NCUA LETTER TO CREDIT UNIONS

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

DATE: **December 18, 1997** **LETTER NO. 97-CU-12**

TO: **All Federally Insured Credit Unions**

SUBJECT: **Credit Union Year 2000 Self-Analysis Guide**

Attached for your information and use is NCUA's Credit Union Year 2000 Self-Analysis Guide. This guide has been developed for NCUA by Coopers and Lybrand, L.L.P. to help credit unions analyze their readiness for the Year 2000. Included in the Guide is a narrative providing a general overview of the processes required to ensure Year 2000 compliance and a *Credit Union Checklist* to use as a tool to assess readiness.

I encourage credit union management and boards of directors to review the narrative section and address the questions in the *Checklist*. The *Checklist* was designed to be completed on a periodic basis as an ongoing assessment tool. Your examiner may want to review the responses to the *Checklist* with you during your regular examination.

The Year 2000 is a situation that will not go away. Every credit union must ensure they are prepared for it. The Self-Analysis Guide was developed to help in your preparations for full compliance and undisturbed service to members.

Sincerely

/S/
Norman E. D'Amours
Chairman

EI

INTRODUCTION

By now, you have heard more than you probably ever wanted to hear about the inevitable, the millennium, the problem of the Century.....Year 2000 and its impact on your various systems which rely upon date functions. Hopefully, you have already begun the necessary steps to ensure that your credit union will be ready on January 1, 2000. If you have not, you have a lot of work ahead of you. This guide has been developed to help you analyze your readiness for the Year 2000.

Throughout this document, you will see many references to "Year 2000 compliance" and "compliant systems." Although a formal definition of compliance has not been communicated before now, compliance criteria have been established. Your credit union will be deemed to be **Year 2000 compliant when all of your "critical systems" have been either renovated or replaced and are able to process both 20th and 21st century transactions.** Critical systems are those which must be converted or replaced to ensure continued functioning of the credit union after December 31, 1999. The only way to ensure that your systems are compliant is through adequate testing and validation.

The National Credit Union Administration (NCUA) has issued three letters to credit unions regarding Year 2000 compliance:

- Letter No. 96-CU-5 issued to all federally-insured credit unions on August 16, 1996, addressed the Federal Financial Institutions Examination Council's (FFIEC) Statement on the Risks to Financial Institutions Involving Computer Systems in the New Millennium. In this letter, you were encouraged to develop a plan of action to ensure that your computer systems are capable of handling transactions in the 21st century.
- Letter No. 97-CU-6 issued June 3, 1997 to all federally-insured credit unions, entitled "Year 2000 Conversion", and was more specific in nature. It included the numerous problems that your institution might encounter with system miscalculations, and provided guidance on specific steps that your institution or data center must take to prepare for the Year 2000. It also outlined the risks and implications of non-compliance and discussed your examiner's responsibility to assess your readiness for the Year 2000 during upcoming reviews. Finally, the letter discussed the steps that NCUA is taking to assist credit unions in this endeavor.

- Letter No. 97- FCU-2, issued to all Federal credit unions on August 22, 1997, discussed the Senate's mandate that federal agencies take "an aggressive approach to the Year 2000 issue for institutions which they regulate or have oversight authority." The purpose of the letter was to update readers on the Year 2000 examination program, agency plan, and actions taken by NCUA since the last letter; and to provide additional information regarding vendor compliance.

Aside from information provided to your institution by NCUA, there is no doubt that you have already been inundated with a fair amount of information from media sources as well. The purpose of this guide is not to rehash all of this information. Rather, it is designed to:

- discuss your responsibilities relative to the Year 2000 issue;
- provide "best practice" for assessing your institution's readiness for Year 2000; and
- describe the activities that should be implemented, following a **5-phase repair approach**, which if followed properly, should substantially reduce the risk of your institution's non-compliance on January 1, 2000.

The status of credit unions' Year 2000 compliance is of interest, not only to NCUA, but to the General Accounting Office (GAO) and Congress. On a quarterly basis, NCUA must provide Congress with a report specifying federally-insured credit unions' Year 2000 compliance status. NCUA has developed a special Year 2000 Quarterly Credit Union Report to capture and report this data to the federal government. NCUA will mail the report quarterly to all federally-insured credit unions starting December 31, 1997 and to all non-compliant federally-insured credit unions each quarter thereafter.

