**ANNEXURE C : INFORMATION SYSTEMS FINDINGS**

1. **User Access Control: Inadequate implementation of user access controls at operating system level**

**Audit finding**

The following deviation was noted:

We have noted in one of the communications between the departments IT team, SITA and Data-centrix that there are 16 user accounts with “root” access defined on Unix 11 operating system, the current hosting environment of PMIS.

The finding occurred as a result of the fact that:

Management did not ensure that there is always compliance to the user account management processes outlined in the IS Operating Manual

The impact of the finding

This type of access allows the users unlimited access to the operating system resources and utilities which can indirectly be used to gain access to PMIS. Due to the powerful access rights/privileges associated with “root”, it is possible that a log of activities (authorised and unauthorised) is not maintained resulting in errors and incidents of fraud going undetected for extended period of times. It will also not be possible to determine and apportion accountability as some of these accounts are not linked to specific users.

**Internal control deficiency**

Leadership:

Implementation of policies and procedures

**Recommendation**

Both the directors of IT Applications and Infrastructure with the assistance of the Security Manager should establish a process to conduct regular logical access controls reviews on the infrastructure and platforms hosting the department’s key business application systems. This process should also outline how security issues and exceptions coming out of the reviews will be dealt with to ensure that business application systems are operated within secured environments.

Furthermore a cleanup exercise of users’ and administrator accounts should be done by 30 September 2012 to ensure that only valid user and a reasonable number of administrator accounts are used and adequately managed.

**Management response**

I am in agreement with the finding and internal control deficiency.

The following user accounts must remain as they are used for the purposes below:

Spooler - used by system spooler

Spooler1 - used by system spooler

Root2  - used by system for back-ups

Permaulr  - used by system administrator

Uvadm9 - used for user administration

Uvadm10 - used for user administration

The rest of the logins in the list will be deleted.

Name: Kobedi Matsafu

Position: Director: IT Applications

Action date: 30 September 2012

Auditor’s conclusion

Management comments are noted; however, an assessment of the corrective actions agreed upon by management will be performed after three months or as per due date.

1. **User Access Control: Inadequate implementation of user access controls on PMIS**

**Audit finding**

The following deviations were noted:

Two PMIS user lists were provided in March and June respectively. Both user lists were reviewed and the following weaknesses were identified:

1. Twenty-three user accounts were created on PMIS but were never used.
2. Three-hundred and three (303) users accounts defined on PMIS did not have login names.
3. “SUPPMAIN” is one of the user profiles confirmed to be in use on PMIS was also defined as a user code and user name in one of the submitted user list.
4. User code (“1”) linked for username “Njijkik Lolo” was not consistent with the naming convention used on PMIS to uniquely differentiate user codes of different users.
5. A number of profiles (i.e. “XXX”, “W”, “Bestuur” and “Data”) were confirmed to be no longer in use, but were still linked to users.

The finding occurred as a result of the fact that:

Inadequate implementation of user access controls might result in user accounts being used to perform unauthorised activities which might compromise data integrity, confidentiality and availability.

**Internal control deficiency**

Leadership

Oversight responsibility regarding reporting and compliance

Management did not conduct regular review of user accounts created to ensure that they were still in line with the purpose they were created for.

**Recommendation**

1. Director: IT Applications in consultation with the business representative should ensure that all user accounts on the PMIS system are properly managed and linked to specific usernames.
2. Management should also develop and implement formal processes to periodically review user accounts as this will help identify inactive and invalid users on the system. These control measures should be implemented immediately.

**Management response**

I am in agreement with the finding and internal control deficiency and the following will be implemented:

1. A list will be generated by the system and will be available to the user administrators who will delete users with no login activity in the last 2 months.
2. Login names are for the Unix operating system and are not used in PMIS.
3. SUPPMAIN is the template profile used in PMIS and is a system requirement.
4. User code “1” – to be re-assigned.
5. Old profiles (XXX, VV, Bestuur etc.) will be removed.

Name: Kobedi Matsafu

Position: Director: IT Applications

Action date: 31 July 2012

Auditor’s conclusion

Management comments are noted; however, an assessment of the corrective actions agreed upon by management will be performed after three months or as per due date.

