NCUA LETTER TO FEDERALLY INSURED CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: December 1, 1997 **LETTER NO.: 97-CU-10**

TO: CHAIRMAN OF THE SUPERVISORY COMMITTEE
ALL FEDERALLY INSURED CREDIT UNIONS

SUBJECT: Supervisory Committee's Role in Year 2000 Compliance

The supervisory committee has a critical role in the success of Year 2000 initiatives, and it is this role we want to address.

We previously issued to all federally insured credit unions two *letters to credit unions* dealing with Year 2000 compliance: Letter No. 96-CU-5 dated August 16, 1996, and Letter No. 97-CU-6 dated June 3, 1997. These letters are enclosed.

Both letters alerted credit unions to the substantial risks represented by the programming code in existing computer systems as we enter the new millennium. Virtually every organization will have its computing operations affected in some way by the roll over of the two digit year value from "99" to "00". We strongly urged boards of directors and senior management to achieve Year 2000 compliance by performing a high level risk assessment of how systems are affected, followed by the development of a detailed action plan to timely address the problems. The supervisory committee plays a critical role in the credit union's success.

Under §701.12 of the NCUA Rules and Regulations, the supervisory committee must ensure that the financial condition of the credit union is accurately and fairly presented in the credit union's financial statements; and the credit union's management practices and procedures are sufficient to safeguard members' assets. To meet these responsibilities, §701.12(b)(2) sets forth four requirements. The first, dealing with ensuring internal controls are sufficient to meet financial reporting objectives, and the fourth, dealing with policies and control procedures sufficient to safeguard against error and carelessness, are the most relevant to the Year 2000 discussion.

During your next annual supervisory committee audit, but even more importantly now in interim periods, an assessment of the credit union's progress and testing of the implementation of Year 2000 modifications is critical. It is your immediate responsibility to assess the board and management on their success in:

- Developing a risk assessment that identifies systems and applications that must be modified, such as, mainframes, personal computers, networks, telephones and PBX systems, audio

voice systems, fax machines, elevators, security systems (vaults, badge readers, surveillance systems, etc.).

- Identifying the segments of computer systems that must be modified.

- Identifying and testing the various interface linkages between communication systems, software packages, and delivery systems.

- Evaluating various alternatives (determining which applications that should be redeveloped, replaced, or modified).

- Estimating costs for modifications.

- Reviewing, approving, and establishing milestones to ensure the timely completion of their institution's millennium plan.

- Ensuring that new systems are Year 2000 compliant.

- Planning, developing and putting into place an adequate contingency plan for critical systems (fall back position) in the event of catastrophic conditions.

If your review leads you to assess that the credit union lacks the necessary expertise to comply with the above requirements, you need to make a written recommendation that the board seek help from outside resources and periodically follow-up on that recommendation. During regulatory and insurance examinations, as applicable, we will be looking for the committee's review and oversight of the credit union's Year 2000 initiatives.

Later this year, NCUA will publish and issue a self-analysis guide which credit union management can use to measure successful Year 2000 implementation. This Guide will be a resource for the supervisory committee, as well. Enclosed you will find the examination procedures that NCUA examiners will employ in evaluating credit union Year 2000 compliance. Additionally, the AICPA has issued a document which may be helpful to you, "*The Year 2000 Issue: Current Accounting and Auditing Guidance*" -- it is available through the AICPA or via their homepage on the worldwide web at www.aicpa.org.

The integrity and success of your credit union will depend on cooperation and timely efforts to meet Year 2000 concerns. If, even with your best efforts, the credit union's board or management continues to defer dealing with Year 2000 concerns, you may contact your supervising NCUA regional director or state supervisory authority.

Sincerely,

/S/

Norman E. D'Amours
Chairman

Enclosures

SERVICED INSTITUTIONS AND TURNKEY ENVIRONMENTS

EXAMINATION OBJECTIVES

YEAR 2000 DATE CHANGE PROBLEM

1. To determine if the institution has an effective plan for identifying, correcting, testing, and implementing solutions necessary for Year 2000 processing.

2. To assess the impact of Year 2000 effort on the institution's strategic and operating plan.

3. To determine if the institution has effectively coordinated Year 2000 processing capabilities with its customers, vendors, and payment systems partners.

4. To assess the soundness of internal controls over the Year 2000 process.

5. To identify situations where further corrective action may be necessary to assure an appropriate level of attention to Year 2000 processing capabilities.

INTRODUCTION

The following work program procedures are intended for serviced institutions and turnkey environments. The examination procedures will help the examiner in determining if the institution is addressing or has successfully addressed the Year 2000 date change and associated problems inherent in many computer software and hardware systems. The examination procedures are designed to focus on the state of Year 2000 preparedness of each examined institution.

EXAMINATION PLANNING AND CONTROL

1. Determine the institution's source of Information Systems (IS) support for hardware (mainframe, mid-range, networks, personal computers) and related applications and operating system software. Note if the information systems processing is provided internally, externally, or a combination of both.

2. Review previous examination, audit, or consultant findings relative to Year 2000 issues.

3. Review management's responses to any significant Year 2000 findings.

4. Determine the scope of the Year 2000 examination based on findings from the steps above and discussions with the EIC.

Select from the following examination procedures the steps necessary to meet those objectives. Note: Examinations do not require completion of all steps.

EXAMINATION PROCEDURES

1. Determine if the institution's board of directors and senior management are aware, and understand the risks and complexities, of the Year 2000 problem.

    a) Obtain and review minutes of board of directors meetings for discussions of Year 2000 issues.
    b) Obtain and review minutes of committees established to address Year 2000 issues.

2. Has management developed a plan to assure the institution's computer systems and any interfacing computers and networks are Year 2000 compliant?

3. Determine if the institution's Year 2000 assessment includes computer controlled systems such as ATM's, audio response systems, vaults, security and alarm systems, elevators, telephones, FAX machines, etc.

    a) Has management identified critical and non-critical systems?
    b) Has management prioritized both critical and non-critical systems?

4. Does management have on-going communications with its vendor(s) and/or servicers to determine their progress toward implementing Year 2000 compliance/solutions.

5. Determine if the institution has:

    a) performed a third party software contract review to identify risks associated with licensing and maintenance agreements protections for Year 2000 compliance;
    b) reviewed all data processing outsourcing agreements to determine if the vendors have Year 2000 maintenance obligations; and
    c) a process in place that certifies that a vendor(s) and products(s) are Year 2000 compliant. If so, describe.

6. Determine if management has assessed the financial and operational capabilities of their hardware and software vendors to provide Year 2000 processing capabilities. Note the results of this assessment.

7. Determine the status of the Year 2000 project including any anticipated barriers and how management plans to address these barriers.

8. If it is evident that the institution's or vendor/servicer's systems are not fully Year 2000 capable:

    a) determine if all critical applications will be Year 2000 capable and fully tested by December 31, 1998;
    b) determine which significant applications will not be Year 2000 capable and fully tested by December 31, 1998;
    c) has management anticipated the impact to the institution's operation in the event that all systems will not be Year 2000 capable by December 31, 1998; and
    d) if the institution's systems will not be Year 2000 compliant by December 31, 1998, determine what steps management is taking to assure the institution's ongoing operations.

9. Has management discussed the impact of the Year 2000 issue with its customers to assure customers' ability to meet financial and informational obligations to the institution? Will customer PC Banking program interface be an issue, operationally or from a customer service viewpoint?

10. Determine if the institution has assessed the impact of Year 2000 processing capabilities, as applicable, with its payment systems providers including:

    a) wire transfer systems;
    b) automated clearing houses;
    c) check clearing providers;
    d) credit card merchant and issuing systems;
    e) automated teller machine networks;

f) electronic data interchange systems; and
g) electronic benefits transfer systems.

11. Determine if management has assured the soundness of internal controls associated with the Year 2000 effort.

OVERALL CONCLUSIONS

1. If appropriate, discuss the following in the examination report:

   a) the institution's computer system's Year 2000 processing capability;
   b) management's effectiveness in managing the Year 2000 process;
   c) the adequacy of plans for identifying, correcting, testing, and implementing solutions for Year 2000 processing;
   d) the status of the plan and the capability to complete necessary changes by December 31, 1998;
   e) management's effectiveness in coordinating Year 2000 processing capabilities with their hardware and software vendors, customers, and payment system providers;
   f) the impact of the Year 2000 effort on the institution's strategic and operating plans including earnings, capital projections, and insurance; and
   g) the effectiveness of the audit function and its assessment of internal controls over the Year 2000 process.

