AUDITOR-GENERAL

Report of the Auditor-General

to Parliament on information systems audits conducted regarding the Electronic National Traffic Information System

May 2008

Published by authority

RP 94/2008

ISBN 978-0-621-37845-0

Report of the Auditor-General

to Parliament on information systems audits conducted regarding the Electronic National Traffic Information System

May 2008

TABLE OF CONTENTS

REPORT OF THE AUDITOR-GENERAL TO THE NATIONAL PARLIAMENT ON INFORMATION SYSTEMS AUDITS CONDUCTED REGARDING THE ELECTRONIC NATIONAL TRAFFIC INFORMATION SYSTEM

1. EXECUTIVE SUMMARY

1.1 The Department of Transport (DoT) developed the Electronic National Transport Information System (eNaTIS) to centralise the management of licensing records. The eNaTIS replaced the National Transport Information System (NATIS) with effect from 12 April 2007.

The eNaTIS information systems (IS) audits conducted in 2006 and 2007 in the pre-production development environment of eNaTIS identified a significant number of weaknesses. Many of these weaknesses were, however, addressed by the DoT management prior to the implementation of eNaTIS in the production environment. Of the 103 original audit findings and those found to be unresolved in the post-implementation review, only 12 significant findings remained after subsequent follow-up audits, as reported in paragraph 6 of this report. These findings have either been partially resolved or still need to be addressed. In addition, four new findings were identified, which are documented in paragraphs 6.2.1, 6.2.2 and 6.3.2.

In their comments on these audit findings, management referred to various corrective measures taken or planned to address the findings. These measures will be reviewed during a future follow-up audit.

1.2 The following findings are historical and can no longer be rectified but have been noted to ensure that future system development projects are planned and implemented more effectively. These include:

- Scope changes resulted in significant overruns in terms of both the implementation date and the total cost of the project (see paragraph 6.1.1).
- The Web-based architecture that was planned to support eNaTIS was replaced by a client-server architecture, which also negatively impacted the planned milestones and cost (paragraph 6.4.1).
- A security officer was not appointed timely to ensure that adequate IT security would be built into the system (paragraph 6.1.2).

- The project manager had to perform multiple functions, resulting in inadequate segregation of duties (paragraph 6.1.3).
- The planned full-system stress testing was not performed prior to implementation to ensure that eNaTIS could cope with the volume of transactions in production (paragraph 6.1.4).

1.3 The following significant findings are in the process of being addressed:

- The project costs significantly exceeded the original tender amount and documentary evidence could not be provided to verify the costs incurred to date. The total costs of eNaTIS will be subject to the 2007-2008 regularity audit (paragraph 6.1.1).
- The disaster recovery site is operational and backups are being taken but the disaster recovery plan (DRP) for this site has not yet been tested (paragraph 6.3.4).
- Many users have multiple user identifications (UIDs), which could result in a lack of segregation of duties (paragraph 6.3.3).
- The physical access controls in place at the building that houses the eNaTIS data centre (DC) were not adequately designed (paragraph 6.3.1).
- Inadequate hardware and insufficient server capacity have resulted in slow system performance (6.4.2).
- While users generally believe that eNaTIS is user friendly and that training and manuals are adequate, a number of system and user/manual processes and procedural enhancements are still required and support at provincial call centres could be improved (paragraphs 6.4.3 and 6.4.4).

1.4 Some findings relating to system and database security still need to be addressed (paragraph 6.3.2) while others have been partially addressed.

1.5 In summary, most of the findings reported in both the pre-implementation and post-implementation reviews have been addressed. The eNaTIS system is now generally functioning effectively and system response has improved significantly. Slow response times can now be attributed to network congestion, in response to which the DoT has budgeted for a hardware upgrade to improve the situation. In general, the controls evaluated are adequate but priority should

be given to project cost management, disaster recovery testing, capacity planning and database security as mentioned above.

