1. INTRODUCTION

1.1 The Year 2000 is a global challenge. Whether the financial industry has the ability to rise to this challenge and avoid serious difficulties as the date change occurs will be determined by the actions that individual firms and the financial community have taken and the steps they take between now and the eve of the Year 2000. It is the responsibility of management of each organisation to identify and address their Year 2000 risk exposures. To delay work on the issue harbours the risk as not all the code modifications, testing and other changes can be carried out at the last minute. It is equally important that contingency plans are drawn to ensure smooth functioning of the financial sector. Unlike most projects involving technology, the certainty of movement from 1999 to year 2000 makes it impossible to delay the finality of preparedness of all computers to meet processing needs of the next century.

1.2 Unfortunately, the Year 2000 issue is not always presented properly. Routine observations that the problem is exaggerated and not worthy of the attention dilutes the real dimension and the likely impact of non-compliance. Conversely, alarmist scenarios bring about unnecessary panic. Such extreme views often fail to provide the key to deal with the problem. With regard to the issue of Year 2000, each financial institution has to bear responsibility for its own systems. However, supervisors should be able to assess whether the steps being taken by financial institutions to achieve Year 2000 readiness appear to be reasonable and prudent. It is essential that senior management recognise that the Year 2000 is more than a technical issue and that they become involved in ensuring timely resolution of the problem. The financial institutions that have not yet begun the Year 2000 renovation process would find it difficult, if not impossible to change the internal systems and interface with others. Institutions that have not progressed sufficiently should quickly focus on identifying and renovating those systems that are deemed to be "mission critical". All financial institutions, regardless of their level of preparedness, need prioritise work yet to be done and initiate a contingency planning process.