2. As appropriate, prepare recommendations for the EIC regarding any additional actions necessary to assure the institution's safety and soundness associated with Year 2000 processing capabilities.

3. Summarize the strengths and weaknesses and reach a conclusion regarding Year 2000 compliance.

4. Discuss the conclusions with the appropriate level of management and document responses.

INSTITUTIONS WITH IN-HOUSE SOFTWARE DEVELOPMENT

EXAMINATION OBJECTIVES

YEAR 2000 DATE CHANGE PROBLEM

1. To determine if the institution has an effective plan for identifying, correcting, testing, and implementing solutions necessary for Year 2000 processing.

2. To assess the impact of Year 2000 effort on the institution's strategic and operating plan.

3. To determine if the institution has effectively coordinated Year 2000 processing capabilities with its customers, vendors, and payment systems partners.

4. To assess the soundness of internal controls over the Year 2000 process.

5. To identify situations where further corrective action may be necessary to assure an appropriate level of attention to Year 2000 processing capabilities.

INTRODUCTION

The following work program procedures are intended for institutions with in-house software development capabilities. The examination procedures will help the examiner in determining if the institution is addressing or has successfully addressed the Year 2000 date change and associated problems inherent in many computer software and hardware systems. The examination procedures are designed to focus on the state of Year 2000 preparedness of each examined institution.

EXAMINATION PLANNING AND CONTROL

1. Determine the institution's source of Information Systems (IS) support for hardware (mainframe, mid-range, networks, personal computers) and related applications and operating system software. Note if the information systems processing is provided internally, externally, or a combination of both.

2. Review previous examination, audit, or consultant findings relative to Year 2000 issues.

3. Review management's responses to any significant Year 2000 findings.

4. Determine the scope of the Year 2000 examination based on findings from the steps above and discussions with the EIC.

Select from the following examination procedures the steps necessary to meet those objectives. Note: Examinations do not require completion of all steps.

MANAGEMENT

1. Determine if the institution's board of directors and senior management are aware, and understand the risks and complexities, of the Year 2000 problem.

    a) Obtain and review minutes of board of directors meetings for discussions of Year 2000 issues.
    b) Obtain and review minutes of committees established to address Year 2000 issues.

2. Has management developed a plan to assure the institution's computer systems and any interfacing computers and networks are Year 2000 compliant?

3. Determine if the institution's Year 2000 assessment includes computer controlled systems such as ATM's, audio response systems, vaults, security and alarm systems, elevators, telephones, FAX machines, etc.

    a) Has management identified critical and non-critical systems?

b) Has management prioritized both critical and non-critical systems?

4. Does management have on-going communications with its vendor(s) and/or servicers to determine their progress toward implementing Year 2000 compliance/solutions.

5. Determine if the institution has:

   a) performed a third party software contract review to identify risks associated with licensing and maintenance agreements protections for Year 2000 compliance;
   b) reviewed all data processing outsourcing agreements to determine if the vendors have Year 2000 maintenance obligations; and
   c) a process in place that certifies that a vendor(s) and products(s) are Year 2000 compliant. If so, describe.

6. Determine if management has assessed the financial and operational capabilities of their hardware and software vendors, including those operating under a facilities management agreement, to provide Year 2000 processing capabilities. Note the results of this assessment.

7. Determine the status of the Year 2000 project including any anticipated barriers and how management plans to address these barriers.

8. If it is evident that the institution's or vendor/servicer's systems are not fully Year 2000 capable:

   a) determine if all critical applications will be Year 2000 capable and fully tested by December 31, 1998;
   b) determine which significant applications will not be Year 2000 capable and fully tested by December 31, 1998;
   c) has management anticipated the impact to the institution's operation in the event that all systems will not be Year 2000 capable by December 31, 1998; and
   d) if the institution's systems will not be Year 2000 compliant by December 31, 1998, determine what steps management is taking to assure the institution's ongoing operations.

9. Has management discussed the impact of the Year 2000 issue with its customers to assure customers' ability to meet financial and informational obligations to the institution?

10. Determine if the institution has assessed the impact of Year 2000 processing capabilities, as applicable, with its payment systems providers including:

    a) wire transfer systems;
    b) automated clearing houses;
    c) check clearing providers;
    d) credit card merchant and issuing systems;
    e) automated teller machine networks;
    f) electronic data interchange systems; and

g) electronic benefits transfer systems.

11. Based on discussions with management and reviews of Year 2000 committee minutes, identify whether management has:

    a) inventoried all hardware and software systems;
    b) developed a risk assessment model identifying hardware and software systems requiring modifications for Year 2000 processing;
    c) evaluated various alternatives for dealing with Year 2000 processing issues;
    d) estimated financial and other resources necessary for Year 2000 modifications;
    e) prioritized software and hardware systems to ensure that the most critical applications are addressed first;
    f) considered all software systems including core banking, investments, fiduciary, management information, retail delivery, operating systems, subsidiary systems, backup systems, etc.;
    g) considered the impact of Year 2000 issues on electronic data transactions throughout the institution;
    h) reviewed and approved milestones to ensure the timely completion of Year 2000 efforts;
    i) developed a testing strategy for Year 2000 modifications;
    j) ensured that any new systems are Year 2000 compliant; and
    k) addressed the establishment and review of an effective system of internal controls over the Year 2000 effort.

12. Has management's assessment of the Year 2000 issue determined:

    a) the type of technical expertise needed;
    b) the amount of time needed for corrective action;
    c) the type and amount of financial resources needed and whether the institution has sufficient financial resources to make all hardware (mainframe, mid-range, networks, personal computers) and related application and operating system software Year 2000 capable;
    d) if any other resources are required;
    e) the budgetary impact for Year 2000 changes; and
    f) the impact of the Year 2000 project on earnings, capital, and liquidity. Does the assessment appear reasonable?

13. Determine if the board of directors and/or senior management have approved and allocated resources, based on project management's (Year 2000 committee) assessments, for addressing Year 2000 issues including:

    a) establishing appropriate Year 2000 budgets;
    b) assigning adequate numbers of competent and skilled project managers and staff to accomplish the effort; and
    c) requiring thorough project management techniques including periodic senior management and board project updates.

14. Determine if the institution has individuals, or access to individuals, with sufficient technical expertise to make all hardware and software systems Year 2000 compliant.

    a) If outside resources will be used, are these resources under contract?
        i) If not, what assurances does management have that these resources will be available when needed?

15. Determine how the board of directors and senior management are updated on the progress of Year 2000 efforts.

16. Determine if the board of directors and/or senior management has established clear lines of authority and responsibility for the Year 2000 effort.

17. Determine if Year 2000 project teams receive sufficient support from the board of directors and senior management.

18. Describe the institution's planning schedule including time frames for completing major steps necessary for Year 2000 processing. Does the schedule appear reasonable?

19. As applicable, review the selection process for any Year 2000 service provider(s). Does the process appear adequate?

20. Determine if management has developed an adequate Year 2000 conversion management process and procedure and whether the process considers:

    a) who will perform the work;
    b) institution of the conversion or development process;
    c) use of outside resources;
    d) which programming languages and tools the institution will use;
    e) whether a common application development platform is required;
    f) whether specific date conversion methodology is required;
    g) the type and extent of testing required;
    h) the establishment of priorities;
    i) grouping of systems for conversion;
    j) quality assurance;
    k) the role of end users;
    l) the need for a configuration management plan; and
    m) controls over project management.

AUDIT

1. Assess (internal and external) audit personnel's independence and involvement in reviewing the institution's Year 2000 efforts.

2. Review audit plans and budgets through 1999 and determine if they include the identification of specific audit resources necessary to review Year 2000 issues. Also, determine if these plans are based on a formal inventory of all critical systems impacted by Year 2000 issues.

3. Determine if auditors are actively involved in Year 2000 efforts to assess and monitor the effectiveness of the project management process and soundness of related internal controls. Is audit management communicating this information to the board of directors?

4. Review Year 2000 project audit reports and determine the adequacy of their scope and the timeliness and completeness of management responses. Also assess the appropriateness of audit follow-up on actions taken in response to Year 2000 project audit findings.

SYSTEMS AND PROGRAMMING

1. Evaluate the adequacy and level of experience of internal and external software development personnel to address Year 2000 issues and determine any impact on operating plans.

2. Has the institution determined that the computer system environment is adequate to support the implementation of software changes? If so, describe.

3. Determine which method(s) the institution is using or will use to resolve Year 2000 date calculations (e.g. conversion to four position year fields, windowing, etc.). Note, a combination of methods may be utilized.