2. BACKGROUND

The DoT developed the eNaTIS over a period of five years (1 June 2002 to 11 April 2007), at a cost of R594 million to centralise the management of the vehicle and driver's licensing records of the Republic of South Africa. The eNaTIS replaced the NaTIS from 12 April 2007. One of the most significant features of the new system was that the 15 databases of the previous system were migrated into one national database.

3. PURPOSE AND CONTENT OF THE REPORT

3.1 The purpose of this report is to bring to the attention of Parliament the findings of the IS audits conducted on eNaTIS. The report is based mainly on the requirements of section 4 (1) (a) of the Public Audit Act, 2004 (Act No. 25 of 2004) (PAA).

3.2 It is anticipated that this report will give rise to corrective steps that would contribute constructively to the establishment and implementation of appropriate management measures and controls and, consequently, to improved value for money, especially in respect of future system developments and in the course of sharing departmental practices.

4. RESPONSIBILITIES, STANDARDS AND DUE PROCESS

4.1 RESPONSIBILITIES

4.1.1 The auditing of government institutions is based on the premise that it is the responsibility of the accounting officer to institute measures to ensure that resources are procured economically and utilised efficiently and effectively. The responsibility for instituting these measures rests with management.

4.1.2 The primary objectives of the IS audits were to confirm independently that these measures do exist and are effective and to provide management, the

Executive and Parliament with information on shortcomings in the management measures and the effects thereof by means of a structured reporting process.

4.2 STANDARDS

IS audits are conducted in accordance with the standards on auditing as adopted by the International Auditing and Assurance Standards Board and the Standards for Information Systems Auditing of the Information Systems Audit and Control Association. The effectiveness of the system development life cycle methodology, the data migration from NaTIS to eNaTIS and the general controls surrounding eNaTIS at the DoT was measured against the internationally accepted control objectives for information and related technology framework as well as industry best practices.

4.3 DUE PROCESS

4.3.1 As the audits progressed, the findings were informally discussed with staff members to clear any uncertainties. Once the findings had been summarised in a draft report, they were submitted to the eNaTIS project manager and his team to confirm factual correctness and to afford management the opportunity to comment on the findings. Meetings were regularly held with the project team to clear findings and discuss matters and the report was also discussed with the accounting officer on 13 May 2008 to reach consensus about the factual correctness of the findings.

4.3.2 Sufficient audit work was performed to provide substantiating evidence for the findings set out herein.

5. SCOPE

5.1 IS audits in respect of the system development life cycle (SDLC), general controls and network security of eNaTIS were conducted during 2006 and 2007 in the pre-production development environment at the DoT and management reports were issued. Further IS audits were performed in the production environment of eNaTIS during 2007 and 2008. The eNaTIS project

was evaluated against three key objectives, namely whether the project had been completed within budget, within time, and within scope. The IS audits conducted in the production environment of eNaTIS during 2007 and 2008 focused on the following components:

5.1.1 SDLC methodology followed in the development of the eNaTIS

5.1.2 Data migration from NaTIS to eNaTIS

5.1.3 General and network controls surrounding the eNaTIS production environment

5.1.4 Post-implementation status of eNaTIS

5.2 The scope of the audit did not include the tender process or the process leading up to the development in the test environment. Also, the audit did not include an application-level (system functionality) process review.

6. DETAILED AUDIT FINDINGS AND RECOMMENDATIONS

6.1 SYSTEM DEVELOPMENT LIFE CYCLE

6.1.1 Audit finding: Scope changes resulted in significant overruns in terms of both the implementation date and the cost of the eNaTIS development project

The initial contract (RT1194KA) allowed for a development period of three years from 1 February 2002 to 7 December 2004 whereas the actual development extended over a period of five years (1 June 2002 to 11 April 2007). The following factors were the main causes of the delay in the completion of the project:

- An application made by another tenderer to the high court for the awarding of the contract to be overturned caused a delay for four months. The application was unsuccessful but caused the starting date to be postponed from 1 February 2002 to 1 June 2002. The eNaTIS implementation was consequently rescheduled to April 2005.

