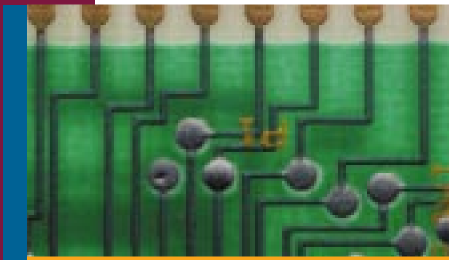

A Year 2000 Prioritization Scheme for Your Business Operations

BY LOUIS A. MASCELLI

In order to ensure that Y2K problems will be effectively resolved by the turn of the century, it is important that you determine the type and degree of risk that is associated with your business operations and the mission criticalness of each system.

EVERYONE is aware of and working diligently to ensure that Year 2000-related problems will be effectively resolved by the turn of the century. In spite of the hard work being done to test systems for Y2K changes, we must anticipate that some things will be overlooked, ignored, or simply not completed on time. We must also realize that there are things beyond our control that could affect this effort. Due to the tight timeframe (less than 15 months before the turn of the century), your business operations should focus on those systems with the greatest risk of causing Y2K problems for critical missions.

In order to do this, it is necessary to understand the type and degree of risk that exists in this peculiarly unique endeavor. For example, there may not be enough resources to test everything. Some solutions may not be available or work in time because they will be too complex, too costly, or implemented incorrectly. Additionally. testing according to predefined and pre-developed test plans may not be thoroughly implemented.

This article is based upon established Year 2000 business practices performed for clients of my consulting firm, LAM & Associates, LTD.

TRIAGE: THE RECOMMENDED APPROACH

My colleagues and I recognize that no matter what priority criteria are used, a lower priority system may be ready before one with higher priority. Obviously, if resources are available, the system should be tested and advanced. However, because of the number of Year 2000 projects in your business' operations area, we believe that Year 2000 testing should be prioritized based on a triage approach. This means identifying applications that are mission-critical and must be completed at all costs as well as distinguishing applications that have a contingent manual workaround solution from those that do not.

In making a triage evaluation, an important element to consider is the level of risk that exists in each facet of this endeavor, particularly within each of your information technology (IT) legacy systems, your standalone outside vendor business systems, and each of your in-house developed PC/LAN-based business systems. The major sources of risk include (see Figure 1):

- technical risk due to the complexity of your applications and the number of interfaces with other systems, clients, vendors, and other external entities