4. Has the institution determined the software development function's ability to have Year 2000 software changes in effect by December 31, 1998. If so, describe.

5. Has/will the institution devote(d) appropriate time to testing and error checking of all software changes?

6. Determine if the institution has software development resources necessary to respond to Year 2000 issues associated with various computing environments including mainframes, mid-range, networks, and personal computers.

7. Obtain a list of programming tools that the institution is, or will be, using to fix the Year 2000 problem(s). Examples of the tools may include software inventory, cost estimation, Year 2000 date reference identification, altering of dates, impact analysis, editors, debuggers, code generators, testing and systems conversion, etc. Have the institution describe the tools.

8. Describe how the institution will maintain sound internal controls over the software change

process for Year 2000 issues.

9. Determine if the institution has/will be coordinating modification and testing activities with vendors, servicers, and institutions with whom critical data is received or sent.

COMPUTER OPERATIONS

1. Review management's assessment of the institution's anticipated systems resources required specifically for operating systems, telecommunications (including ATM) networks, and security software, to handle Year 2000 processing. Describe the results of the assessment.

2. Does the institution's Year 2000 assessment include determining if adequate computer resources exist for testing Year 2000 changes and performing day-to-day processing activities?

3. Determine if the institution's Year 2000 assessment includes computer controlled devices such as ATM's, audio response systems, vaults, doors, alarms, elevators, security systems, telephones, FAX machines, etc.

4. Describe management's assessment of the impact of any changes in operating practices from the Year 2000 effort.

5. Determine if any interim work procedures are required as part of the Year 2000 effort.

6. Has the institution assessed the impact of Year 2000 efforts on business continuity/recovery planning? If so, describe.

7. Has the institution compromised sound internal controls over operations as a result of addressing Year 2000 issues?

OVERALL CONCLUSIONS

1. If appropriate, discuss the following in the examination report:

   a) the computer system's Year 2000 processing capability;
   b) management's effectiveness in managing the Year 2000 process;
   c) the adequacy of the institution's plans for identifying, correcting, testing, and implementing solutions for Year 2000 processing;
   d) the appropriateness of the date methodology/methodologies selected to provide Year 2000 processing;
   e) the status of the institution's plan and the capability to complete necessary changes by December 31, 1998;
   f) management's effectiveness in coordinating Year 2000 processing capabilities with their hardware and software vendors, customers, and payment systems providers;

g) the impact of the Year 2000 effort on the institution's strategic and operating plans including earnings, capital projections and insurance;
h) the effectiveness of the audit function and its assessment of internal controls over the Year 2000 process; and
i) the impact of the Year 2000 issue on the institution's earnings, capital, and liquidity.

2. Note the date methodology/methodologies (four position year codes, windowing, etc.) the institution uses or plans to use to meet their Year 2000 challenges.

3. As appropriate, prepare recommendations for the EIC regarding any additional actions necessary to assure the institution's safety and soundness associated with Year 2000 processing capabilities.

4. Summarize the strengths and weaknesses and reach a conclusion regarding Year 2000 compliance.

5. Discuss the conclusions with the appropriate level of management and document responses.

Coopers and Lybrand L.L.P.
Washington, DC

.....

NCUA Year 2000 Examination Scope Guide

Serviced Institutions And Turnkey Environments

.....

Presented by
Renell Dixon and Ronni Allen
Computer Assurance Services

October 1997

Coopers and Lybrand L.L.P.
Washington, DC

.....

NCUA Year 2000 Examination Scope Guide

Institutions With In-House Developed-Systems

.....

Presented by
Renell Dixon and Ronni Allen
Computer Assurance Services

October 1997

NCUA YEAR 2000 EXAMINATION AUDIT SCOPE GUIDE
SERVICED INSTITUTIONS AND TURNKEY ENVIRONMENTS

Institution	
Name of Contact	
Phone Number of Contact	
Fax Number of Contact	
Date Interviewed	

Preliminary Review

1. Obtain and review the enterprise schematic that depicts all systems, servicers, vendors, and internal and external interfaces. If an enterprise schematic is not available, determine how management identified all components in possible need of Year 2000 repair and review supporting documentation.

2. Has management identified:
   a) the number of financially significant turnkey applications or applications outsourced to ISVs
   b) the number of these applications that are currently vendor-supported
   c) the number of other significant applications (i.e., PC-based applications) that are packaged and whether these are currently vendor-supported
   d) the number of applications that were developed in-house or modified packages that are critical to the institution
   e) the number of non-critical applications

3. How many of the applications indicated above do management claim is Year 2000 compliant and how many are not or have not yet been confirmed?

4. For those that are considered Year 2000 compliant, how did management make this assessment?

5. Is this assessment based on validation and testing? And did management's validation and testing efforts entail ensuring that date methodologies for interfacing systems have been properly bridged? Review test results.

6. Computer hardware used:

7. Operating system software used:

8. Networks used:

Section I – Examination Planning and Control

Audit Program Step	Findings	W/P Ref.
1. Note to what extent the institution relies on internal sources, external sources, or a combination of both for IS processing.		
2. Review previous examinations, audits (internal or external) or consultant findings relative to Year 2000.		
3. Review and evaluate the current status of any significant Year 2000 findings and recommendations previously reported to management.		
4. How well has management demonstrated an ability to estimate the time, costs and other resources needed to address major projects (i.e., are schedule and cost targets typically overrun) in the past?		
5. Does the institution have and use a project management or cost modeling tool? If so, how comprehensive are the tools and how well are they adhered to?		
6. How were the tools developed or were they purchased?		
7. Based on the Preliminary Review and Questions 1 - 6 above, determine the scope of the Year 2000 examination. Discuss with the EIC.		

Section II - Adequacy of Management Support, Awareness and Monitoring

Objective - To determine if the institution's board of directors and senior management are aware of and understand the risks and complexities of the Year 2000 problem and whether they have demonstrated their support of and willingness to monitor the institution's efforts to ensure Year 2000 compliance.

Audit Program Step	Findings	W/P Ref.
1. Review board of directors and/or senior management meeting minutes to identify discussions of Year 2000 issues.		
2. What is the credit union's board and senior management team's view of the Year 2000 issue? Is it a major concern (typically, the awareness level of the IS community is high while management and the user community's is low)?		
3. Has the institution's management and the board of directors been apprised of the risks associated with the Year 2000 (especially those risks related to hardware and software, vendors, suppliers, and members not being compliant)?		
4. Has management and/or the board approved a budget for the Year 2000 fix? What is the budgeted cost to correct the problem? Does the budget take all components of the fix into consideration? How is management monitoring adherence to or the need to adjust this budget?		

Audit Program Step	**Findings**	**W/P Ref.**
5. By when does the credit union estimate or has the Year 2000 issue already affected its systems?		
6. By when does the credit union estimate that the Year 2000 problem, current or future, will be corrected ?		
7. Has senior management mandated that all other significant projects be put on hold or given consideration only after the Year 2000 issue has been satisfactorily resolved?		
8. Has management anticipated the impact to the institution's operations in the event that all systems are not Year 2000 compliant by December 31, 1998. If all systems will not be compliant by December 31, 1998, what steps will management and the board take to assure the credit union's on-going operations?		
9. Has management and the board reviewed and approved the Year 2000 assessment and prioritization of critical and non-critical systems?		

Section III – Adequacy of Assessment

Objective – To evaluate the adequacy of the Year 2000 risk assessment and the reliability of the cost and time estimates for corrective action.

Audit Program Step	Findings	W/P Ref.
1. Has the credit union performed a Year 2000 assessment? If not, discuss and document the reasons and management's estimation of the assessment start date.		
2.Review the assessment. What does it include? At a very high level, the assessment should include: a) an inventory of all hardware and software systems b) an enterprise schematic and risk assessment model identifying hardware and software systems, interfacing computers, and networks requiring modification, and c) estimated financial and other resources necessary for the fix.		
3. The assessment should also include: a) prioritized software and hardware systems to ensure that the most critical systems are addressed first b) operating systems, telecommunications (including ATM) networks, and security software, c) any interfacing systems, and d) vendor/supplier relationships.		

Audit Program Step	Findings	W/P Ref.
4. Does the assessment include devices with embedded dates such as ATM's, audio response systems, physical security systems (vaults and alarms), elevators, telephones, fax machines, etc.?		
5. Does the assessment address the adequacy of resources (human and information systems) for Year 2000 changes and day-to-day processing activities?		
6. Describe management's assessment of the impact of any changes in operating practices due to the Year 2000 effort.		
7. Has the institution assessed the impact of Year 2000 efforts on business continuity and disaster recovery planning?		
8. Does the assessment estimate how many hours it will take to correct the problem, lines of code affected, estimated costs per line of code, how interfacing systems will handle shared date fields and other information that will be influenced by the Year 2000?		