The Year 2000 Fix - The Scope (What It Entails)

It is important to note that the Year 2000 fix is about much more than just your application software's ability or inability to process data past December 31, 1999. It is also about more than your placing reliance on a software vendor's assertions regarding its readiness for the millennium change. Actually, **the Year 2000 fix is about whether or not your institution will successfully survive the century change and be able to operate normally, or at all, on and after January 1, 2000.** As a result, you must consider the risk that might be involved in your efforts to prepare for the century change when dealing with all parties, software vendors, third party servicers, information system vendors (ISVs), and consultants. In your dealings with these individuals and entities, you must act responsibly, never placing too much reliance on hearsay, promises, or commitments without the necessary due diligence, including proper testing and validation.

The Year 2000 challenge is not as complicated a technical issue as it is a project management issue. From a programming perspective, the fix is not that complicated or difficult to achieve. There are many techniques and alternatives available to ensure that calculations and processes will properly occur past December 31, 1999. The problem occurs, however, and the issue becomes more complex, when issues such as the following come into play:

- taking the necessary time to plan for the fix;
- setting aside the right resources (i.e., money, time, and people) to address the fix;
- ensuring that all systems and devices with embedded dates such as: ATMs, audio response systems, security systems (vaults and alarms), elevators, telephones, fax machines, heating, venting, and air-conditioning systems (HVAC), and lighting systems are identified;
- assessing the impact of Year 2000 processing capabilities with payment system providers including: wire transfer systems, ACH, share draft processors, credit card merchant and issuing systems, ATM networks and electronic benefits transfer systems (internal and external);
- coordinating the timing of, and the various date methodologies for, internal and external interfacing systems, including home-banking;
- managing vendors;
- testing new or renovated systems; and
- implementing new or renovated systems.

As if these issues are not complicated enough, there's the looming date, January 1, 2000, that can not be extended or negotiated. Unlike past system conversions, which could be postponed if needed, January 1, 2000 cannot be postponed.

As mentioned earlier, the fix entails identifying all hardware, software, information system vendors, embedded processors, and third party servicers which may be affected by the century change. Next, you must develop and implement a strategy, referred to as your renovation approach, for repairing, replacing, or retiring related systems and components. This is necessary so that your credit union can function properly past January 1, 2000. While performing these tasks, you must always consider what is and what is not important. You must also face the fact, hopefully sooner rather than later, that your credit union may not function exactly the same after December 31, 1999. Some of the "nice to have" systems or devices, or maybe even some of your critical systems' functionality, may not be fixed in time to ensure full Year 2000 compliance.

And remember, the Year 2000 fix also entails teamwork, teamwork, and teamwork. No matter what the asset size or the particular make-up of your credit union, the same processes must take place and the same ingredients are necessary for success.

Key factors to success are described in the following sections:

- **Senior Management and Board of Directors Involvement;**
- **Project Planning and Project Management;**
- **Risk Assessment; and**
- **Contingency Planning.**

Senior Management and Board of Directors (board) Involvement - These individuals must support the Year 2000 effort and allocate the right resources, including the right money, time, and people to get the job done. The tone at the top will play a key role in your credit union's success. During the assessment phase, senior management and the board should be apprised of both the strategy and the estimated costs related to the renovation, replacement, or retirement of existing systems. If it has not already been done, the necessary funds should be set aside to ensure that, monetarily, the credit union will be able to handle the fix.

When discussing the credit union's short and long-range plans, senior management and the board should also be cognizant of the need to address and resolve the Year 2000 compliance issue before delving into other resource-consuming projects. Senior management and the board must be involved in every phase of the Year 2000 effort and should constantly monitor the credit union's efforts and progress toward compliance. They should also ensure that the appropriate decision-making infrastructure exists within the credit union. Responsibility for the Year 2000 fix rests with the board and should not be delegated to a level that would not facilitate keeping the board apprised of significant issues during the fix. Actually, this authority should probably lie with the President/CEO or designated Vice President of the credit union.

It is also important that these lines of communication remain open at all times. Your examiner will want to meet with the CEO **and** designees to ensure that the Year 2000 issue is receiving the proper attention within the credit union.

Project Planning and Project Management - Planning is one of the most important aspects of the Year 2000 fix. Without a documented project plan, your credit union can not effectively address this issue. A project plan should be developed initially which encompasses the 5 phases (detailed below) to be followed to address the fix and should include critical milestones and deliverables. This plan should also be updated on a frequent basis to indicate the status of the project. A project manager, one who has previously demonstrated an ability to handle complex tasks (e.g., particularly information systems related, if available) should be selected to lead the project team. Team members should be representative of all major areas of the credit union and should be encouraged to fully participate in all decisions. Prior to forming the project team, serious consideration

should be given to the level of commitment required from team members and whether external help is needed. If so, it would be prudent to request this help as soon as possible since available resources will be limited as time passes. The use of outside help, however, does not relieve the credit union's senior management and board of their responsibilities to monitor and oversee the Year 2000 Plan. The dynamics may be somewhat different, but the approach should be the same.