- A further delay of two years was due to milestone dates being revised to accommodate additional functionalities to be incorporated into the software development baseline, changes in the migration plan, additional hardware requirements and additional sites.

The DoT also indicated that the eNaTIS operated in a dynamic environment that constantly changed. Changes in legislation, an increase in vehicle and driver populations and additional functionality required, necessitated several formalised scope amendments, which impacted on the cost and implementation date of the eNaTIS project. The scope changes were also required due to the fact that the eNaTIS was continuously expanding.

The original tender price was R354,7 million. The revised fixed contract price after contractual adjustments for the consumer price index (CPI) and foreign exchange variations was R410,8 million.

The project costs incurred significantly exceeded the original tender amount of R410,8 million by an amount that could not be accurately determined. The DoT indicated that the overruns related to, among others, the following:

- R44,9 million for additional sites, hardware implemented by provinces
- R69,8 million for continued maintenance and enhancement of the system, i.e. standard maintenance of the system; enhancements and upgrades requested by provinces were financed from the eNaTIS transaction fees as approved by the National Treasury
- Additional DoT expenditure outside fixed price of R39,5 million
- Maintenance (RT1194KA) costs amounting to R17,7 million

The project expenditure could not be verified due to a lack of accurate information.

In addition, overruns included R98,3 million for additional software requirements of which R54,1 million related to changes required to align eNaTIS to NaTIS release 85.3, as well as additional functionality changes. However, no

evidence was available to confirm that this request was considered and approved by the eNaTIS national steering committee.

The total cost mentioned above excludes the DoT's departmental resource costs, such as the salaries of staff seconded to the project and hardware maintenance costs that are the responsibility of the DoT.

The DoT indicated that additional unplanned project costs were incurred due to the ongoing development work that had to be done on the old NaTIS system as a result of changes in legislation, enhancements of system functionality required and error corrections. The developer was consequently required to continually realign eNaTIS to NaTIS, resulting in additional expenses.

Financial records should reflect all components of project-related expenditure. The DoT should establish whether the additional software details were presented to the eNaTIS national steering committee for approval and appropriate action should be taken accordingly. Documentary evidence of all approvals should also be kept for future reference and audit purposes.

6.1.2 Audit finding: Security officer not appointed timely to ensure adequate security design

An eNaTIS information security officer was not appointed timely to take responsibility for all eNaTIS security issues from the inception of the project. As the eNaTIS information security officer was only appointed during the last quarter of 2006, a security officer was not involved for a considerable period of the development process (since 1 June 2002).

The DoT therefore relied heavily on the developer for inputs on all aspects of the development to ensure compliance with best practice regulatory and statutory IT security requirements, as specified in ISO 17799, the Minimum Information Security Standards (MISS) and the Public Finance Management Act, Act No. 1 of 1999, which should be incorporated into any IT system of this magnitude.

Neither independent external auditors nor internal auditors were involved in the development of the system to proactively evaluate the controls to be built into the system.

An eNaTIS security committee was only established at the beginning of 2007 to assess the security risks at its meetings that took place on a quarterly basis. This means that for most of the time the system was being developed the committee had not even been established to provide the required security inputs.

The eNaTIS security committee makes recommendations to the eNaTIS national steering committee and the eNaTIS User Group (eNUG). However, a detailed review (audit) by the DoT of the risks and controls in respect of access to the system and the functionality and programmed controls of the system was not performed. The weaknesses referred to in paragraph 6.3 could be attributed to this omission.

An application-level (system functionality) process review regarding access to, and the functionality of the eNaTIS system should be performed as soon as possible.

6.1.3 Audit finding: Inadequate resources inhibited proper segregation of the multitude of functions

As a result of a lack of adequate DoT resources during the project development, the project manager had to perform a multitude of additional functions (e.g. financial manager, software development regulator and mediator between the DoT and the developer). Additional resources should have been allocated by the DoT to assist in managing the eNaTIS system and to provide financial management and administrative support skills.