Audit Program Step	**Findings**	**W/P Ref.**
9. Does the assessment address: a) the amount of time needed for corrective action b) the type and amount of financial resources needed and whether the credit union has sufficient financial resources to make all hardware (mainframe, midrange, networks, personal computers) and related application and operating system software Year 2000 compliant c) any required external resources and associated timing issues d) the budgetary impact of Year 2000 changes and available funding, and e) the impact of Year 2000 project on earnings, capital, and liquidity?		
10. Determine if the credit union has assessed the impact of Year 2000 processing capabilities, as applicable, with the payment system providers, including: a) wire transfer system b) automated clearing houses c) share draft processors d) credit card merchant and issuing systems e) automated teller machine networks f) electronic benefits transfer systems (internal and external).		

Audit Program Step	Findings	W/P Ref.
11. Has the institution determined whether it has the individuals, or access to individuals, with sufficient technical expertise to make all hardware and software systems Year 2000 complaint? If so, does the assessment address incentive and bonus programs required to retain in-house technical experts and recruit additional resources, if needed?		
12. If outside resources will be used, are these resources under contract? If not, what assurances does management have that these resources are available?		

Section IV – Project Management

Objective – To determine if the institution has developed an effective plan for identifying and correcting information system components in need of repair to ensure Year 2000 compliance.

Audit Program Step	Findings	W/P Ref.
1. Who is the Year 2000 project manager? What was his/her role prior to becoming the project manager? How is he/she managing and monitoring the project? What project management tools/reports is he/she using? Are the tools adequate?		
2. If a formal Year 2000 project or assessment is not in progress, discuss and evaluate the credit union's strategy for addressing the issue.		

Audit Program Step	**Findings**	**W/P Ref.**
3. Obtain, review and evaluate project team minutes addressing the Year 2000 issue. Does the documentation support actions taken or planned to ensure Year 2000 compliance?		
4. Determine the status of the Year 2000 project including anticipated barriers and how management plans to address these barriers.		
5. Given management's estimation of when the Year 2000 issue will affect its systems, evaluate whether the current status of the project or management's plans to address barriers provide reasonable assurance that all related matters will be addressed.		
6. Does management have on-going communications with its vendor(s) and/or ISV to determine their progress toward implementing Year 2000 compliance solutions? Has management considered alternative resources such as vendor/ISV websites, other credit unions, and agency automated tracking system?		
7. Obtain any written correspondence between the institution and its vendors and/or servicer providers regarding Year 2000 compliance.		

Audit Program Step	Finding	W/P Ref.
7. Determine if the institution has a) performed a third-party contract review to identify risks associated with licensing and maintenance agreement protections for Year 2000 compliance; and b) reviewed all data processing agreements to determine if the vendors have Year 2000 compliance obligations.		
8. Determine if management has assessed the financial and operational capabilities of their hardware and software vendors to provide Year 2000 processing capabilities. Note the basis and results of this assessment.		
9. How is the project team managing the identification and synchronization of external interfacing systems (payment processing, sponsor and servicers' systems) which may use different date methodologies? How is management addressing the required programming to build data bridges for these interfaces?		

Section V – Action Plan Completeness

Objective – To evaluate the adequacy of plans for correcting, testing and implementing solutions for Year 2000 processing and any formal and informal corrective action plans

Audit Program Step	Findings	W/P Ref.
1. How much time will it take to address the Year 2000 problem? (Get this assessment from the Year 2000 project manager, if applicable.)		

Audit Program Step	**Findings**	**W/P Ref.**
2. Has the credit union broken the project out into manageable phases and estimated how much time each phase of the project will take (vendor contact, vendor follow-up, testing, etc.)?		
3. Have specific Year 2000 related tasks been prioritized from most critical to least critical?		
4. Will the majority of time be devoted to testing and quality assurance?		
5. Has the credit union developed an appropriate testing strategy? Describe the strategy.		
6. What is, or will be, the role of the user community relating to the Year 2000 problem?		
7. Has management developed a strategy for responding to external inquiries regarding its Year 2000 compliance?		
8. If it is evident that the institution's, its vendors or servicer's systems are not fully Year 2000 capable: a) determine if all critical systems will be Year 2000 compliant and fully tested by December 31, 1998, and b) determine which critical applications will not be Year 2000 capable and fully tested by December 31, 1998.		

Audit Program Step	**Findings**	**W/P Ref.**
9. Review and evaluate management's contingency plan in case compliance is not achieved by December 31, 1998. What is the date that management plans to revert to the contingency plan? Has sufficient time been allocated to implement the alternative solution to the Year 2000 fix?		
10. How is management ensuring that any new systems are Year 2000 compliant?		

NCUA YEAR 2000 EXAMINATION AUDIT SCOPE GUIDE
INSTITUTIONS WITH IN-HOUSE DEVELOPED SYSTEMS

Institution	
Name of Contact	
Phone Number of Contact	
Fax Number of Contact	
Date Interviewed	

Preliminary Review

1. Obtain and review the enterprise schematic that depicts all systems, servicers, vendors, and internal and external interfaces. If an enterprise schematic is not available, determine how management identified all components in possible need of Year 2000 repair and review supporting documentation.

2. Determine whether management has identified the:
   a) financially significant applications that were developed in-house or modified packages
   b) financially significant turnkey applications
   c) applications that are currently vendor supported
   d) other applications (i.e., PC-based applications) that are packaged and whether these are vendor-supported
   e) non-critical applications

3. How many of the applications indicated above does management claim are Year 2000 compliant? How many are not or have not yet been confirmed?

4. For those that are considered Year 2000 compliant, how did management make this assessment?

5. Is this assessment based on validation and testing? And did management's validation and testing efforts entail ensuring that date methodologies for interfacing systems have been properly bridged? Review test results.

6. Computer hardware used:

7. Operating system software used:

8. Networks used:

NCUA YEAR 2000 EXAMINATION AUDIT SCOPE GUIDE
INSTITUTIONS WITH IN-HOUSE DEVELOPED SYSTEMS

Section I – Examination Planning and Control

Audit Program Step	Findings	W/P Ref.
1. Note to what extent information systems are internally developed.		
2. Review previous examinations, audits (internal or external) or consultant findings relative to Year 2000.		
3. Review and evaluate the current status of any significant Year 2000 findings and recommendations previously reported to management.		
4. How well has management demonstrated an ability to estimate the time, costs and other resources needed to address major projects (i.e., are schedule and cost targets typically overrun) in the past?		
5. Does the institution have and use a project management or cost modeling tool? If so, how comprehensive are the tools and how well are they adhered to?		
6. How were the tools developed or were they purchased?		
7. Based on the Preliminary Review and Questions 1 - 6 above, determine the scope of the Year 2000 examination. Discuss with the EIC.		

Section II - Adequacy of Management Support, Awareness and Monitoring

Objective - To determine if the institution's board of directors and senior management are aware of and understand the risks and complexities of the Year 2000 problem and whether they have demonstrated their support of and willingness to monitor the institution's efforts to ensure Year 2000 compliance.

Audit Program Step	Findings	W/P Ref.
1. Review board of directors and/or senior management meeting minutes to identify discussions of Year 2000 issues.		
2. What is the credit union's board and senior management team's view of the Year 2000 issue? Is it a major concern (typically, the awareness level of the IS community is high while management and the user community's is low)?		
3. Has the institution’s management and the board of directors been apprised of the risks associated with the Year 2000 (especially those risks related to hardware and software, vendors, suppliers, and members not being compliant)?		
4. Has management and/or the board approved a budget for the Year 2000 fix? What is the budgeted cost to correct the problem? Does the budget take all components of the fix into consideration? How is management monitoring adherence to or the need to adjust this budget?		

Audit Program Step	**Findings**	**W/P Ref.**
5. By when does the credit union estimate or has the Year 2000 issue already affected its systems?		
6. By when does the credit union estimate that the Year 2000 problem, current or future, will be corrected ?		
7. Has senior management mandated that all other significant projects be put on hold or given consideration only after the Year 2000 issue has been satisfactorily resolved?		
8. Has management anticipated the impact to the institution's operations in the event that all systems are not Year 2000 compliant by December 31, 1998. If all systems will not be compliant by December 31, 1998, what steps will management and the board take to assure the credit union's on-going operations?		
9. Has management and the board reviewed and approved the Year 2000 assessment and prioritization of critical and non-critical systems?		