Consultants, if needed, should come highly recommended and should not be novices to the Year 2000 arena. Any contractual arrangements should be thoroughly reviewed by senior management, the board, and a legal representative, if deemed necessary. While engaged, the consultant should be teamed with credit union personnel who will provide insight into the credit union's systems and processes. This arrangement will also ensure that senior management and the board will receive candid feedback regarding the team's progress and any barriers encountered. Consultants should be held to a high standard and should make senior management and the board comfortable with their approach, deliverables, and progress.

Overall, the project team should focus on these three major tasks: fixing the Year 2000 problem, testing the solution, and documenting their results and progress. Fixing the problem will vary, depending on your credit union's information system environment and the selected renovation approach. However, fixing the problem may entail a lot more than is readily apparent. For example, if you rely on in-house developed systems, and your strategy is to repair these systems, fixing the problem will entail not only identifying the affected code and making programming changes, but will also involve retaining programmers and ensuring that adequate documentation exists to support the changes made. If, on the other hand, your environment consists of systems provided by an outsourcing firm, also known as an information system vendor (ISV), the solution is altogether different. Your credit union's biggest challenge may be managing those vendors, including initiating letters to vendors of all critical systems requesting their:

- Year 2000 compliance status;
- estimated completion dates;
- methodology for the date change; and
- hardware infrastructure required to handle the change.

Testing and validating the Year 2000 technology solution entails ensuring your systems can properly handle both 20th and 21st century dates. Aside from the assessment phase, testing and validation is the most important phase of your Year 2000 project. It is critical that sufficient testing is done to ensure that your credit union will derive the expected results from any date calculations or manipulations including interest calculations, transaction postings, expiration dates, and payroll processing. You must also ensure that

embedded systems like elevators, security systems, phone systems, and HVAC systems will function properly past December 31, 1999.

One of the most significant issues related to testing is ensuring that interfacing systems will be able to communicate with one another electronically past December 31, 1999. It is senior management and the board's responsibility to ensure that internal and external interfaces will be able to handle shared date fields. If your internal and external systems use different date methodologies for the Year 2000 fix, a "data bridge", or interface, may be necessary to ensure that these systems will be able to communicate with one another before and after January 1, 2000. You may need to consult with a vendor or consultant to build such a bridge for your systems. This area has to be thoroughly tested to ensure that electronic data can be properly exchanged both within and outside of your institution.

The project team should maintain detailed records and meeting minutes. These records and minutes should document the steps planned or taken to address Year 2000 compliance from beginning to end, including functional and decision-making processes, vendor management, and expected and actual test results related to the fix. **Documentation is necessary in case the credit union ever has to defend itself with a vendor, member, sponsor, or other party. Also, your examiners will request and review documentation supporting your progress.**

Risk Assessment - Depending on the number of systems and devices in your credit union which may be potentially affected by the Year 2000, there may not be sufficient time to address every system you currently use. Therefore, it might be necessary to renovate only those systems that are required to stay in business (i.e., critical systems) past December 31, 1999. In fact, some of your critical systems that store future dates may have already begun to malfunction and need renovation. To properly address the Year 2000 issue, senior management and the board should make a decision about which systems will be renovated and which can wait until after January 1, 2000. Critical systems must be renovated; however, non-critical systems can wait. This approach may result in some inefficiencies and require possible "work-arounds." However, you should focus on saving the credit union, not saving the systems that may not provide much benefit.

Contingency Planning - As with other system implementation efforts that are date reliant, Year 2000 implementation efforts should include a contingency plan in case progress of the primary repair plan is impeded. A contingency plan provides an alternative path to follow to ensure that there is something in place at the time that the system is needed. The repair plan should define a specific point in time at which progress is measured to determine if the contingency plan should be activated. This trigger must allow sufficient time for the implementation of the contingency plan to be completed before December 31, 1999.

During the assessment phase, your credit union should have identified more than one option available as a solution to its Year 2000 data processing needs. One of these options, while probably not your first choice, may be a good candidate for your credit union's contingency plan, i.e., "Plan B." Simply put, your Year 2000 project team, senior management, and board should agree upon a date by which another course of action will be taken if all is not well with the original plan. After identifying a good alternative solution, your credit union's contingency plan should be documented in enough detail to include, at a minimum, the: (1) planned date of execution, (2) estimated time to implement, and (3) estimated cost to implement.