6.1.4 Audit finding: Planned full-system stress testing was not conducted prior to the implementation of eNaTIS in production due to a lack of user commitment

Normally, tests are performed in a development or test environment before a system is taken into the live (production) environment. No full-system stress testing was, however, performed prior to the implementation of eNaTIS in the production environment. Performance, database and transaction volume stress tests were conducted with users in the eNaTIS test environment. Two pilot runs involving the network and users were undertaken in an attempt to execute a full-system test. These tests were, however, not conclusive due to various problems that were experienced, as well as a lack of adequate user participation. It was determined during the test phases that a few transactions that were not often effected placed a disproportionate load on the system. It was therefore not possible to determine what the transaction response times and processing capability would be once the eNaTIS system had been fully implemented and all the users were using the system simultaneously. Consequently, it could not be determined whether transactions might slow down or degrade the system, network, database or processing servers, or when high-volume processing periods would occur and what their impact on the system would be.

When the eNaTIS eventually went live, the system initially experienced huge performance problems, which highlighted the fact that the stress testing performed during the development of the system had been inadequate.

Although the servers had been upgraded, they were already running at full capacity. Management had, however, identified the need for further upgrading of the servers prior to the audit.

The DoT should address the insufficient system capacity as a matter of urgency (also see paragraph 6.4.2).

6.2 DATA MIGRATION

6.2.1 Audit finding: Data errors on the NaTIS were not all fixed prior to migration and had to be transferred to eNaTIS*

Not all data errors were fixed prior to the migration and conversion of data from the different decentralised databases to the centralised database. Data errors that existed on the old system required further investigation by the DoT to ensure their satisfactory resolution. Resolving these errors required lengthy processes to be executed and not all errors could be fixed prior to the transfer to the production environment. At the time of compiling this report, the DoT indicated that certain errors were in the process of being corrected in the production environment through a change control process.

6.2.2 Audit finding: Lack of data migration documentation to evaluate the data migration process*

The adequacy of the process followed when data was copied from the 15 regional databases to the data conversion tapes could not be evaluated since documentation detailing the process followed could not be made available. The DoT indicated that such documents existed and that users were required to sign off their data as correctly transferred.

The DoT should locate and store the documentation compiled and/or used during the conversion process at an off-site storage facility for possible further audits and as an audit trail.

6.3 GENERAL CONTROLS

6.3.1 Audit finding: Inadequate design of physical access controls

Nine officials identified by management as no longer requiring access to the building were still enabled on the access control system to enter the building, which created the risk that the system might become unavailable due to

* New finding identified during the follow-up audit

damage or invalid transactions being processed via the consoles housed in the facility.

The types of access that could be requested on the physical access request forms were, moreover, not aligned to the access that could be granted on the access control system (e.g. the form indicated areas A, B and C, while the system options related to access to areas B, D and E).

The DoT indicated that access to the building housing eNaTIS was reviewed on a quarterly basis to remove the access rights of users who no longer required them from the access control system.

The DoT should disable or remove the access rights of officials no longer requiring access to the building from the access control system as soon as possible. The access card authorisation form should be amended in line with the types of access that may be granted on the access control system to ensure that all future requests for access would be appropriately completed and granted. Staff to whom access has already been granted should be required to complete the new updated access card authorisation form and any changes that need to be made in respect of their access should be appropriately rectified on the access control system.

6.3.2 Audit finding: Logical access controls and database and operating system security inadequate to ensure data integrity, confidentiality and availability

A number of users had not changed their passwords for extensive periods. Furthermore, a number of profiles had weak password policy settings that would not prevent users from using inadequate and easily guessable passwords. Privileges assigned to powerful facilities were overly permissive. Although the auditing facility was enabled, it was not configured to record either successful and failed connection attempts or the actions of the system controller on the system.

The current security configuration settings of the workstations at the regional offices audited had not been documented in a formalised configuration standard. The antivirus software on the workstations reviewed was outdated.