Section III – Adequacy of Assessment

Objective – To evaluate the adequacy of the Year 2000 risk assessment and the reliability of the cost and time estimates for corrective action.

Audit Program Step	Findings	W/P Ref.
1. Has the credit union performed a Year 2000 assessment? If not, discuss and document the reasons and management's estimation of the assessment start date.		
2. Review the assessment. What does it include? At a very high level, the assessment should include: a) an inventory of all hardware and software systems b) an enterprise schematic and risk assessment model identifying hardware and software systems requiring modification, and c) estimated financial and other resources necessary for the fix.		
3. The assessment should also include: a) prioritized software and hardware systems to ensure that the most critical systems are addressed first b) operating systems, telecommunications (including ATM) networks, and security software, c) any interfacing computers d) networks, and e) vendor/supplier relationships.		

Audit Program Step	Findings	W/P Ref.
4. Does the assessment include devices with embedded dates such as ATM's, audio response systems, physical security systems (vaults and alarms), elevators, telephones, fax machines, etc.?		
5. Does the assessment address the adequacy of resources (human and information systems) for Year 2000 changes and day-to-day processing activities?		
6. Describe management's assessment of the impact of any changes in operating practices due to the Year 2000 effort.		
7. Has the institution assessed the impact of Year 2000 efforts on business continuity and disaster recovery planning?		
8. Does the assessment estimate how many hours it will take to correct the problem, lines of code affected, estimated costs per line of code, how interfacing systems will handle shared date fields and other information that will be influenced by the Year 2000?		

Audit Program Step	Findings	W/P Ref.
9. Does the assessment address: a) the amount of time needed for corrective action b) the type and amount of financial resources needed and whether the credit union has sufficient financial resources to make all hardware (mainframe, midrange, networks, personal computers) and related application and operating system software Year 2000 compliant c) any required external resources and associated timing issues d) the budgetary impact of Year 2000 changes and available funding e) the impact of Year 2000 project on earnings, capital, and liquidity?		
10. Determine if the credit union has assessed the impact of Year 2000 processing capabilities, as applicable, with the payment system providers, including: a) wire transfer system b) automated clearing houses c) share draft processors d) credit card merchant and issuing systems e) automated teller machine networks f) electronic benefits transfer systems (internal and external) g) internal and external resources, if needed.		

Audit Program Step	Findings	W/P Ref.
11.Has the institution determined whether it has the individuals, or access to individuals, with sufficient technical expertise to make all hardware and software systems Year 2000 complaint? If so, does the assessment address incentive and bonus programs required to retain in-house technical experts and recruit additional resources, if needed?		
12. If outside resources will be used, are these resources under contract? If not, what assurances does management have that these resources are available?		

Section IV – Project Management

Objective – To determine if the institution has developed an effective plan for identifying and correcting information system components in need of repair to ensure Year 2000 compliance.

Audit Program Step	Findings	W/P Ref.
1. Who is the Year 2000 project manager? What was his/her role prior to becoming the project manager? How is he/she managing and monitoring the project? What project management tools/reports is he/she using? Are the tools adequate?		

Audit Program Step	Findings	W/P Ref.
2. If a formal Year 2000 project or assessment is not in progress, discuss and evaluate the credit union's strategy for addressing the issue.		
3. Obtain, review and evaluate project team minutes addressing the Year 2000 issue. Does the documentation support actions taken or planned to ensure Year 2000 compliance?		
4. Determine the status of the Year 2000 project including anticipated barriers and how management plans to address these barriers.		
5. Given management's estimation of when the Year 2000 issue will affect its systems, evaluate whether the current status of the project or management's plans to address barriers provide reasonable assurance that all related matters will be addressed.		
6. Determine which method(s) the institution is using to resolve Year 2000 date calculations (e.g. date expansion or windowing).		
7. How is the team identifying affected source members (or lines of code) in need of Year 2000 repair? Obtain a list of programming tools that the credit union is using to fix the Year 2000 problem. Examples of tools include Year 2000 data reference identifiers, date altering tools, editors, debuggers, code generators, etc. Have the institution describe the tool.		

Audit Program Step	**Findings**	**W/P Ref.**
8. Review and analyze any tool output (i.e., graphs, charts, timelines, etc.). Determine if this output supports verbal communications with management and the project manager regarding the Year 2000 project status.		
9. How is the team identifying filters (i.e. values used other than actual dates in date fields)?		
10. As additional source members and filters are identified, how is the project manager ensuring that cost estimates are adjusted accordingly?		
11. How is the project team managing the identification and synchronization of external interfacing systems (payment processing, sponsor and servicers' systems) which may use a date methodology/methodologies different from the credit union's? Which bridging tools is the institution using to address this issue?		

Section V – Action Plan Completeness

Objective – To evaluate the adequacy of plans for correcting, testing and implementing solutions for Year 2000 processing and any formal and informal corrective action plans

Audit Program Step	Findings	W/P Ref.
1. How much time will it take to address the Year 2000 problem? (Get this assessment from the Year 2000 project manager, if applicable.)		
2. Has the credit union broken the project out into manageable phases? Has the amount of time been estimated for each phase of the project (e.g., hardware and software inventory, scanning, cost estimation, altering of dates, impact analysis, editing, debugging, testing, and systems conversion)?		
3. Have specific Year 2000 related tasks been prioritized from most critical to least critical?		
4. Has the credit union developed an appropriate testing strategy for Year 2000 modifications? Describe the strategy.		
5. Will the majority of time be devoted to testing and quality assurance?		
6. Has the credit union established appropriate program change management standards to be used during the Year 2000 change efforts?		
7. What is, or will be, the role of the user community relating to the Year 2000 problem?		

Audit Program Step	**Findings**	**W/P Ref.**
8. How is management ensuring that all new systems are Year 2000 compliant?		
9. If it is evident that the institution's systems are not fully Year 2000 capable: a) determine if all critical systems will be Year 2000 compliant and fully tested by December 31, 1998, and b) determine which critical applications will not be Year 2000 capable and fully tested by December 31, 1998.		
10. Review and evaluate management's contingency plan in case compliance is not achieved by December 31, 1998. What is the date that management plans to revert to the contingency plan? Has sufficient time been allocated to implement the alternative solution to the Year 2000 fix?		

Section VI - Audit

Objective – To assess internal and external audit's independence, effectiveness and level of involvement in reviewing the institution's Year 2000 efforts.

Audit Program Step	Findings	W/P Ref.
1. Review audit plans and budgets through 2000 and determine if they include the identification of specific resources (personnel, training, and budgeted hours) necessary to review Year 2000 issues. Also, determine if audit has independently and formally assessed all critical systems impacted by Year 2000.		
2. Is audit management communicating relevant issues regarding Year 2000 compliance issues to senior management and the board of directors?		
3. Determine if auditors are actively involved in Year 2000 efforts to assess and monitor the effectiveness of project management and adequacy of related internal controls.		

NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: August 16, 1996 **LETTER NO.: 96-CU-5**

TO ALL FEDERALLY INSURED CREDIT UNIONS:

SUBJECT: Federal Financial Institutions Examination Council's (FFIEC) Statement on the Risks to Financial Institutions Involving Computer Systems in the New Millennium

The FFIEC has issued the attached statement on the substantial risks to financial institutions involving their computer systems as the industry enters the new century (year 2000). These risks are attributed to the programming code in many existing computer systems that may result in inaccurate calculations based on any two-digit year field containing the value "00" which the system may read as 1900.

The FFIEC statement alerts financial institutions, servicers, and vendors to the need to adequately address the risks, including system failures or erroneous data, associated with the existing programming code. This issue potentially affects all organizations that rely upon computer systems.

Management should take action to ensure the credit union's computer system (hardware and software) is capable of handling the transitions into the twenty-first century correctly. We encourage you to use the attached statement as guidance for developing a plan of action. Credit unions which use outside electronic data processing vendors and servicers should seek assurance that their vendors and servicers are adequately addressing the system and software issues related to the coming millennium.

If you have any questions, please contact your regional office or your state supervisory authority.

Sincerely,

/S/
Norman E. D'Amours
Chairman

EI
Attachment

Federal Financial Institutions Examination Council
2100 Pennsylvania Avenue, NW, Suite 200 - Washington, DC 20037 (202) 634-6526 - FAX (202) 634-6556

THE EFFECT OF YEAR 2000 ON COMPUTER SYSTEMS

To: Chief Executive Officers of all Federally Supervised Financial Institutions, Senior management of each FFIEC Agency, and all examining personnel.