1. **Data Centre Management: Aging PMIS infrastructure that is no longer supported by the manufacturer**

**Audit finding**

The following deviations were noted:

The server hosting PMIS is old and is no longer supported by the manufacturer. This was noted in the August 2011 communication by SITA to the department. It was further confirmed during the visit at SITA by the audit team to evaluate the extent of the issues from the above referred communication.

SITA is currently having an SLA to maintain the PMIS hosting environment, however, their responsibility to deliver their service according to the agreed service levels is hindered by department as they are taking long to address the following issues:

1. Most of the system files are 90% utilised
2. The L class server running UNIX 10.6 are no longer supported by Hewlett Packard
3. The Processor Dependent Code (PDC) firmware no longer accessible as the master processor password cannot be reset
4. The current version of the operating system (UNIX 11) is outdated and renders the applied patches ineffective.

The finding occurred as a result of the fact that:

Due to the limited resources currently available as well as the old hardware and limited support from the manufacture and service providers could result in PMIS being unavailable for extended period of times as the issues listed above, if not addressed will not guarantee successful restarting and processing on the application.

**Internal control deficiency**

Leadership

Oversight responsibility regarding reporting and compliance

The role that the IS Steering committee is supposed to fulfil is lacking as their support and guidance to the IS management team is not visible

Financial and performance management

Control over IT systems to ensure the reliability of the system and the availability, accuracy and protection of information

There is lack of forward planning and decision making by the department’s management team as there seems to be no policy for optimising IT technology at the department.

**Recommendation**

The Head of Property Management unit together with the IS management team should meet and decide on the migration plan to ensure successful migration of PMIS to a new environment. It is recommended that the recommendation is implemented by 31 August 2012.

**Management response**

I am in agreement with the finding and internal control deficiency.

1. The various role players required for migration have been identified and co-opted into the migration team and implementation is set for 20/07/2012.
2. The migration to the new server is set for 20/07/2012.

Migration to the new IE-Works environment will help a greatly in addressing some of PMIS data centre issues

Name: Kobedi Matsafu / Dintheng Matlala and Acting CD: IS

Position: Director: IT Applications / Support / IT projects

Action date: 31 August 2012

Auditor’s conclusion

Management comments are noted; however, an assessment of the corrective actions agreed upon by management will be performed after three months or as per due date.

1. **Data Centre Management: Delays in migrating PMIS application to new infrastructure/platform**

**Audit finding**

The following deviations were noted:

Since October 2010, the department had for several times attempted to migrate PMIS to a new environment. The current status is that PMIS is still operating in an old environment and the delay was as a result of the following issues:

1. The new server required a printing spooler that took the department over a year to procure. The latest update is that the spooler has since been installed.
2. The current licence for DB2/Universe is not active and the department is in the process of resolving matter with the software vendor.

Impact of the finding:

1. The department is facing the risk of PMIS disk failing should there be a huge spike in number of transactions to be processed.
2. There is also a risk of not being able to successfully restore data from the application back-up media.

**Internal control deficiency**

Leadership

Oversight responsibility regarding reporting and compliance

The support and maintenance agreement with Data-centrix expired on 31 March 2011.

Financial and performance management

Control over IT systems to ensure the reliability of the system and the availability, accuracy and protection of information

There is lack of forward planning and decision making by the department’s management team as there seems to be no policy for optimising IT technology at the department.

**Recommendation**

The Head of Property Management unit together with the IS management team should meet and decide on the migration plan to ensure successful migration of PMIS to a new environment. It is recommended that the recommendation is implemented by 31 August 2012.

**Management response**

I am in agreement with the finding and internal control deficiency.

1. The various role players required for migration have been identified and co-opted into the migration team and implementation is set for 20/07/2012.
2. The migration to the new server is set for 20/07/2012.

Migration to the new IE-Works environment will help a greatly in addressing some of PMIS data centre issues

Name: Kobedi Matsafu / Dintheng Matlala and Acting CD: IS

Position: Director: IT Applications / Support / IT projects

Action date: 31 August 2012

Auditor’s conclusion

Management comments are noted; however, an assessment of the corrective actions agreed upon by management will be performed after three months or as per due date.

