NATIONAL ASSEMBLY

QUESTION FOR WRITTEN REPLY

QUESTION NUMBER 1686

DATE OF PUBLICATION: 28 MAY 2010

Mr M H Steele (DA) to ask the Minister of Finance:

(a) What guidelines has he issued to national departments with regard to the implementation of the new Integrated Financial Management System in respect of (i) maintenance of data integrity, (ii) security of access by employees of the particular department and (iii) recovery and restoration of data following a major disaster and (b) what measures did he put in place to ensure compliance with these guidelines?

NW1952E

REPLY:

(a) The Integrated Financial Management System (IFMS) will be implemented in a phased manner to replace the current legacy systems. The phased implementation strategy includes a number of frameworks and processes to ensure the validation of data before migrating to the new IFMS system.

(i) The National Treasury continuously engages with departments and provinces through structures such as the Chief Financial Officers' Forum and the Budget Council to encourage departments to carry out data cleaning exercises. The DPSA has also initiated a project called "HR Connect" which is focused on data cleaning of departmental organizational structures and HR information. Further, the IFMS Project has developed a change management framework that will allow departments to prepare themselves, with the support of the project team, for the migration to the new systems. The IFMS Project team has also developed a readiness assessment framework that will assist in prioritizing departments and the level of effort required to support them prior to migrating them to the new systems. It should be pointed out however that notwithstanding the ongoing support which is provided to departments, the validation and maintenance of the integrity of their data will continue to remain the responsibility of each and every Accounting Officer.

(ii) The new systems are designed with sufficient security features and controls that allow for segregation of duties and profiling of users. Added security features will include flagging of users with multiple roles, an ability to use biometric technology and other electronic security systems as may be determined by departments. Within the context of the change management process, departments are made aware of these security features prior to implementation of the new IFMS modules.

(iii) The IFMS will be hosted centrally by SITA in its capacity as the Primary Systems Integrator. Disaster Recovery will therefore be managed from a central point, where proper provision will be made for procedures to recover data, when necessary. The risk of departments losing their data following a major disaster will therefore be fully mitigated and managed. Departments will nevertheless continue to be responsible for the maintenance of their Business Continuity programmes should they be confronted with a major disaster.

(b) We are confident that the change management and support processes that we have adopted will be sufficient to ensure the successful implementation of the IFMS modules. We therefore at this stage do not deem it necessary to promulgate any additional guidelines over and above the current implementation strategy and change management process that we have adopted.