PURPOSE

This interagency statement alerts financial institutions to substantial risks to the industry represented by the programming code in existing computer systems as the industry enters the new millennium (year 2000).

BACKGROUND

The "year 2000" problem is pervasive and complex. Virtually every organization will have its computing operations affected in some way by the rollover of the two digit year value to 00. The majority of computer operating systems and programs currently in use have been developed utilizing six digit date fields (YYMMDD). For example, December 31, 1999, would be represented by "991231" in computer code. The two digit field for the year (in example "99") is the basis for all calculation formulas within most computer systems, particularly those processed through mainframes.

Up until now, this two digit field has sufficed, using a subtraction of current date from some future date (up to 12-31-99). As the industry enters the year 2000, the two digit field "00" will not permit accurate calculations based on the current formulas. January 1, 2000 would be read as 000101. Many computer systems will recognize this date as the year 1900. The potential impact is that date sensitive calculations would be based on erroneous data or could cause a system failure. This affects all forms of financial accounting (including interest computation, due dates, pensions, personnel benefits, investments, legal commitments). It can also affect record keeping, such as inventory, maintenance, and file retention. Reliable information is necessary for financial institutions to conduct business.

These coding changes impact billions of lines of program code, throughout government, banking, and all other users of computer technology. Most large financial institutions should be aware of this potential problem, however, industry estimates are that only 30 percent are currently addressing the issue. In some cases, individual financial institutions are projecting costs of $50 to $100 million over the next three years. Most vulnerable are the community financial institutions that do their own programming with in-house developed software systems. According to industry "guesstimates," costs to resolve these programming challenges worldwide will approach $600 billion (all computer systems, not just banking). Banking, however, is a heavily technology sensitive industry and will be impacted greatly.

CONCERNS

Many financial institutions, servicers, and vendors have not adequately addressed the risks associated with the coming millennium. This lack of planning could result in the extended or permanent disruption of computer system operations. This may be the result of either the problem itself or the cost of fixing it.

Time is critical. Commitments to action and funding cannot be deferred, as the year 2000 is a finite date. This issue affects EVERY financial institution, whether processing information internally, through service bureaus, or a combination of both.

ACTION PLAN

Financial institutions should achieve year 2000 compatibility by performing a high level risk assessment of how systems are affected. This should be followed by the development of a detailed action plan. The board of directors and senior management should take the following steps in addressing this issue:

- Developing a risk assessment that identifies systems and applications that must be modified.
- Identifying the segments of computer systems that must be modified.
- Evaluating various alternatives (determining which applications that should be redeveloped, replaced, or modified).
- Estimating costs for modifications.
- Reviewing, approving, and establishing milestones to ensure the timely completion of the institution's millennium plan.
- Ensuring that new systems are year 2000 compliant.

An institution should review all aspects of computer systems to include those provided by service bureaus, hardware vendors, and other software vendors. For any aspect of its information systems processing management must:

- Ensure that external vendors and servicers are adequately addressing the system and software issues related to the coming millennium.
- Ensure that the institution has taken adequate steps to ensure that critical operations will continue if the servicers or vendors are unable to achieve millennium requirements.

TESTING

All reprogramming efforts must be completed in time for adequate system testing. It is recommended that reprogramming efforts be completed by December 31, 1998. This will provide one full year for testing. It is important to note that all systems from mainframes to personal computers and local area networks are susceptible to the impact of year 2000 consequences.

The appendix to this issuance provides a suggested outline of the process that should be followed to ensure that issues concerning the millennium are addressed.

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

APPENDIX

Millennium Planning Process

I. Establish a Year 2000 Review Team

A. Management should consider utilizing both internal and external information systems and audit resources to ensure that a risk-based Year 2000 Action Plan is developed.

B. An inventory of all computer operating systems, applications and files should be created. All those with year 2000 issues must be identified.

II. Develop an institution wide year 2000 plan.

A. The initial step in developing the plan should be to consider whether current systems and files should be modified, replaced, outsourced, or discontinued. It should be noted that even if new systems are purchased, old files may still have to be modified. (All computer systems, including mainframes, personal computers, local area networks, etc., should be considered).

B. The year 2000 plan should also identify and prioritize applications and processes that are the most date sensitive and those which are most vulnerable. Interdependent applications should be grouped together.

C. Management and the board of directors need to ensure that adequate funds and resources are allocated so that all year 2000 projects are completed in a timely manner.

III. Year 2000 Plan Implementation.

A. Initiate pilot projects to test solutions to identified problems. It may be feasible to work with more than one vendor in order to evaluate their various solutions/capabilities before making a final decision.

B. Begin the process of systematically implementing year 2000 changes by priority in accordance to risk. These projects should be conducted within the framework of the system development life cycle process currently in place.

C. Conduct post implementation reviews to ensure the integrity and functionality of the modified systems.

NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNIONS ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: June 3, 1997 **LETTER NO.: 97-CU-6**

TO ALL FEDERALLY INSURED CREDIT UNIONS:

SUBJECT: Year 2000 Conversion

Virtually every financial institution relies on computers, either their own or a servicer's, to provide for processing and updating of records and a variety of other functions. Most institutions cannot survive without the use of computers. Because of this, all institutions are vulnerable to problems associated with the Year 2000.

All levels of management, including the Board of Directors, must understand the implications of this problem; specifically, the fact that all computer systems will be affected; the cost of the solution may be significant; and, because the deadline for compliance is an immovable date and fully implementing solutions may take years, management cannot delay action.

Many computer systems and programs may not be currently designed to handle the Year 2000 for a variety of reasons. The core problem is that a majority of the systems in use today have a two-digit field for the year. When the Year 2000 comes, the date will be reflected as "00", but many systems will mistake that for the year 1900, leading to numerous problems when calculations requiring the use of dates are performed such as:

- calculating interest;
- calculating truth-in-lending or truth-in-savings disclosures;
- determining a person's age; and
- determining amortization schedules.

Automated Teller Machines (ATMs) may also assume all cards are expired due to this problem. Errors caused by these miscalculations may also expose institutions and data centers to financial liability and risk of damage to customer confidence in the institution. If computer systems are not made Year 2000 compliant, systems and programs may fail.

For an institution or data center to prepare for the Year 2000, several steps must be taken. The hardware and software used by the institution and/or its servicers must be analyzed for compliance. Any system with a date function built into it may need to be made Year 2000 compliant either by being replaced or reprogrammed. If there are deficiencies, new software, and possibly hardware, which is compliant, will have to be identified and purchased in time for records to be converted; or massive reprogramming of existing software may be necessary. Due to the complexity of the issue, both options will be expensive and, in some cases, cost millions of dollars. Institutions and data centers that have begun to research how to address this issue are finding that the solution will take several years to define, test, and fully implement.

The Year 2000 problem is not limited to one type of software or hardware, critical or non-critical. Examples of affected critical systems include mainframes, personal computers (PCs), and networks. Other critical systems which could be affected include:

- telephones and PBX systems;
- audio voice systems;
- elevators;
- security systems (badge readers, surveillance systems, parking lot gates, vaults);
- time dependent controls (parking lot lighting, programmable thermostats);
- power management functions (heating/air conditioning controls, uninterruptable power supply systems, building lighting systems); and
- environmental safety systems.

Examples of non-critical systems that could be affected include:

- fax machines;
- electronic time clocks;
- vending machines; and
- landscaping systems.

In researching acceptable solutions, institutions and data centers will need to bear in mind the interrelationships between the various software systems they use, as well as any data received from or provided to outside sources, such as Automated Clearing

Houses (ACH) or payroll servicers. Data from outside sources not compliant with the Year 2000 may corrupt an institution's or data center's files causing disruption in the institution or data center's ability to process transactions. Alternatively, institution data or files not compliant which are sent to outside sources may corrupt those outside sources leaving the institution with potential liability for any incurred losses.

The ability to adequately manage the time left to deal with the situation is critical. There are a finite number of companies and individuals capable of reprogramming existing systems. The longer institutions and data centers wait, the fewer of these companies or individuals will be available to assist them and the higher the price will be.

Institutions and data centers which purchase their software need to take a proactive approach to this situation. They cannot assume their software vendors are adequately addressing the problem. Situations have already arisen where institutions have contacted vendors and been informed that software products currently being used are not Year 2000 compliant, and the vendor does not intend to make them compliant.

