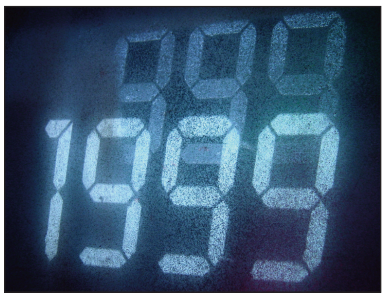
Note: A Decilog affiliate participated in the following project.

Year 2000 (Y2K) Contingency Planning

CHALLENGE



In the late 1990s, there was considerable concern that computer software could not handle the date change from 1999 to 2000 correctly. The testing of a number of software products and custom-built software verified that this was a serious issue and that, if not remediated, serious and even catastrophic failures might ensue. As a result, a huge remediation effort was initiated. Nevertheless, there was still concern, because of the enormity of the effort, that a considerable number of date errors remained.Consequently many organizations and industries developed contingency plans to handle system failures.

APPROACH

In order to derive effective contingency plans, it was necessary to try to anticipate all the different components that could be affected and how severe the impact of a computer-program error might be. This required building an inventory of all computer and network applications, system software and hardware, other equipment, facilities, business processes and their dependencies. The inventory items were then classified as to criticality to the business.

It was then necessary to determine the risk level and potential impact of failure for each component and process. This involved surveying all involved parties as to their estimates of the losses that would be incurred if the various systems and processes were unavailable or did not work properly. Depending on the results of the survey, contingency plans were developed to reduce the impact of a failure.

BENEFITS

By assessing the risks of a negative event related to specific systems and processes, the organization was able to develop contingency plans and assign responsibility for developing and testing procedures in the event that the primary systems were not available due to residual errors. This allowed stakeholders, including senior management, partner organizations and customers to feel a higher level of comfort that the organization was well prepared for adverse events.

RESULTS

While the additional precautions, such as having staff monitor systems over the millennium weekend, and relatively few serious incidents led to a relatively uneventful Y2K transition period, there was a greater degree of confidence that organizations were prepared in the event of failures of systems and facilities that might have resulted from programming errors.