As with the original plan, the credit union should strive to implement the new, compliant system (identified in your contingency plan) in sufficient time to adequately test the system. For example, credit unions that rely on an in-house developed system may plan to renovate their systems in order to ensure Year 2000 compliance. During its fix, a credit union may run into difficulties that may negatively impact its ability to renovate the system. In this case, there should be a predetermined date by which the credit union should decide if it can indeed make the fix. As the date approaches, the project team may have fallen behind schedule and determine that they are unable to meet critical milestones and deliverables. Therefore, it may be necessary for the team to forego the renovation option and go to Plan B. Instead of renovation, the team may have previously decided that the contingency plan is to purchase a commercial off-the-shelf (COTS) application. As part of the contingency planning process, the credit union should have already identified, reviewed, and analyzed several COTS applications, and ranked those systems in order of preference, based upon credit union operations and needs.

Similarly, your credit union may be relying on a vendor's fix. If the vendor does not provide a satisfactory response as to its date of compliance or facilitate the testing of the fix by a predetermined timeframe, your credit union may also have to revert to Plan B. Your contingency plan may also be to purchase a COTS package.

Knowing when to revert to Plan B will be key as your timing could affect whether your credit union is in compliance in sufficient time to ensure adequate Year 2000 processing. The following timeline may help you to determine the amount of time you have available and when your Plan B should be put into effect.

NCUA Timeline

Time is of the essence. And remember, you have achieved **Year 2000 compliance when all of your critical systems have been either renovated or replaced and are able to process both 20th and 21st century transactions.** To evaluate whether your efforts, both past and present, are in line with NCUA's guidelines, review the following critical dates around which all of your Year 2000 activities should be centered:

September 30, 1997 - Credit unions should have completed the awareness and assessment phases of their Year 2000 plan.

December 31, 1998 - Credit unions' critical systems, at a minimum, must be renovated or replaced and tested for Year 2000 compliance.

September 30, 1999 - Credit unions must have implemented all new or enhanced systems necessary to process data for Year 2000.

December 31, 1999 - All critical systems must be operational.

This schedule, while aggressive indeed, especially if your credit union has not yet begun its assessment, only leaves one year following the completion of testing to ensure that at a minimum, your critical systems will be ready on January 1, 2000.

NCUA 5-Phase Repair Approach

NCUA has adopted the General Accounting Office's (GAO's) 5-phase repair approach to addressing the Year 2000 problem. Following are the 5 phases and the main activities that should occur during each phase. It should be noted that some tasks might be concurrent while others may be dependent on the completion of previous tasks.

Phase I – Awareness

Although the timeline indicates that the awareness phase should have been completed by September 30, 1997, in actuality, this phase should extend throughout the entire Year 2000 effort to keep everyone abreast of progress. During this phase, you must create and execute a strategy for defining and explaining the Year 2000 problem to everyone in your credit union including senior management and the board. This strategy should focus on enlightening the skeptics and enlisting the necessary support to address the issue. Someone with a high level of authority should be given this responsibility to communicate that the risk of non-compliance is one that the credit union will not tolerate and that senior management and the board are addressing the issue very seriously.

The credit union should also have a separate strategy and plan for addressing external Year 2000 communications. Inquiries related to the credit union's Year 2000 compliance efforts or status may be received from sponsors, members, or other external parties and should be anticipated by the credit union. All such inquiries should be forwarded to one individual who will be responsible for handling the inquiry in the manner agreed upon by senior management and the board.

Phase II - Assessment

As with the Awareness Phase, the Assessment Phase also should have been completed by September 30, 1997. The only way that your credit union will be able to determine the extent of your Year 2000 problem is to identify all Year 2000 problem areas. This can only be done after you have performed a detailed inventory of all systems, including hardware, software, operating systems, and any interfacing networks. The inventory should also include all devices with embedded dates, software vendors, suppliers, sponsors, and ISVs, as well as the credit union's processing capabilities with its payment system providers (e.g., ATM and ACH networks). During the assessment phase, you must solicit feedback from key credit union personnel to ensure that every affected system and component is identified and not overlooked.

The credit union must also evaluate the risk of non-compliance for all identified systems. Each system and device needs to be prioritized as:

- **mission critical:** must be converted or replaced to ensure continued functioning of the credit union after December 31, 1999;
- **essential:** should be converted or replaced to ensure minimal disruptions of the credit union's ability to provide services; and
- **non-essential:** support marginal functions and may be converted and replaced later.