It is imperative that management take an aggressive and proactive approach to this problem in order to meet the deadline. Institutions and data centers should inquire specifically as to what plans the outside software vendors have made and/or implemented to make their software compliant. Time frames should allow for any reprogramming to be accomplished, and full testing done, well before December 31, 1999. Institutions and data centers which do in-house programming of their software must make an assessment of the costs and time involved immediately so that reprogramming can be completed and fully tested well before December 31, 1999.

Institutions lacking the expertise to address this problem should seek help from outside resources such as trade organizations, EDP auditing firms, and Year 2000 resource firms.

To assist credit unions in this endeavor, we sent the enclosed letter to the major credit union vendors (listed in the attachment) inquiring about their Year 2000 compliance status. If your vendor is not on the list, we ask that you forward their company name, address, and contact person (if available) to: National Credit Union Administration, Examination & Insurance, 1775 Duke Street, Alexandria, VA 22314-3428. If you have access to the Internet, you may send this information to: eisupv@ncua.gov. We ask that you send this information by one method only. Periodically, we will make the vendor information available to assist you in obtaining knowledge of your vendor's status.

We have also enclosed an Appendix which discusses in more depth the complexity of the problem and viable solutions. Your examiner will be inquiring about your readiness and ability to handle the Year 2000 problem. Those credit unions not in compliance should expect to reach formal agreements with their examiner to ensure compliance by December 31, 1999.

If you have any questions, please contact your regional office or your state supervisory authority.

Sincerely,

/S/
Norman E. D'Amours
Chairman

EI

Appendix

PROBLEM

Many computer systems may not recognize or process information with dates beyond December 31, 1999. Unless corrected, beginning January 1, 2000 computer systems worldwide will begin to fail and/or produce incorrect information. This issue is not just limited to financial institutions. It is pervasive among all computer systems including both government and private sectors. Also, the problem is not limited to large mainframe computers. Smaller computer systems, including local area networks (LANs) and personal computers (PCs), may be affected. Unless corrected, the Year 2000 problem could have a substantially negative effect on the financial institution industry worldwide.

Systems that use a YYMMDD format (year, month, day) to record dates will generally recognize the year 00 as 1900 rather than 2000 since they have no provision to reflect a century. Note that the year field contains only two positions; therefore, the YYMMDD date of 970704 translates to July 4, 1997. Computers which use the YYMMDD format automatically assume the century to be 19 (hence 1997). After the new millennium arrives, these computers would record July 4, 2000 as 000704 and interpret this date to be July 4, 1900. However, in some cases these systems may actually default to another year, such as 1980 (the beginning of time for PCs), 1984 (the beginning of time for DOS systems), or some other incorrect date.

Correction of Year 2000 problems will, in many cases, require a file conversion. Some institutions and data centers will not have available sufficient disk space or time to perform the conversion and run parallel to the old system for a period of time to ensure that all problems have been resolved.

If institutions do not have their converted systems in place by December 31, 1998, they may not have enough time to fully test and debug those systems by December 31, 1999. Also, as time passes valuable Year 2000 resources may become more scarce and/or costly thereby preventing the conversion of systems in time to meet the deadline.

SOLUTIONS

The Year 2000 problem has three basic software solutions:

- **Rewrite:** This solution requires re-coding date calculations where necessary with a four-position year field. The re-coding not only involves changing the program source code, but also changing the screen displays. This is a permanent solution but probably the most costly.

- **Renovate:** This solution calculates the date using a technique called "windowing." As an example of this technique, two position year fields greater than 50 are assumed to be in the 20th century. Those date fields that are less than 50 are assumed to be in the 21st century. Not every windowing technique, however, will use the same assumptions. This is not a permanent solution but will buy time in some situations for institutions unable to develop a permanent solution before the deadline.

- **Replace:** This solution may be the quickest approach, but also could be extremely expensive. Institutions that elect this approach must ensure that the new systems they purchase are Year 2000 compliant. Another benefit to the replacement approach is that it provides the opportunity for institutions to upgrade their aging systems. Of course, institutions may also take an approach that incorporates any, or all three, of the basic software solutions. Institutions must make this decision based upon their current systems, needs, and time available to accomplish the conversion.

The Year 2000 problem has two basic hardware solutions: upgrade or replace. In those institutions where the hardware is relatively old, replacement will most likely be a less costly approach than an upgrade. However, institutions must ensure that the upgraded equipment will interface with both existing software applications and hardware configurations.

Whatever solution an institution selects, it must also ensure that the solution addresses two basic components. First, financial institutions and other organizations must solve this problem with respect to their own internal systems. That is, assuring that their internal computer systems properly handle date-dependent transactions and computations in the new millennium. Second, financial institutions and other organizations (corporations, governments, and payment systems both domestically and internationally) must assure that they can exchange date-dependent information effectively and efficiently. Standards are necessary to facilitate this exchange of information for payment systems and general commerce. The National Institute of Standards and Technology (NIST) in FIPS Pub 4-1, dated March 25, 1996, recommends the use of a four-digit year element with a contiguous two-digit century element (e.g., 1999, 2000, etc.).

Over the next two and half years, the financial institutions industry will expend significant resources to address Year 2000 issues. Some experts predict that it may be one of the largest project management efforts the financial institutions industry has undertaken.

Most computer industry participants agree that the process firms will use to manage the Year 2000 efforts consists of the following basic phases:

- **Awareness:** Management at all levels must become fully aware of the Year 2000 issue and its impact on the institution and customers. Management must:

- define and explain the importance of achieving Year 2000 compliance;
- select an overall approach for structuring the institution's Year 2000 program;
- assess the adequacy of the existing information resource management infrastructures to support the Year 2000 effort; and
- mobilize resources, including the establishment of a Year 2000 committee.

- **Assessment:** The institution must assess the impact of the Year 2000 on both hardware and software systems. This process of identifying and ranking information systems should not be limited to a simple inventory of applications and platforms, but must also include assessment of the impact of information system failures on the institution's operations and processes. Institutions must also consider whether there are enough resources, skill, or time to convert or replace all of the affected systems. Therefore, institutions must determine which systems:

  - are mission critical and must be converted or replaced;
  - which systems support important functions and should be converted or replaced; and
  - which systems support marginal functions and may be converted or replaced at a later date.

- **Renovation:** The renovation phase addresses the conversion, replacement, or elimination of the institution's various systems. Renovation either involves:

  - conversion of an existing software/hardware system;
  - replacement and/or development of a new software/hardware system; or
  - elimination of an existing unneeded software/hardware system.

  In all three of the above cases, the process must consider the complex interdependencies among applications, hardware platforms, databases, and any internal and external interfaces. This phase requires a high degree of coordination and adequate documentation due to the interdependencies of the various systems.

- **Validation and Testing:** The validation and testing phase may consume over half of the Year 2000 program resources and budget. The actual length of this process is directly related to the number of systems impacted and their complexity. Computer industry representatives anticipate that this phase will be the most difficult step comprising at least 50 percent of the project's time. As part of this phase, institutions will have to validate and test the interactions between the various platforms, operating systems, utilities, applications, databases, and interfaces. All converted or replaced systems must be fully tested to:

- uncover errors introduced during the renovation phase;
- validate Year 2000 compliance; and
- verify operational readiness.

- **Implementation:** Once converted or replaced and subsequently tested, Year 2000 compliant applications and system components must be implemented. Since not all systems will be converted or replaced simultaneously, institutions should expect to operate in a computing environment of compliant and non-compliant systems. The reintegration of the Year 2000 compliant systems in the production environment must be carefully coordinated to account for system interdependencies. Institutions will also need to consider parallel processing (running the old and converted systems concurrently) to ensure accuracy and reduce risk.

RISKS

Financial institutions are a technology sensitive industry. Nearly every aspect of the industry is automated and depends on computer systems for processing transactions and providing management information. If the computer systems financial institutions rely on cannot handle processing of transactions in the new millennium and/or their systems produce inaccurate information, financial institutions face the potential of failure.

There is an additional complication. Industry customers, vendors, and payment system partners must be able to handle Year 2000 date changes. There is thus the potential for a cascading effect from a payment system, network provider, major customer(s), or information processing vendors. Accordingly, financial institutions must develop comprehensive solutions to this problem and prevent unintentional consequences from affecting their systems and the systems of others.

A tremendous interrelationship exists between payment systems at the local, national, and international levels. Financial institutions must be able to exchange clearings at the local level, send and receive automated clearing house (ACH) transactions and clear checks at the national level, and send and receive wire transfers at the international level. All these systems are interdependent. And, loss sharing arrangements are in effect in case of any type of settlement failures.