Figure 1: Types of Risk

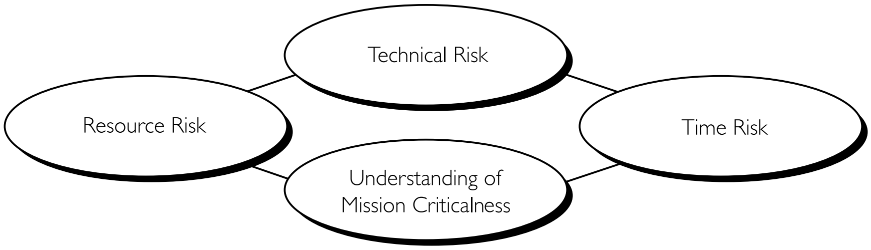

Figure 2: Technical Risks

Risk Factor	Recommended Action
1. Significant and repeated slippage in completion dates for correction or replacement testing.	• All correction activity should have been completed by the end of 1997. Remediation activities should have been completed around June 1998. This will create a major bottleneck for testing during the third and fourth quarter 1998.
2. Incomplete awareness of the Y2K issues in end-user departments.	• Upgrades should be made to packaged software releases that deal satisfactorily with Year 2000 dates. Applications should be remediated with Y2K compliant "middleware." • Compilation of an up-to-date inventory of significant user-written and existing vendor application software is still an ongoing activity. • Identification of software that will not be Year 2000 compliant is ongoing while PC hardware is upgraded.
3. Late recognition of interfaces between systems.	• All interfaces between systems should have been recognized by now as part of the system inventory. We continue to ferret them out as we develop test plans. This introduces previously unknown dependencies in the system being tested and the ones to which it interfaces.
4. Since Y2K compliance testing activities have not been prioritized during the remediation process, the more important systems or those that will fail early/first have not been adequately recognized.Procedures to rearrange priorities according to importance to the organization are not in place.	• The priority for dealing with various systems probably should have been created immediately after the initial inventory and remediation process. By now, there should be in place a prioritized schedule of Y2K compliance testing.This schedule should be subject to regular weekly monitoring and should change as circumstances change. This monitoring should particularly consider interfaces between systems. • Any prioritization scheme should be based on those systems with possible early failure dates and those that are highly critical. Highly critical systems should have been renovated first.
5. Not all environmental software has been recognized nor has testing for MVS, client/server, or other platform operating system software been assigned to a single group.	• Different tools might be (or might have been) used to identify application dependent software during PC hardware compliance efforts. Even now, using different tools (those that may "learn"new occurrences) might be helpful. • A single, central group should be responsible for testing all "middleware." Identifying these as application owner concerns wastes significant time.
6. Upgrading and enhancing along with the Year 2000 changes.	• Strict guidelines on enhancements should be given to individuals working on the conversion effort. • It should be possible to design enhancements during Year 2000 work but, unless the changes are essential, their development should be postponed. • The prioritization process should determine whether enhancements are essential.
7. Maintaining compliance in renovated and newly developed systems.	• Year 2000 testing requirements must be included for all new systems developments/enhancements. • Software developers must understand what is and is not Y2K compliant (for example, MS Access 2.0).
8. Business application test bed facilities and test data do not exist in many systems.	• Standard testing practices do not work for Y2K testing, therefore, time must be expended in developing for each project a test bed applicable to the developed test suites.

- resource risk due to the shortfalls in the availability of facilities, and the availability, capability, technical skill sets of people

- time risk due to an immovable deadline

As triage principles are applied, some low priority systems may not be tested at all. Some medium priority systems may not be thoroughly tested. Finally, even after thorough testing, some mission-critical systems may still have errors due to complexities and oversights.

OBSERVATIONS AND CONCERNS

To apply triage criteria, users of each business system must establish its mission criticalness based on the importance of the system (or group of systems) to the organization. This should be based on an estimate of the operational impact of errors in date-dependent data generated and used by the system, passed on to another system, or received from another system.

The following categories and criteria should be set up to determine the level of criticalness.

Mission Critical: Failure of the system to operate, to complete operations, or to give correct responses can cause one of the following "showstoppers":

Figure 3: Resource Risks

Risk Factor	Recommended Action
1. Possible confusion with respect to roles, responsibilities and authority of business users, owners and testers.	• Identify where roles are different than normal operations. • Establish lists of critical skills among personnel. • Users and their testers have limited testing experience. Historically, outside sources have performed this function for them. There seems to be too much new activity in each business area overburdening the limited resources of knowledgeable personnel (is a particular concern).
2. Possible that the organization's resources are insufficient to meet the needs.	• The ongoing assessment of the scale of the possible shortfall in resources should be reassessed in light of findings during remediation conversion. • Comparisons between planned and actual resources should be monitored and the assessment algorithm updated as needed. • Long-term arrangements should be made with contractors as appropriate.
3. Possible loss of key people..	• Documentation generally does not exist.Where it does exist it is often outdated.System knowledge, and, by inference Y2K testing, depends on the people who use the systems. • Reward schemes may be considered to retain people up to the Year 2000.
4. Staff performing Year 2000 changes may have inadequate training.	• There should be an assessment of skills needed after the methods and tools to be used have been determined. • Plans for training should be included in the overall plans (particularly for business systems, which provide money flows, as CHIPS and ACH/PEP+).
5. It may be difficult to obtain good outside help.	• Getting outside resources has become an issue. Contract now for possible future needs.
6. Possible difficulty securing an appropriate test environment.	• Because your remediation schedules have slipped, there will be excessive demand for testing facilities through the end of 1998. An overseer committee or group should be created to manage scheduling. The systems requirements should be identified during test planning. • These requirements should account for all resources including office space, personnel (determined with the business users), machines (mainframe, servers and PC/workstations) and networks. • Test systems will also require support from technical and help desk staff.
7. Possible lack of sufficient resources will cause a shortfall in user testing.	• This overseer group should schedule business user testing. Because they lack expertise in this area, users will require significant assistance to determine test data. • Many project managers are inexperienced with major testing projects. This is particularly true with respect to test data preparation and outside entity coordination.
8. Possible difficulty performing integrated testing (including external interfaces).	• Testing partners may not be ready. To date, not all interfaces have been identified.Current schedule slippage will introduce timing problems. The overseer group should be charged with assuring that such integrated testing is scheduled.
9. Possible status reporting problems.	• The Y2K project structure should clearly define reporting lines and accountability. • Responsibility for monitoring progress should be clear, as should the circumstances under which problems should be escalated for decision by senior management.