If you can live without the system or device, retire it until after the Year 2000. Perhaps after the Year 2000 fix, you may be able to take the time to address the compliance of non-critical systems or devices. **However, due to the limited amount of time before the century change, it is essential to focus on the critical systems first.**

The process of identifying and ranking your systems should not be limited to a simple inventory of applications and platforms, but must also include assessments of the impact of systems failures on your core business areas and processes. To adequately assess and prioritize your credit union's Y2K issues, senior management and the board must approve the assessment and the list of credit union priorities. As a management group, they must determine the priorities for Y2K renovation, anticipate the impact of non-compliance on the credit union's on-going operations, and take the steps necessary to assure the credit union's viability.

During this phase of the project, you should also begin to contact, in writing, the following entities regarding their compliance status and strategies as well as their estimated date of compliance:

- hardware and software vendors;
- ISVs;
- embedded device manufacturers and suppliers;
- third-party servicers; and
- payment system processors.

This, of course, is not necessary for any system or device that your credit union, during its risk assessment, deems to be non-critical and plans to retire. If your credit union plans to use the system or device past December 31, 1999, however, these related parties must be contacted.

In your formal, documented request, you should ask that these external parties be as specific and detailed as possible about the date methodology that they will use to make their systems compliant. Further, you should request any information that they may have regarding how other methodologies will work with their option and whether they would be willing to do the necessary programming to "bridge" the two systems for your credit union. Bridging is necessary so that your interfacing systems will be able to communicate with one another after the fix, even if they use different date methodologies to resolve the problem. Date methodologies may include expansion, windowing, and compression as described below:

- The date expansion technique uses a "physical" approach to resolve the Year 2000 problem. Expansion requires re-coding dates with a four-digit year field, expanding the year field from 2 to 4 digits. Therefore, the century information is stored with the year information.

- The windowing technique uses an internal computer logic approach for interpreting dates. Based upon the 2 digit year, this approach assigns a century value (19 or 20) to the year value. As an example of this technique, two-digit year fields greater than 50 (pivot or base year) represent years in the 20th century – i.e., 84 refers to 1984; while two-digit year fields that are less than 50 represent years in the 21st century – i.e., 12

stands for the year 2012. Since there are no standards, the pivot year can be any number the vendor elects to use. To compound this problem further, the window technique may be a fixed or sliding (the pivot year moves) window. A fixed window is one in which the pivot year, once assigned, does not change. A sliding window is one in which the pivot year will move forward 1 year for each year that passes. For example, assume an initial pivot year of 35 and starting date of January 1, 1998; the pivot years are calculated as follows:

Date	Fixed Window Pivot Year	Sliding Window Pivot Year
January 1, 1998	35	35
January 1, 1999	35	36
January 1, 2000	35	37

- The compression (sometimes called encoding) technique is an internal computer logic approach which may use an algorithm or formula to compress numbers into a tighter space than is needed to hold "human readable" values. This method expresses numbers in a form that is understandable by the software, but not easily understandable by the average person. Another method of the compression technique is to use an alphanumeric character to represent the century. For example, "A" may represent 1900 and "B" may represent 2000. Therefore, in this example, A97 would translate to 1997 and B25 would translate to 2025. As a final note, the compression technique would require date fields to be converted from a "date format" to another format (such as alphanumeric).

During the Assessment Phase, a detailed project plan should also be developed and documented outlining:

- the resources and skill level needed to address each task;
- estimated timeframes for each task and an estimation of when the Year 2000 issue will be fixed;
- critical milestones which must be met or exceeded to ensure that the project is on target; and
- estimated costs.

Phase III – Renovation

Following the assessment phase, the resulting system inventories and application portfolios will provide a listing of Y2K impacted system components needing renovation. The repair or conversion consists of the renovation, replacement, or retirement of identified hardware platforms, applications, operating systems, databases, COTS packages, utilities, embedded devices, and internal and external interfaces. A renovation consists of modifying the existing system to conform to Year 2000 standards; a replacement involves the development of a new application to replace the one affected; and a retirement involves

the elimination of a system. The efforts during this phase involve making and documenting software and hardware changes, developing replacement systems, and decommissioning eliminated systems. Special consideration should be given to cost, age of hardware and software, availability of future vendor support, and the criticality of the system. Although this phase may take a significant amount of time, it is the least complex given that the repair options are expected to be relatively straightforward.