Although security patches had been installed on the servers reviewed, a secondary server was found to lack critical security patches, which could lead to server compromises. A powerful network facility that could be used to gain unauthorised access to information was found to be running on a server used to manage thin clients that were still in the development phase.

No documented firewall security and configuration standards were in place to ensure that firewalls would be appropriately set up to limit the vulnerability of systems to being compromised. *

Control over the directory where the firewall rule change logs were stored was not appropriately restricted. Log files that are not kept in a secure location could be manipulated and would not be reliable during post-event analysis. *

The DoT should ensure that:

- powerful database administrator accounts are not allowed to use easily guessable passwords and each account should be protected by a strong password that adheres to a carefully structured password policy. A strong password policy should be applied to all profiles. Unnecessary privileges should be removed from sensitive facilities. Auditing of connections to the database and systems operations should be enabled.

- the current security configuration settings are formalised in respect of the workstations at the two regional offices audited as well as those not subjected to the audit. The antivirus software on the workstations should be updated.

- the directory where the firewall rule change logs are stored is secured to prevent unauthorised access and changes.

* New findings identified during the follow-up audit

- the minimum security requirements for the firewall are documented in a security standard. Management of the firewall should be restricted to secure protocols and compliance with this standard should regularly be reviewed. A patch management process should be developed to ensure that critical security patches are timely tested and applied, as required. Unnecessary services that provide potential entry points into the server from the network should be removed. Only those services that meet a business need should be allowed.

6.3.3 Audit finding: Multiple user and system administrator user identifications might impact proper segregation of duties at user level

A large number (3 727) of multiple UIDs were identified, which could increase the risk of duties not being adequately segregated. However, some of these UIDs (489) had enquiry access only. Many of these UIDs were used to access different offices in the same province for business reasons. For example, one person in the Western Cape had UIDs to access the Paarl, George and Hermanus systems. There were 62 active (multiple) system administrator accounts on the system that had access to systems in different areas of the same province. For example, a certain official had powerful system administrator access to the Vryheid and Ulundi systems. The DoT indicated that the allocation of multiple UIDs was a specific business requirement in the eNaTIS environment and that user controls had been implemented in an attempt to limit the risks involved in duties not being effectively segregated. However, the following potential risks were identified which should be further investigated by conducting an application control review:

- A total of 452 (14%) active users on the system had access to both the Driver's Licence Test Supervisor profile and the Driver's Licence Test Cashier profile.
- A total of 44 active users on the system had access to both the Supervisor Province profile and the Registering Authority Live Cashier profile.

- A total of 24 active users on the system had access to both the Registering Authority Supervisor Backlog profile and the Registering Authority Live Cashier profile.
- A total of 1 043 (32%) active users on the system had access to both the Registering Authority Supervisor profile and the Registering Authority Live Cashier profile.

The DoT should undertake an application control review of eNaTIS and operational audits should be conducted at the various regional sites to ascertain whether adequate controls have been built into the system and to confirm that an adequate business case exists for the multiple UIDs in use at each office. It should also be determined during these audits whether the access privileges allocated to the regional administrators are correct and in line with their job functions.

6.3.4 Audit finding: Disaster recovery site and backups not yet tested to ensure reliability

Although a disaster recovery site had been set up and had been operational since 11 January 2008, the DRP for this site had not yet been tested and it was thus unclear whether backups could be restored from this site in case of a major disaster.

The DoT indicated that full database backups of the production environment were taken on a weekly basis and that the backups were stored off site. It was also indicated that the users in the various regions would be able to connect to the disaster recovery centre (DRC) with limited impact on the continuity of their activities.

However, the documentation regarding the weekly backups copied to tape that was requested for audit purposes, such as backup schedules, logs and checklists, was not provided to the audit team. There was consequently a risk that, should backups be needed in the event of a disaster, they might not be available as they might not have been made. Furthermore, management was unable to monitor whether backups had indeed been made as adequate evidence was not available.

