internal controls governing the migration process. During the implementation phase, systems should be verified as Year 2000 compliant and be accepted by the business users. Any potentially noncompliant mission-critical system should be brought immediately to the attention of executive management for resolution. In addition, this phase must ensure that any new systems or subsequent changes are compliant with Year 2000 requirements.

WORK STEPS

4.1 Review the implementation portion of the institution's Year 2000 project management plan.

4.2 Obtain and review a copy of the institution's implementation schedule, if it is not included in the project management plan.

4.3 Obtain and review updated disaster recovery and contingency plans as well as business resumption plans.

4.4 Review correspondence between the service provider or software vendor and its user institutions.

4.5 For large or complex organizations, review the integration phase of the organization's system development life cycle.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL	
4.6 Determine if the institution's plan/process for the implementation of converted or replaced applications and/or system components into the institution's production environment includes:	
a. An assessment of the adequacy of system capacity and DASD/tape storage requirements.	
b. Implementation procedures (steps for getting the program into the production environment and steps for database and archive conversion).	
c. Implementation dates.	
d. Audit review of changes and/or change methodology.	
e. Documented sign-off by management and users.	
f. Methods the organization will use to validate the conversions of existing data files and databases.	
4.7 Determine if management coordinated the institution's implementation schedule with outside entities with which electronic data is exchanged.	
4.8 Determine if the institutions's implementation plan provides for the use of data bridges and filters, where applicable, to allow for the continued exchange of information between compliant systems, non-compliant systems or systems renovated using different date format methods.	
4.9 Determine if adequate controls have been established over the implementation process, and if this process is being applied to Year 2000-related changes.	
4.10 Determine if system security features have been compromised or removed due to Year 2000 renovations.	

SECTION 4 - IMPLEMENTATION

4.11 Determine if management has procedures in place to correct program-related faults discovered after implementation and retest those programs after corrections are made.	
4.12 Determine if the following items have been updated to reflect any changes resulting from Year 2000 modifications:	
a. Balancing procedures.	
b. User training programs.	
c. Documentation (user manuals, system manuals, etc.).	
d. Items maintained in off-site storage (application programs, operating system, documentation, etc.).	
4.13 Verify that balancing procedures have been established to address the verification of post-conversion output.	
TURNKEY INSTITUTIONS	
4.14 Review management's efforts to ensure that all applicable hardware and software at the contracted back-up site has been updated to match Year 2000 compliant versions being used by the institution.	
4.15 If the institution has source code in escrow, determine whether the institution received independent verification that the most recent version of the compliant product is being held in escrow.	
LARGE OR COMPLEX ORGANIZATIONS	
4.16 Review management's efforts to ensure that all applicable hardware and software at the contracted back-up site has been updated to match Year 2000 compliant versions being used by the institution.	
4.17 Determine if internal controls governing the change control process are being applied to the Year 2000 project.	
4.18 Determine if the organization can recover its production system in the event newly renovated applications fail during the implementation process.	

SECTION 5 - CONTINGENCY PLANNING

This section reviews the institution's plans to address remediation and business resumption risks to core business functions that rely on mission-critical systems. Objectives are to determine: 1) that institution management has developed, tested, and implemented contingency plans; 2) whether contingency plans focus on core business functions that pose the greatest risk if lost or seriously compromised by Year 2000 related system failures; and 3) that remediation and business resumption contingency plans contain viable timelines. For further guidance, examiners should reference the Interagency Statement entitled Guidance Concerning Contingency Planning in Connection with Year 2000 Readiness.

WORK STEPS

5.1 Obtain and review any reports or documents provided to the board of directors or senior management pertaining to Year 2000 remediation contingency and business resumption contingency planning.

5.2 Obtain and review a sample of risk analyses developed for core business functions.

5.3 Obtain and review a copy of a report showing the renovation/testing status of all mission-critical systems.

5.4 Obtain and review a copy of the institution's Year 2000 remediation contingency and business resumption contingency plans.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL	
5.5 Determine if the board of directors and senior management have assigned responsibility to appropriate personnel for developing and maintaining a Year 2000 contingency plan.	
5.6 Determine if a process has been established to report progress and changes in the Year 2000 readiness plan to the board of directors and senior management.	
5.7 Determine if contingency planning focuses on identifying, restoring, and continuing core business functions and mission-critical systems that pose the greatest risk to the institution.	
5.8 Determine how Year 2000 contingency planning is coordinated with existing contingency and business resumption plans.	
5.9 Determine if contingency planning for mission-critical systems addresses both remediation contingency planning and business resumption contingency planning.	
5.10 Determine if the organization has identified all customer links into its systems, and addressed such links in the organization's contingency and business resumption planning.	
5.11 Evaluate whether the **remediation contingency plan** includes:	
a. Possible alternative solutions, including the consideration of alternative software vendors or service providers, in the event remediation efforts are not successful.	
b. Trigger dates for activating an alternative plan, taking into account the time needed to deploy alternative solutions.	
c. Functionality of alternative solutions.	
5.12 Evaluate whether the **business resumption contingency plan** addresses the following:	