All changes to systems and their components should be made under the strictest configuration management to ensure that changes are adequately documented and coordinated. You should assess dependencies on external data and develop communication strategies and agreements for both internal and external data interfaces. These strategies may involve interim measures such as development of data "bridges" or conversion to Y2K compliant formats.

Another consideration during this phase is the prioritization of renovation for non-compliant processes. For example, depending on the volume of required changes and available resources, a decision may be made to change only those processes that are absolutely critical to day-to-day processing.

Phase IV - Validation and Testing

Testing may be the largest, single, most important effort within the Y2K Plan life cycle. **Credit unions should not take a vendor's, or third-party's certification of that vendor, assertions that a system is compliant...the system must be tested in the credit union's environment (the environment that the system will actually operate in after December 31, 1999).** During the validation and testing phase, each converted or replaced system component or device must be tested to detect any errors introduced during the renovation phase. All applications and the complex interactions between converted and replaced computer platforms, operating systems, utilities, applications, databases, and interfaces must be tested and proven to provide expected results.

In addition, the credit union's entire environment, including all systems, interfaces, and devices should be tested for operational readiness. The credit union should adequately test its capability to communicate electronically with external third parties, as well as its capability to handle critical processing for key dates including: February 29, 2000 (since 2000 is a leap year), March 31, 2000 (1st quarter-end), and December 31, 2000 (1st year-end). The credit union should also test its ability to display, print, input, and store dates. Systems inventories should be used to track Y2K test and validation progress and to ensure that quality standards have been met. Please refer to questions 43-49 of the attached *Credit Union Checklist* for additional insight on testing your repaired systems.

The credit union should document its test plan and the execution of that plan. Documented test results should be reviewed closely to ensure that tests rendered the expected results and that any errors have been documented and researched until their resolution. It is the credit union's responsibility to maintain test documentation for their systems. Test documentation should also be made available for outside review by accountants, examiners, or others who may request such in the future to support your efforts to ensure compliance.

Phase V – Implementation

Implementation of Y2K compliant systems and their components requires extensive integration and acceptance testing to ensure that all converted or replaced systems and devices perform adequately in real-time operating environments. This, too, may be a lengthy process. During implementation, repaired systems are rolled out to the end-user community and placed into production. All changes to work processes or system procedures should be adequately explained to the users during this phase. In addition, revised system documentation including user manuals and operator manuals should be made available at this time.

* * * * * * * *

The preceding narrative provides a general overview of the processes required to ensure Year 2000 compliance for your credit union. The following *Credit Union Checklist* provides an additional tool to assess your readiness. **However, completing the checklist is not a substitute for your Year 2000 documented plan for taking further action to assure that your credit union is ready for the Year 2000.**

CREDIT UNION CHECKLIST

Management Commitment

1. Has your board of directors and senior management team been apprised of and understand the risks and complexities of the Year 2000 problem?

2. Has your credit union estimated when the Year 2000 issue will affect it or has the Year 2000 issue already affected your systems?

3. Has your board of directors and management team anticipated the impact to the credit union's operations in the event that all systems are not Year 2000 compliant by January 1, 2000? If not compliant by January 1, 2000, what steps will management and the board take to ensure the credit union's on-going operations?

4. Has senior management and the board allocated sufficient resources (i.e., time, money, and people) to the Y2K problem?

5. Has it been mandated that all other projects, or at a minimum all information systems-related projects, are put on hold or given consideration only after the Year 2000 issue has been satisfactorily resolved?

6. If sufficient resources are not available within the credit union, has management obtained the necessary help from sponsors, consultants, programmers, other information systems professionals, or other credit unions?

Project Planning

7. Is your credit union following the GAO/NCUA 5-phase repair approach which consists of : (1) awareness, (2) assessment, (3) renovation, (4) validation and testing, and (5) implementation? If not, how are you ensuring that all phases of the fix will be properly addressed?

8. Has your credit union designated a project manager responsible for the Year 2000 fix? If not, how does your credit union plan on managing the fix? If so, has this individual previously demonstrated an ability to handle complex projects?

9. Has your credit union documented a project plan for addressing Y2K compliance by December 31, 1998 for all critical systems? Does the project plan include the strategy that will be used to renovate non-compliant critical systems (i.e., repair, replace, or retire) and critical milestones that will be evaluated during the project to ensure that your credit union's plan is on track? Does the project plan provide a means to chart and track critical tasks, assign staff, and estimate completion dates?

10. If a project plan has not been developed and documented, how will your credit union ensure that the renovation efforts will yield the desired results and that all required tasks have been identified, assigned to the appropriate staff, and estimated to be completed by deadlines outlined in NCUA's timeline?