- immediate shut down of direct operations
- a security breach

No operational workarounds can be devised to avoid these consequences.

Medium Priority: System generates date information that is used by people only, with no automatic or machine/magnetic interfaces. System delays or failure to operate will not cause showstoppers or failure of the operations.

Low Priority: The system does not receive, use, or transmit dates. There is an operational manual workaround to bypass this system by eliminating its automatic function.

Also, factor in the following types of risk associated with various systems:

Technical Risk - This is due to difficulty in resolving the Year 2000 problem for an application. The size, complexity or

Figure 4: Time Risks

Risk Factor	Recommended Action
1. Possible misidentification of dates describing program contingencies. There may be an over-reliance on replacement system projects that have a tendency to exceed planned delivery time and are, therefore, a high risk.	• Ensure that those dates upon which the final end date depends are clearly identified and monitored. • Timelines whose change may trigger specific actions must be monitored. Contingent actions should be defined if milestone dates are missed. Examples are Correction, Y2K Date Rollover Testing and Y2K External Interface Testing.
2. Possible misidentification of time and resources required for testing (including third-party software "vendor certified"as compliant).	• Detailed testing plans should be incorporated into an overall plan and managed by a business unit test group. Plans should be based on industry estimates indicating that 50 percent to 60 percent of the total time should be allocated to this phase.
3. Possible processing problems at key dates when vendors, clients and other external entities may not be available.	• Ensure appropriate levels of live support are in place for internal and external Y2K interface testing.

the number of interfaces a system has with other systems may cause increased technical risk. Systems with high technical risk require careful monitoring. A banking demand deposit (DDA) application is one example of this type of system.

Resource Risks - This is due to a shortfall in the available resources such as people, facilities or support contracts. Of course, these are the "usual suspects" in any project, but in this project resource issues seem to be acute.

Time Risk - This is due to the short period available for the resolution process,including validation, verification and certification of Y2K changes.

The tables in Figures 2 through 4 detail these risks and, where possible, suggested methods to alleviate them. Since technical risk is legitimately the province of other areas, we have described here what we perceive to be the source of risk and what we would do (or would have done) differently.

CONCLUSION

Understanding that all systems automate some business process and are important to each business owner, specific contingency planning is needed in order to be fully prepared for Year 2000. Single application system managers cannot make the type of contingency decisions suggested here; more senior management must make them. For example, devising operational workarounds involving more than one system or establishing resources that can be shared by several systems may be required. A joint test may be necessary among interfacing systems to allow them to complete the verification process in time. A central facility might be established with resources to perform analyses on systems that can be tested in tandem. This would reduce resource risks for individual systems. Similarly, resources for devising solutions for similar configurations of hardware and software could be shared with a reduction in resource and time risks.

Year 2000 testing should be prioritized based on a triage approach. This means identifying those applications that are mission-critical and must be completed at all costs, those that have no contingent manual workaround solution, and those which have a contingent manual workaround solution.

When there are insufficient resources for all programs (and no matter what is done, there is not enough time), some form of triage is necessary. Performing a triage assessment on your business operations systems should help to alleviate the risk in completing Y2K testing.

Time is short. With the Year 2000 quickly approaching, you may want to ask yourself whether you are on track to provide goods and services to your customers without disruption. Will your organization be Y2K compliant on time? ts

Louis A. Mascelli is principal of LAM Associates, LTD., in Cambridge, Mass. His special interests in Year 2000 projects include application definition and analysis, methodology, risk management, contingency planning, testing, Year 2000 tools, and all aspects of project management. He can be contacted at (617) 225-2026, or email at lamm@mediaone.net.