	a. Assignment of responsibility to an individual or team for implementing the business resumption plan.
	b. Development of a specific recovery plan for each core business process.
	c. A master list of customers, clients, suppliers, institutions, and government agencies that share data with the institution.
	d. Documentation of products necessary for recovery including machine-readable copies of master and transaction files, printed trial balances, and electronic-text format copies of all master files and trial balance reports.
	e. Printouts of transactions received but not posted as of year-end (e.g., Fed letter, ACH warehouse, ATM).
	f. If environmental systems, hardware, and software at the back-up site are Year 2000 compliant.
	g. If manual processing is to be relied on as a back-up measure, whether the institution has written manual processing procedures to follow and whether they are a viable option.
	h. If key personnel are trained to implement the resumption plan.
5.13	Evaluate how the institution has verified that its designated back-up site has adequate capacity for its potential Year 2000 demands.
5.14	**Validation of the Business Resumption Contingency Plan**
	a. Determine the adequacy of the method used, or planned to be used, to validate or test the business resumption contingency plan.
	b. Determine that validation or test strategies adequately cover all core business processes.
	c. Identify the party who is responsible for executing the test or validating the plan.
	d. Determine the adequacy of test objectives and scope.
	e. Determine the institution's documentation requirements for business resumption contingency plan testing.
	f. Determine the adequacy of the process for updating the business resumption contingency plan.

SECTION 5 - CONTINGENCY PLANNING

SERVICED/TURNKEY INSTITUTIONS		
5.15	Determine if the institution's remediation and business resumption contingency plans are consistent with those of its third-party software vendor or service provider.	
LARGE OR COMPLEX ORGANIZATIONS		
5.16	Determine if the description of core business processes distinguishes between the servicer's internal processes and the mission-critical functions of its client institutions.	
5.17	Identify how the organization has assigned roles and responsibilities for maintaining client contacts during the business resumption process.	
5.18	Describe the organization's efforts to communicate its Year 2000 remediation contingency and business resumption contingency plans to its client institutions.	
5.19	Identify how the organization arrived at an understanding with its client institutions as to the minimum service levels to be maintained in a contingency environment.	
5.20	Determine if the organization's contingency plan addresses the restoration of these minimum service levels.	
5.21	Describe the steps taken by the organization to ensure continued service for client institutions if telecommunications or power problems are experienced.	
5.22	Describe the provisions that have been made for testing contingency plans and processes relating to Year 2000 and the services provided to client institutions.	
5.23	Determine if the organization has clearly identified the type of business resumption plan testing to be used for each core business process.	
5.24	Evaluate whether adequate provisions have been made to provide a copy of master files and trial balances as of year-end 1999 in an electronic format to all serviced client institutions.	

SECTION 6 - EXAMINATION CONCLUSIONS

Questions in the Examination Conclusions section are designed to narrow the examiners focus to the primary risk areas associated with the final phases of the Year 2000 project as well as concerns in the areas of Year 2000 indirect risk. Responses should be well documented within the workpapers which accompany this Workprogram. Items detailed below should be addressed within comments prepared for the Report of Examination or Visitation Memorandum resulting from the current on-site review.

		COMMENTS
Develop summary comments for the open section of the report of examination/visitation memorandum. Comments should address the following topics:		
6.1	Assign an overall Year 2000 rating to the institution/organization based on the findings of the review.	
6.2	Describe whether the institution has a formal Year 2000 project plan, if the plan is reasonable, and if the institution is following the plan.	
6.3	Note whether the institution's Year 2000 project plan establishes reasonable and attainable deadlines that will enable the institution to meet the key milestone dates set forth in the Interagency Statement on Guidance Concerning Testing for Year 2000 Readiness.	
6.4	Provide a brief description of the institution's reporting structure, including frequency, in relaying Year 2000 compliance efforts to the board of directors.	
6.5	Address the institution's efforts to monitor the progress of its service providers and software vendors in becoming Year 2000 compliant.	
6.6	Discuss whether data-processing service provider(s) or software vendor(s) have plans to deliver a remediated product which will allow the institution to test within the key milestone dates set forth in the Interagency Statement on Guidance Concerning Testing for Year 2000 Readiness.	
6.7	Provide a brief description and assessment of the institution's testing methodology.	
6.8	Provide an assessment regarding the adequacy of the institution's test plan.	
6.9	Describe if the institution has adequate remediation and business resumption contingency plans.	
6.10	Briefly describe management's plan to address indirect Year 2000 risks such as those associated with counter parties, customers, and fiduciary activities.	
6.11	Describe efforts implemented by the institution towards making customers aware of its Year 2000 efforts.	
6.12	Discuss any major problems which are anticipated by management, towards achieving Year 2000 compliance.	
6.13	List the name(s) of individuals responsible for the institution's Year 2000 efforts, particularly the designated Year 2000 project manager, and describe their status in the organizational structure.	

SECTION 6 - EXAMINATION CONCLUSIONS

6.14	Detail any exceptions or weaknesses noted with the institution's Year 2000 compliance program. Provide management's response detailing commitments for corrective action.	
6.15	Detail efforts made by management to correct deficiencies noted at prior reviews or note previous deficiencies which still remain unresolved.	
6.16	State whether the institution has managed its Year 2000 business risk and contingency planning efforts in a safe and sound manner.	
6.17	List the names and titles of management members with whom Year 2000 findings were discussed.	
6.18	State whether Year 2000 examination results were discussed with the board of directors, if applicable, or a designated committee thereof.	
The following areas should be discussed in the confidential section of the report of examination or visitation memorandum as appropriate:		
6.19	Detail recommendations for follow-up action or recommendations for enforcement action. If enforcement action is recommended, contact the appropriate management official for your regulatory agency.	
6.20	For bank and non-bank service providers and software vendors, prepare a list of serviced institutions which are currently under contract with that provider. Include name, city, state, and charter type.	
6.21	List serviced or turnkey institutions which according to the servicer or vendor will need to take specific action, such as a conversion or upgrade, to achieve Year 2000 compliance.	