11. If your credit union's initial plan can not be achieved by December 31, 1998, have you documented a contingency plan for addressing Y2K compliance for all critical systems? What events will trigger the execution of this contingency plan? Will its execution ensure compliance by December 31, 1998? When is the absolute latest date that the contingency plan will be put into effect?

12. How are management and the board monitoring Year 2000 compliance efforts? At a minimum, are periodic reports provided to management and the board apprising them of the status of the credit union's compliance?

Year 2000 Assessment

13. Has your credit union performed and documented an assessment of its risks related to the Year 2000? Did the assessment include a detailed inventory of all systems and devices potentially affected as follows:

    - critical applications that were developed in-house or customized packages;
    - critical turnkey applications or applications outsourced to information system vendors;
    - other critical significant packaged applications (e.g., PC-based applications);
    - computer hardware, operating system software, and networks;
    - an inventory of devices with embedded dates, (e.g., ATMs, audio response systems, elevators, vaults, alarms, time clocks, heating, venting and air conditioning units, lighting systems, fax machines, and telephone systems); and
    - non-critical systems and devices?

14. Have you identified which of these systems and devices are critical to the on-going operations of your credit union and have to be repaired? What are these systems? Which are non-critical and can wait for their repair until after January 1, 2000?

15. Are you addressing Year 2000 compliance for critical systems and devices only? (You should address compliance for non-critical systems only after critical systems are repaired, tested, and operational.)

16. Has management and the board reviewed and approved the Year 2000 assessment and prioritization of critical and non-critical systems?

17. How many of the critical systems and devices are Year 2000 compliant? Which are not Year 2000 compliant? Are you measuring the system's or device's compliance on its ability to process Year 2000 transactions today, including critical interfaces?

18. If systems are deemed compliant, did you make this determination through validation and testing and not from vendor assertions?

19. For non-compliant critical systems or devices, or those that are claimed to be compliant but not yet tested by your credit union, does the assessment estimate how many hours it will take to correct the problem and test for compliance?

20. Does the assessment also include estimated costs, resources needed, skill level needed, and other information that will be influenced by the Year 2000?

21. Does the assessment address whether the credit union has sufficient financial resources to make all hardware (e.g., mainframe, midrange, networks, personal computers) and related application and operating system software changes to ensure Year 2000

compliance by December 31, 1998 for all critical systems? If sufficient financial resources are not available, what is the credit union's strategy for obtaining the funds required to do the Year 2000 fix?

22. For credit unions with in-house developed systems, does the assessment estimate lines of code affected and costs per line of code? Does it also address the amount of time needed to identify all date fields, make the necessary corrections, and make programming changes required to bridge critical interfaces?

23. For credit unions with critical systems that are developed in-house, will systems be repaired and tested on the credit union's hardware by December 31, 1998? If not, what is the credit union's contingency plan and will it result in a compliant system that will be tested on the credit union's hardware by December 31, 1998?

24. Does the assessment also include the impact of Year 2000 processing capabilities with your critical payment systems providers (including possible penalties if unable to communicate electronically), such as:

    - wire transfer system;
    - automated clearing houses;
    - share draft processors;
    - credit card merchant and issuing systems;
    - automated teller machine networks; and
    - electronic benefits transfer systems (internal and external)?

25. Does the assessment also include non-computer related services (e.g., armored car servicer's automated cash shipment), which are essential to the on-going operations of the credit union?

26. Has your credit union prepared an enterprise schematic, which depicts all systems as well as any internal and external interfaces?

27. Does the schematic highlight systems and interfaces which are critical to the on-going operations of the credit union?

Vendor/Sponsor Communications

28. For credit unions serviced by ISVs, or for those using vendor or sponsor systems, are critical software or applications currently supported by the vendors or sponsors?

29. Have you begun to contact vendors, sponsors, third-party servicers, and manufacturers to determine whether they claim that their products or services are Year 2000 compliant? (This might also involve contacting the leasing company of the credit union's building.)

30. Do your letters to these vendors/sponsors include a request for the date methodology that will be used to correct the Year 2000 problem (i.e., date expansion, windowing, or compression)? If the vendor is using windowing to correct the problem, are they using a fixed or sliding window? What pivot or base year is the vendor using with their chosen windowing technique?

31. Have you determined how interfacing systems will handle shared date fields? If vendors or sponsors of critical interfacing systems are not using the same date methodologies, have you requested that a vendor, sponsor, or independent party build a "data bridge" to ensure that these systems will be able to communicate with one another on January 1, 2000?

