3.1 GOVERNMENT COMPUTER ENVIRONMENT AND CONTROLS

Background

The Government of Bermuda relies heavily on its computers and computer systems. The central computer systems, in particular, are crucial to its ongoing ability to function administratively and to provide services to the citizens of Bermuda.

Audit scope

The audit examined the computer environment, the main applications systems and the general computer related controls of the Government's central computer systems. It focused particularly on entity-wide security, access controls, systems development and change controls, system software controls, segregation of duties, and service continuity arrangements. The controls were reviewed for appropriateness of purpose and design though, in many cases, the work did not extend to testing fully the operation and effectiveness of the controls.

The work was conducted in conjunction with KPMG, Chartered Accountants, whose assistance in this regard is gratefully acknowledged.

The Government's Central Policy Unit is currently developing a strategy to enable the Bermuda Government to take advantage of electronic methods to administer its internal affairs efficiently and to provide better service to the public (E-Government). I have provided the Unit with a detailed copy of the audit report for consideration in its work.

Summary conclusions

As a result of this work, I concluded that the great majority of the controls reviewed are adequately designed to prevent, detect, or mitigate the risks they were designed to address. In some cases I made recommendations to further improve these controls. In the cases described below, I concluded that control or related procedures are inadequate and are deserving of immediate attention:

Information technology risks

No risk assessment or impact analysis has been performed recently to identify the extent to which available information technology resources could constrain the achievement of Government plans and objectives.

Technical support for Government's network needs strengthening…

The Government's information technology infrastructure has evolved over the years from a typical mainframe computer environment to a network environment. Evolution like this calls for changes to the information technology infrastructure and the

way it is managed. It also calls for changes in technical support and controls. To some extent, these changes have not occurred within the Government of Bermuda. For example, the number of users with access to the network has doubled during each of the past three years, yet the Computer Systems and Services Department (CSSD) has received no additional resources to support this increase in users.

...and is below industry standards

CSSD's technical support staff now number considerably below industry standards, with the result that user problems often cannot be resolved promptly. The risk of this adversely impacting the operational efficiency of users increases as their needs and environment become more sophisticated. More technical support with high levels of knowledge and expertise is needed.

Controls need to evolve as technologies and risks evolve

Another risk that increases in an evolving information technology environment is that controls do not evolve to correspond to the changing technical infrastructure. This can render data and systems vulnerable to loss or interference, thereby threatening administrative operations and even Government services. An example of these risks is internet connections through which external parties can gain access to the Government network, data and programs.

A full understanding of all significant threats to Government operations and services is a necessary prerequisite to designing a comprehensive program of security controls. Periodic risk assessments and impact analyses should be performed to provide this understanding.

Recommendation 2

The Computer Systems and Services Department should initiate periodic information technology risk assessments to identify all important risks and the potential impact of those risks on Government resources and operations. The results of such risk assessments and impact analyses should then be the basis for updating information technology security policies and controls.

Department response

Industry standard security measures are in place. It is agreed, however, that security measures will be reviewed and enhanced using the ISO Security Standard as a guide. Then a third party review will be performed to identify risks so that decisions can be made on the cost-benefits of implementing further protective measures.

(For a response reflecting progress achieved toward the

recommendation since the initial response was submitted, see Appendix 14.)

Recommendation 3

Based on a sound assessment of current and future technical network support needs, together with a projection of the resources needed to support known and anticipated new system implementations in the near and mid-term, the Computer Systems and Services Department should inform Government of its technical support needs, and the potential impacts of failure to provide them.

Department response

Agreed. To some extent, a solution is in progress and a review of the Department's structure and resources is underway. Cabinet has approved three new positions for 2001 and four other previously frozen positions will be released and filled thereafter. The ongoing review will determine whether this will be sufficient.

Senior level representation

There is a risk of major program decisions being taken and perhaps announced before the full information technology and related cost issues are fully understood.

IT needs and costs should be factored in policy decisions

Increasingly, major Government decisions on program directions and operating strategies have significant information technology implications. However, the Director CSSD, who reports to the Minister of Telecommunications and E-Commerce, is not formally represented when many of these senior level decisions are reached. As a result, programs or strategies can be agreed and announced without decision-makers knowing whether the necessary information technology infrastructure and support can be in place when needed, or what it will cost.

A related concern is that the Director CSSD is not aware at the earliest possible date of future user needs arising from senior level decisions. This delays his ability to plan for the needed infrastructure and people. New decisions affecting the information technology environment need to be integrated promptly into longer-term information technology plans, otherwise successful investment and business goals can be jeopardized.

Recommendation 4

To enable important Government business decisions to take into account the full information technology and related cost implications, the input of the Director of the Computer Systems and Services Department should be obtained, either through the Central Policy Unit or other medium.

Department response

The process by which project concepts and major initiatives are reviewed by Cabinet prior to approval may represent an opportunity for providing the input recommended.

(For a response reflecting progress achieved toward the recommendation since the initial response was submitted, see Appendix 14.)

Auditor General's comment

Before the audit was completed, the Central Policy Unit of the Cabinet Office was asked for comment on this and certain other recommendations in the draft audit report. The Secretary to the Cabinet responded that this was among the issues being addressed but that, at that time, it was premature to declare the Unit's views.

Disaster recovery

There are weaknesses in the Government's disaster recovery and business resumption arrangements as they relate to computer resources.

In today's world, disaster recovery and business resumption plans need updating regularly

The horrendous events in New York and Washington on September 11 illustrate graphically the importance of disaster recovery and business resumption plans. In Bermuda, the loss of computer facilities and programs resulting from disasters such as fire, flood or hurricane could impact significantly the Government's ability to function for extended periods. They could also potentially damage the Bermuda economy.

The Bermuda Government has disaster recovery plans and arrangements which, in most significant respects, should ensure the protection and swift recovery and operation of its computer programs and data. These plans were reviewed prior to Y2K and no mission-critical applications were identified.

The ready availability of computer programs and data can be achieved by frequently storing copied versions of them off-site in disaster resistant facilities. If the live versions are lost, the copied versions can be up and running in a reasonably short time.

Back-up equipment can be expensive, but so can its unavailability if disaster strikes

However, ensuring the ready availability of computer equipment (computers, switches, servers, etc.) can be more difficult. One method is to have two physically separate processing facilities each with enough capacity to handle the most important processing until the other location can operate again. A disadvantage of this method is that it involves considerable redundancy of expensive resources. A second method is to arrange for processing to be handled by another processing

facility, though this method has limited application in today's network environments.

The Government of Bermuda has two separately located processing facilities. However, their processing capabilities are linked in a way that the destruction of one facility could render the other facility incapable of operating the Government network. In effect, therefore, the second facility is not an effective back-up.

Recommendation 5 **The Government's Central Policy Unit should weigh the potential risks and costs arising from the loss of data processing facilities caused by a major disaster against the costs and redundancies associated with having two totally separate processing facilities each with enough capacity to service the Government's most important needs for a reasonable period of time. Recommendations should then be made to Government on how to handle this issue.**

Department response *A level of redundancy for IT infrastructure is already in place and a plan to enhance the system will be put to Cabinet in 2001. The present plan and proposed improvements are designed to mitigate the risk of technical failures. It will be reviewed with the Accountant-General and Cabinet Office to consider disaster recovery and business continuity concerns.*

(For a response reflecting progress achieved toward the recommendation since the initial response was submitted, see Appendix 14.)