The DoT indicated that a backup strategy that makes provision for the regular testing of backups was developed and documented subsequent to the audit and that backups had been tested by restoring them at the DRC. The DoT also mentioned that the DRP could only be tested after the upgrading of the DC and the DRC and that orders for the required equipment had been placed on 15 April 2008. It was anticipated that the DRP would be tested within two months after the upgrade had been completed and that all aspects of the DRC would be tested, including network connectivity.

While the corrective measures taken by the DoT are noted and supported, the disaster recovery site should be tested as soon as possible. Evidence of the backups successfully run and tested (backup logs) should be kept as an audit trail.

6.4 POST-IMPLEMENTATION

6.4.1 Audit finding: Replacement of Web-based architecture by client-server architecture impacted negatively on the planned milestones and cost of the development project

The eNaTIS was originally planned as a Web-based architecture according to which all transactions performed on eNaTIS would be driven through workflow processes (after a transaction had been performed, it would automatically route to the next person responsible for the transaction). However, all workflow processes were removed to minimise the impact on the end-users during the implementation phase, since it was decided to follow the “one-off data conversion” approach, which would already have a huge impact on the users. A business decision was also taken that the user interface and menu structure of eNaTIS should resemble that of the NaTIS system to ease staff into the change management process (the eNaTIS screens would thus look similar to the previous system’s screens).

The Web-based architecture was subsequently replaced by a client-server architecture. This decision resulted in the redesign of the architecture, the development of the architecture after completion of the development of eNaTIS

releases 1 and 2, the updating of all training documentation and the replacement of the Web-based menus and screens.

These changes were accepted and approved by the national steering committee but had a significant impact on the project. The workflow processes are only scheduled to be implemented in future eNaTIS releases.

6.4.2 Audit finding: Inadequate equipment led to slow system performance and insufficient server capacity

The eNaTIS went live on 12 April 2007, but performance issues were experienced that tarnished the image of the DoT and created the perception among the public that eNaTIS was not functioning as intended. The system's slow performance was mainly caused by database server capacity overloads. As a result, all users still experienced slow response times in the period shortly after commissioning due to the original DC equipment being inadequate to cope with the demand. A further database server was subsequently installed to alleviate the overload issues and to optimise the database.

Although the database at the DC has operated without any downtime since May 2007 and with 99,89% of the transactions being performed adequately, the network response and uptimes at the various offices are not reflected in these statistics and it is at these offices where the problems with performance are experienced.

Currently, the servers in the eNaTIS production environment at the DC are running at full capacity. Although the DoT has commenced with a process of upgrading the DC the risk exists that should the DC experience a critical failure, the DRC would not be capable of sustaining user demand on the system, which would effectively result in the unavailability of the eNaTIS system.

Three application servers are used at the DC for the eNaTIS production environment. One of these servers is a loan unit obtained from a vendor for which no formal contract was in place at the time of the review. Should the vendor request that this unit be returned, a significant increase in load would be

experienced on the two remaining servers, which would result in redundancy not being available at the DC should one of the remaining servers fail.

Four database servers are used in the eNaTIS production environment and all four servers are currently operating at full memory capacity. Due to its superior processing capabilities, one of these servers is responsible for 50% of the current memory demand. This server is also on loan from a vendor. No contract has been established for this server and the cost and basis of payment negotiated with the vendor could not be determined. Should this server fail or be removed, the remaining three servers would not be capable of sustaining user demand on the system, which would effectively result in the unavailability of the eNaTIS system.

The DoT should address the capacity issues and the risks associated with the loan servers as a matter of urgency. The cost and basis of payment should be agreed upon in a formal agreement, which should require the prompt recovery or immediate replacement of servers. Network response time should be monitored and problem areas addressed to ensure appropriate response time and availability.