32. Does the letter to the vendor or sponsor also include a request whether the hardware and operating system will perform as specified?

33. Does the letter request that the vendor/sponsor disclose the estimated date of delivery of the compliant system to your credit union?

34. Have you determined whether the estimated dates of compliance and delivery will provide you with sufficient time to ensure that the renovated systems will be adequately tested by December 31, 1998? If not, what is your contingency plan?

35. If vendors have not responded to initial requests, have you considered sending a letter from a legal representative?

Contingency Planning

36. If the vendor letter is not eventually answered, or if the compliant system is not estimated to be delivered in sufficient time to ensure adequate testing by December 31, 1998, what is your credit union's contingency plan? Will the system identified in your contingency plan be tested for compliance on your credit union's hardware by December 31, 1998?

37. If your credit union has an existing contract with the vendor referred to in #31 above, have you contacted a legal representative to determine your recourse if you have to resort to an alternative processing solution due to the vendor's non-compliance or inability to provide a compliant system which has been tested on your credit union's hardware by December 31, 1998?

38. If sponsors have not responded to requests or have indicated that their systems will not be renovated, have you identified an alternate system for all critical processing currently done on a sponsor-provided system? Will this alternate system be tested for compliance on your credit union's hardware by December 31, 1998?

Acceptance of Compliant Software

39. For critical systems that are both non-compliant and not currently supported, how will your credit union ensure receipt of a compliant version of the application or software? Will these applications and software be tested for compliance on your credit union's hardware by December 31, 1998? If not, what is your credit union's contingency plan, and will this plan result in a compliant system which will be tested on your credit union's hardware by December 31, 1998?

40. If your credit union is not using the most recent version of vendor software, have you confirmed with the vendor what effort will be necessary to convert to the compliant version (i.e., will you have to upgrade to multiple incremental versions before implementing the compliant version)? Will this software be tested for compliance on your credit union's hardware by December 31, 1998? If not, what is your credit union's contingency plan, and will it result in a compliant system, which will be tested on the credit union's hardware by December 31, 1998?

Project Management

41. How is your credit union tracking program changes as they are made or received to repair non-compliant systems? Are procedures adequate to ensure the orderly turnover of older, non-compliant versions of software, and are these changes properly controlled and documented as they are implemented?

42. Has your credit union considered the risk that critical personnel may not remain at the credit union through the entire Year 2000 fix (i.e., programming staff, Y2K project manager, and knowledgeable staff)? Have you considered possible incentives, bonuses, or other agreements to ensure key personnel remain employed at the credit union?

Testing

43. Has your credit union documented a test plan for ensuring that all systems to be used on January 1, 2000 are Year 2000 compliant?

44. Prior to testing your systems for Year 2000, has your credit union practiced its back-up and restore procedures to ensure that production data can be restored and that the Year 2000 testing will not negatively impact live processing?

45. Does this test plan involve testing transactions on the identical systems that will be used by the credit union on January 1, 2000?

46. Following the back-up and restore procedures and during the actual test, will the operating system clock be set to a date in the Year 2000 and transactions tested using dates in the 20th and 21st centuries? In addition, does the plan include:

    - all critical transactions and processes;
    - testing criteria;
    - expected results;
    - test data;
    - review of any input, display, or storage of dates;
    - estimated dates of testing; and
    - testing completion dates?

47. Will testing of all critical systems for Year 2000 compliance be completed by December 31, 1998?

48. Will or has your credit union maintained written test results which highlight any errors noted during testing, research performed on these errors, and their ultimate resolution?

49. Will or have users been involved in system testing, including providing user acceptance criteria?

Training

50. Have personnel been trained for changes in procedures or the implementation of manual procedures resulting from:

    - errors noted during Year 2000 testing;
    - systems that were not repaired for Year 2000 compliance;
    - functionality that may have been replaced or not addressed during the Year 2000 repair; and
    - system reports and screens that may be altered or not available due to the Year 2000 fix?

Documentation

51. Has all documentation relating to your credit union's Year 2000 compliance efforts been safely stored on-site and off-site? Does the documentation include the:

    - assessment and detailed inventory of systems and their components;
    - project plan and project team minutes;
    - contingency plan;
    - correspondence from and approvals by senior management and the board;
    - any correspondence between the credit union and any third party regarding Year 2000 compliance (e.g., vendors, sponsors, manufacturers, third-party servicers);
    - agreements and any other correspondence between the credit union and any external parties engaged to assist in the Year 2000 project; and
    - testing documentation including the plan, the results, and any follow-up?