1. **Governance: Information Services business plan not adopted by the steering committee**

**Audit finding**

The following deviation was noted:

The Information Services (IS) business plan submitted for audit purposes had not been presented to nor adopted by the IS Steering committee.

The finding occurred as a result of the fact that:

The steering committee was only established late into the 2011-12 financial year around October 2011and by then a business plan was already developed. Furthermore, the IS steering committee together with the IS management team did not implement the provisions and directives outlined in paragraph 4 of the steering committee terms of reference which outlines the responsibilities and activities of the committee.

The impact of the finding:

This could result in misalignment of IS initiatives with the department-wide business and strategic goals.

**Internal control deficiency**

Leadership

Establish an IT governance framework that supports and enables the business, delivers value and improves performance

Recommendation

1. The 2012/2013 IS business plan must be must be presented to the IS Steering Committee for adoption.
2. It is further recommended that the IS management team should drive the committee’s self evaluation process as required by the terms of reference by 30 April 2012 to determine if the IS initiatives and activities are aligned to the department’s business and strategic goals.

**Management response**

I am in agreement with the finding and internal control deficiency:

The Business Plan for the financial year 2011/12 was only presented to the Steering Committee in the middle of the financial year. This as the IS Steering Committee had just been appointed officially. During the 2012/13 financial year the Business plan is signed by the Acting DDG Corporate Service and will be presented to the Steering Committee during the first quarter of the year

Name: Masutu Ramatlotlo

Position: Director: IT Projects

Action date: 31 May 2012

1. **Governance: Position of the Chief Director Information Services not yet filled**

**Audit finding**

The following deviation was noted:

The Chief Director: Information Services position has been vacant for almost three months. During

this period, the Director: IT Projects was temporarily appointed to act whiles the process to appoint

a suitable candidate was underway.

The current situation is further exacerbated by the expiry of the acting period which was set from 17 January 2012 to 16 February 2012 and it is not clear if the acting appointment was extended or not.

The finding occurred as a result of the fact that:

The department’s human resources recruitment processes are taking long to fill vacant positions.

The impact of the finding:

The vacant position of the chief director could result in strategic IT initiatives not being presented

and addressed at correct levels of management should the position remain vacant for extended

periods of time.

**Internal control deficiency**

Leadership

Implement effective HR management to ensure that adequate and sufficiently skilled resources are in place and that performance is monitored

Recommendation

1. The Deputy Director General: Corporate Services and the Chairperson of the IS Steering committee should expedite and prioritise the filling of the Chief Director IS position, as this is a critical position that will ensure that information technology resources are optimised in order for the department to derive value.
2. The appointment should be made by 30 June 2012.

**Management response**

I am in agreement with the finding and internal control deficiency/I am not in agreement with the finding/internal control deficiency for the following reasons [and supply the following/attached information in support of this]:

Name: Butcher Matutle

Position: Acting Deputy Director General: Corporate Services, Chief Operations Officer / Chairperson of the IS Steering Committee

Action date: 30 June 2012.

1. **Governance: Inadequate design of controls around the management of 3rd party IT service providers**

**Audit finding**

The following deviations were noted:

There are approximately 13 external companies that are providing various services to the

department. The companies are mainly appointed to execute projects or are brought in to provide

certain skills to the department.

The general approach for managing services provided is by means of project milestones,

timesheets and attendance registers. This is also a basis for processing invoices and payments

due to these companies. During the review the following are examples of weaknesses identified

from the informal processes followed at the department:

a) One of the skills contract (i.e. server infrastructure, Cisco Telephony, Networks, etc) prescribes that the terms of reference and a work plan should be maintained, but this requirement was not addressed based on the documentation that was provided for audit purposes

b) A Service Level Agreement for video conferencing facilities was still in the process of being finalised. This was a proactive measure that will become applicable once the project reaches the maintenance phase. For now a project charter is used for managing the services being provided

c) A project charter for the migration of Microsoft 2003 to 2010 was still not signed after a project has been running for almost a year

d) No contract or agreement was submitted for one of the service providers.