The payment systems affected include CHIPS, SWIFT, Fedwire, Automated Clearing Houses, MasterCard, VISA, regional and national ATM switches, and Electronic Benefits Transfer (EBT) systems. In addition, beginning January 1, 1999, all transactions with the U.S. Government must be via ACH. These systems must be able to handle Year 2000 processing and communicate with each other to facilitate normal banking and commerce. Accordingly, financial institutions must make certain that their solution is consistent with their business and payment systems partners.

OTHER IMPLICATIONS

These Year 2000 issues will absorb resources and management's attention that would otherwise focus on other business issues. Solving the Year 2000 problem will generally not add value to the financial institution. Nor will it likely improve earnings or capital, provide new revenue sources, or reduce expenses. In addition, any new products and services must be Year 2000 compliant. Accordingly, financial institutions have to fix their old systems and develop new systems concurrently. Solving this problem will likely strain the financial institution's resources, yet it is absolutely necessary.

May 9, 1997

«FNAME» «LNAME», «TITLE»
«VENDOR_NAME»
«ADDRESS»
«CITY», «ST» «ZIP»

Dear «Surname» «LNAME»:

As you are probably aware, the Year 2000 concern is becoming a forefront issue. We are taking an active role in determining Year 2000 compliance in federally insured credit unions. We plan to assess the Year 2000 compliance status of every federal credit union by the end of this year and have a goal of achieving compliance by the end of 1998. We want to work with you and your credit union customers in a joint effort to ensure that credit unions are capable of transitioning into the new millennium. Consequently, our examiners will be discussing these issues with credit unions. We anticipate that your credit union customers will be contacting you about your systems' Year 2000 compliance status.

Specifically, we are interested in the following:

- Your overall Year 2000 plan(s):
  - explanation of the process;
  - where you are in the process;
  - how testing will be, or has been, accomplished;
  - whether your plan requires compliance certification from an independent third party for each system/application you offer; and
  - how you plan to share your systems' compliance status with your customers.

- Year 2000 compliance information for each of your credit union systems as well as their current compliance status.

- Any plans you have in place for Year 2000 customer support such as:
  - how to determine if their systems are compliant;
  - what they should do if their systems are not compliant; and
  - whether there is an upgrade (if required) to their existing system.

- The name of a contact person in your company who we may communicate with directly.

We would like to coordinate the dissemination of information concerning the status of your various programs/products/systems. We believe this would reduce the burden on credit unions and their vendors. We propose to share this information with our examiners, credit unions, and various state and federal agencies. By sharing this information, we will be able to educate our examiners on which systems are Year 2000 compliant thereby reducing the number of contacts and inquiries you may receive from your customers.

To accomplish this task, we ask that you complete the attached Systems Information Questionnaire for each credit union application program/system you offer. We also ask that you return the questionnaire to our office by May 30, 1997.

We would also be interested in holding a vendor's meeting in our central office (Alexandria, VA) to discuss Year 2000 issues and vendor concerns; specifically those that relate to credit unions and their systems. We would like to target a June or July 1997 date for the meeting. If you are interested in attending, please let us know.

If you have any questions, please do not hesitate to contact Roger Blake in our office at 703-518-6360.

Sincerely,

David M. Marquis
Director, Examination & Insurance

EI/RAB:rab
SSIC #13200

cc: Executive Director
Director of OTIS
NASCUS Representative

s:\supr\y2k\y2kedp.doc

Systems Information Questionnaire
(Please complete a separate questionnaire for each application.)

- Name of your company: _____
- Name of Program/Application: _____
- Version # (or other identifying product number): _____
- Is this version fully Year 2000 compliant? _____Yes _____No
  - ♦ If yes, has this version been certified compliant by an independent third party? _____Yes _____No

    If no, do you plan to have this version certified? _____Yes _____No
  - ♦ If no, do you plan to make this version compliant? _____Yes _____No

    If yes, when do you expect to complete the process for this version?
    _____

    If no, what action, if any, do you intend to initiate for customers with the non-compliant version?

    _____

    _____

    _____

    _____

    _____

    _____

Please return this questionnaire to:

National Credit Union Administration
Examination and Insurance
1775 Duke Street
Alexandria, VA 22314-3428

Aftech
18 Great Valley Pkwy
Malvern, PA

American Business Computers Inc.
3930 E. Apple Ave.
Muskegon, MI

AMI, Inc.
P.O. Box 167
Franksville, WI

Benchmark
17500 West Liberty Lane
New Berlin, WI

Benchmark Systems
P.O. Box 787
Mechanicsville, VA

Brick and Associates
2875 Northwind Drive, Suite 230
East Lansing, MI

C.U. Processing, Inc.
26200 Lahser Rd. Suite 100
Southfield, MI

CMC
2450 East 70 South
Salt Lake City, UT

CompuSource Systems, Inc.
3820 Ridge Lea Road
Amherst, NY

Computer Consultants Corp.
47 W 2nd St, Suite 200
Salt Lake City, UT

Credit Union National Association
P.O. Box 431
Madison, WI

CU Technology
151 Kalmus Drive - Suite F1
Costa Mesa, CA

CUSA, Inc.
969 E. 4800 South
Salt Lake City, UT

Datamatic
5545 Enterprise Drive

Lansing, MI

EDS Credit Union Services
2600 Technology Drive
Orlando, FL

EDS Credit Union Services
5400 Legacy Drive
Plano, TX

EDS Newtrend
2600 Technology Drive
Orlando, FL

EPL, Inc.
1225 Fifth Avenue North
Birmingham, AL

FedComp
7115 Leesburg Pike, Suite 200
Falls Church, VA

FIserv
P.O. Box 979
Brookfield, WI

FIserv
707 West Algonquin Road
Arlington Heights, IL

FIserv - Spokane
P.O Box 597
Spokane, WA

FIserv - Summit Information Systems
850 Southwest 35th Street
Corvallis, OR

FIserv / ADOL
6995 Tico Road
Titusville, FL

Fiserv / Minneapolis
5249 West 73rd Street
Edina, MN

FIserv Flint
3031 Airpark Drive North
Flint, MI

FIserv Galaxy 2000 CU Systems
5600 Crooks Road, Suite 101
Troy,MI

FiTECH Systems
3098 Piedmont Road, Suite 400
Atlanta, GA

Helvetya Delcaribe
P.O. Box 5174
Carolina, PR

IDC Financial Publishing, Inc.
PO Box 140
Hartland, WI

Innovative Technology, Inc.
4203 South 120th Street
Omaha, NE

Integrated Business Systems, Inc.
2205 West Wabash Ave., Suite 201
Springfield, IL

International Software Systems (ISS)
8101 College Blvd. Suite 290
Overland Park, KS

IPS, Inc.
14040 North Cave Creek, Suite 100
Phoenix, AR

Maine Credit Union League
P.O. Box 1236
Portland, ME

Modern Computer Systems
12224 Nicollet Avenue, South
Burnsville, MN

National Assoc. of Federal Credit Unions
3138 N. 10th Street, Suite 300
Arlington, VA

NCS
1250 East 223rd Street, Suite 119
Carson, CA

Pearless Systems
1212 East Arapahoe
Richardson, TX

Premier Systems, Inc.
P.O. Box 10361 - 1600 36th Street
West Des Moines, IA

ProfitStar, Inc.
11128 John Galt Blvd., Suite 350
Omaha, NE

re:Member Data Services
8900 Keystone Crossing Suite 1100
Indianapolis, IN

Share 1 Systems
2750 Colony Park Drive, Suite 10
Memphis, TN

Sheshunoff
505 Barton Springs Road, Suite 100
Austin, TX

SOS Computer Systems, Inc.
720 East Timpanogos Parkway
Orem, UT

Sunbelt Computer Systems, Inc.
223 Main Street
Fort Mill, SC

Symitar
5151 Murphy Canyon Road
San Diego, CA

Syntropy Inc.
P.O. Box 2215
Durango, CO

Systronics
9655 Lackman
Lenexa, KS

Total/1 Credit Union Services
1815 Coral
Houston, TX

Ultradata
5020 Franklin Drive
Pleasanton, CA

Users, Inc.
1250 Drummers Lane
Valley Forge, PA

WESCO
4695 44th Street Suite 180
Kentwood , MI

Western New York Computing Systems
2136 Five Mile Line Road
Penfield, NY

XP Systems
301 Science Dr.
Moorpark, CA