6.4.3 Audit finding: Functional limitations of eNaTIS

Users generally felt that eNaTIS was user friendly, that training was adequate and that the training manuals were readily available and up to date. The system provided the same functions as NaTIS and was aligned to current legislation. However, a number of limitations were identified by interviewing key project personnel, selecting and interviewing a random sample of eNaTIS end-users, reviewing project documentation and observing processes. The following are examples of the limitations identified:

- Recurring slow system response times experienced at the offices
- Adequate support not provided at all provincial call centres
- Processing at the eNaTIS DC running at critical levels, often close to maximum capacity, which could result in eNaTIS becoming unavailable
- Certain aspects of the eNaTIS functionality found unsatisfactory by some users

The DoT should investigate the validity of the weaknesses identified and, if necessary, enhancements should be prioritised and implemented to ensure that user needs are met and effective service delivery is promoted. While the auditors were apprised of certain reasons for the limited functionality experienced, the users should also be informed to limit negative perceptions.

6.4.4 Audit finding: Inadequate management controls and cumbersome processes at the regional sites

Notices informing the public that eNaTIS was not available were used when users were not available due to other commitments, such as attendance of funerals and union meetings. This created the impression among the public that eNaTIS was unreliable and unstable when this was not the case.

Some of the user/manual processes and procedures followed at certain regional offices were found to be cumbersome and resulted in unnecessary queuing of customers. The DoT commented that this matter related to a competency delegated to the provincial authorities and that it should thus be evaluated in the specific locations where problems are experienced.

The DoT should review the manual procedures and processes followed at regional offices and streamline them as far as possible to address public frustrations and misperceptions. The management of the regional offices should contribute to the promotion of the benefits provided by eNaTIS rather than to the perceptions that eNaTIS is unreliable and unstable.

7. OVERALL CONCLUSION

Most of the findings reported in both the pre-implementation and post-implementation reviews have been addressed. The eNaTIS system is now generally functioning effectively and system response has improved significantly. Where response time is slow it can be attributed to network congestion. Management has indicated that budget has been allocated to the upgrading of the hardware, which should alleviate this problem. Moreover, some of the problems being experienced are not due to the system but to inefficiencies in the manual processes being followed at regional offices. In

general, the controls evaluated are adequate but priority should be given to project cost management, disaster recovery testing, capacity planning and database security, as mentioned above.

Auditor-General

Pretoria
15 May 2008

AUDITOR-GENERAL

GLOSSARY OF TERMS AND ACRONYMS

Access control

The process that limits and controls access to the resources of a computer system

Antivirus

An application that detects, prevents and in many cases removes all known viruses from files located in a microcomputer hard drive

Call centre

A centralised office used for receiving and transmitting a large volume of requests by telephone

Client-server architecture

A group of computers connected by a communications network, where the client is the requesting machine and the server is the supplying machine.

CPI

Consumer price index

Database

A stored collection of related data needed by organisations and individuals to meet their information processing and retrieval requirements

DC

Data centre

DRC

Data recovery centre

eDate

Electronic date

eNUG

eNaTIS user group

End-user

An abstraction of the group of persons who will ultimately operate a piece of software

Firewall

A device that enforces security policies governing traffic traversing network segments

Full-system testing

A series of tests designed to ensure that the modified program interacts correctly with other system components

General controls

Controls that apply to all areas of the organisation

Hardware

The technical and physical features of the computer

Logical access

Refers to user-based, authenticated access to an application system and the data that is processed

Network security

Network security involves all activities that organisations, enterprises and institutions undertake to protect the value and ongoing usability of their assets and the integrity and continuity of operations.

Pre-production development environment

An environment in the test laboratory that is subjected to testing once before production begins and matches the production environment as closely as possible

Privilege

An identified right that a particular user has to a particular system resource

Production environment

Where an application or system that hosts actual/real data resides

SDLC

System development life cycle - the deployment phases in the development or acquisition of a software system

Security patch

Software designed to update a computer program and its supporting data or to fix problems related to the above.

Slow system response

Relates to the tempo at which transactions are completed

Software

Programs and supporting documentation that enable and facilitate the use of the computer

UID

User identification

Accountability

Integrity

Independence

Impartiality