

# Farm Credit Administration

1501 Farm Credit Drive  
McLean, Virginia 22102-5090  
(703) 883-4000

---

## INFORMATIONAL MEMORANDUM



June 30, 1998

To: Chairman, Board of Directors  
Chief Executive Officer  
All Farm Credit System Institutions

From: Roland E. Smith, Chief Examiner  
Office of Examination

Subject: Contingency Planning for Business Continuity

The Year 2000 problem can cause operational failure for a Farm Credit System (FCS or System) institution in two ways. First, any or all of the institution's systems could fail or may not be Year 2000 ready by January 1, 2000. Second, even if the institution is Year 2000 ready, other entities (i.e., utilities, other financial institutions, etc.) that the institution interfaces with could adversely impact the institution's operations if those entities are not fully Year 2000 ready. Therefore, the board of directors of each FCS institution should establish a contingency plan to ensure business continuity after December 31, 1999. Such a plan must be in place by December 31, 1998.

The development, validation, and implementation of the Year 2000 contingency plan should be a high priority of the board of directors and senior management. Each System institution must evaluate its own unique circumstances and environment to determine the actions necessary to ensure the continuity of operations after December 31, 1999. For that reason, the plan should cover a reasonable period of time into the Year 2000. The board should also ensure that management periodically reviews, updates, and validates the plan.

Attaining Year 2000 readiness is one of the most complex and challenging issues facing an institution's board of directors and senior management. FCS institutions may expend substantial resources to renovate or replace mission-critical systems; yet, despite this effort and commitment, the risk of disruption to business processes remains. A Year 2000 contingency plan should be designed to provide assurance that the mission-critical functions will continue if one or more systems fail.

The plan will need to address one or both of the following possibilities:

- Risks associated with the failure of the institution to successfully complete renovation, validation, and implementation of its systems at critical dates.
- Risks related to the impact of external systems, including service providers, software vendors, other institutions, customers, business partners, etc.

Each institution should evaluate the risks associated with the failure of core business processes. Core business functions or processes of an institution are groups of related tasks which must be performed together to ensure that the financial institution continues to be viable. Evaluation of these risks should include comparing the cost, time, and resources needed to implement the contingency alternatives.

### **Organizational Planning Guidelines**

The development of a contingency plan requires consideration of numerous factors. The comments that follow are intended to assist the board of directors and senior management in the development of a contingency plan but may not fully address a particular institution's situation. While the production of the document may be delegated to staff, the board of directors and senior management must be cognizant of the plan's content including the business continuity strategies to be used.

Each System institution should develop a timeline of events that incorporates the schedule of renovation and testing in the institution's Year 2000 plan. Critical stages must be identified, assessed for feasibility of implementation, and updated as necessary.

Business risks should be prioritized with the contingency planning efforts focused on the core business processes that, should they be compromised, pose the greatest risk to the institution. Year 2000 readiness risks should be identified and a system developed that provides an adequate means of reporting progress and changes in the Year 2000 plan.

To develop a contingency plan, the institution will need to assess the potential impact of mission-critical system failures on the core business processes. A risk analysis of each core business process should be made, and the following should be considered in such an analysis:

- The status of Year 2000 readiness renovation or replacement plans for mission-critical systems, whether administered internally or by service providers;
- The financial and marketing impact of the loss of a core business process, including what impact the loss might have on the viability of the financial institution; and
- The impact of regulatory requirements.

The analysis also should define and document Year 2000 failure scenarios. The risk of both internal and external failures should be considered. The results of tests run on renovated systems may lead to the development of the failure scenarios.

FCA recognizes that a contingency plan to ensure business continuity may need to change because of subsequent events or the loss of key staff members. Periodic tests of the plan may ensure that changes are made when appropriate and that the level of support for the core business processes is adequate.

The guidance provided in this Informational Memorandum is consistent with the GAO statement entitled “Year 2000 Computing Crisis: Business Continuity and Contingency Planning,” released in March 1998 (GAO/AIMD-10.1.19 at [www.gao.gov/special.pubs/publist.htm](http://www.gao.gov/special.pubs/publist.htm)). Also, the FCA Home Page ([www.fca.gov](http://www.fca.gov)) contains links to other sources of helpful information.

Questions pertaining to this document should be directed to Thomas M. Glenn, Director of Operations, Office of Examination, at (703) 883-4412. Contact may also be made at the following e-mail address: [glennt@fca.gov](mailto:glennt@fca.gov).