Consequently, it was not possible for the audit team to determine if adequate and formal

documentation of technical and organisational relationships covering the roles and responsibilities,

goals, expected deliverables, and credentials of the representatives of the service providers

exists.

The finding occurred as a result of the fact that:

The IS management team did not establish adequate processes to monitor and manage services provided by the service providers.

The impact of the finding:

This could result in unclear roles and responsibilities leading to miscommunications, poor services

and increased costs.

**Internal control deficiency**

Leadership

Establish an IT governance framework that supports and enables the business, delivers value and improves performance

Recommendation

The acting Chief Director IS together with his management teams should establish processes to monitor and evaluate the quality of service they get from the 3rd party service providers. These processes must be implemented by 30 June 2012.

**Management response**

I am in agreement with the finding and internal control deficiency:

a) The delay with the signing of the project charter was due to project scope changes that have now been agreed to.

b) The SLA for the Video Conference could not be signed at the time of this audit as this was still at project phase. Since the completion of the project the SLA is in process of be agreed to and of being signed.

c) All consultants to develop work plans on a monthly basis as a means of measuring progress

Name: Masutu Ramatlotlo

Position: Acting Chief Director: Information Services

Action date: 30 June 2012.

1. **Security Management: Database management and security controls not adequately designed**

**Audit finding**

The following deviations were noted:

As was previously reported, critical database management and security controls were still not designed for the Oracle 10g which host IE Works and Expanded Public Works Programme Web-based application systems, as a result the following key processes could not be reviewed as there were no processes defined for:

a) Monitoring the activities of database users, including those with administrator privileges, i.e. network/system managers

b) Controls aimed at managing access to sensitive data or functions within the database

c) Auditing – a list of audit logs maintained for the databases in use at the department.

The finding occurred as a result of the fact that:

The Director: IT Applications is continuously working on refining the database management and security controls, however during the time of the review management had still not implemented the commitments they have made during the previous review.

The impact of the finding:

The lack of controls at a database level do not guarantee accountability for changes to data as it would be impossible to trace back actions to a specific person.

**Internal control deficiency**

Leadership

Develop and monitor the implementation of action plans to address internal control deficiencies

Recommendation

The Director IT Applications should ensure that existing database procedure and implementation framework is revised to include the abovementioned processes. This will further enhance the security management processes once Oracle database is fully implemented and on production.

**Management response**

I am in agreement with the finding and internal control deficiency: The database procedures will be updated and implemented and the recommendations implemented during the 2012/13 financial year

Name: Kobedi Matsafu

Position: Director: IT Applications

Date:

1. **Security Management: The design of the domain controller security controls was found to be inadequate**

**Audit finding**

The following weaknesses with regard to the domain controller security controls were identified:

a) The user account management standards and procedures that can be used as a guideline for the management of the user access on the domain controller was not formally documented.

b) The department have a software solution implemented to ensure that the servers are securely installed and configured. However, the activities or processes that are followed to manage and operate the solution were not formally documented.

c) The domain controller logon violations were logged but not regularly reviewed.

d) Although it was indicated that there are only 3 users that have administrator privileges to the domain controller, several additional user accounts were found to have access to the administrator privileges. Also, these user accounts could not be linked to specific user.

The finding occurred as a result of the fact that:

Over reliance on the software solutions and the auditee does not see the importance of having the documented processes / guidelines since their informal processes / guideline are working well for them.

The impact of the finding:

If the security management controls are insecurely configured (i.e. not adequately designed and implemented), the application systems that generate the information used to prepare the financial statements are vulnerable to unauthorised access which negatively affects the integrity of the data being generated.

**Internal control deficiency**

Leadership

Establish and communicate policies and procedures to enable and support, understanding and execution of internal control objectives, processes and responsibilities

**Recommendation**

1. The Director Infrastructure and Security Manager should work together with the Director Applications to review and update the Information Service Manual to incorporate the user account management standards and procedures that can be used as a guideline for the management of the user access on the domain controller.
2. The Director Infrastructure and Security Manager should also work together with the operational staff to document the current informal processes and guidelines followed to manage the software solutions in place.

**Management response**

I am in agreement with the finding and internal control deficiency: The IT Security procedures manual will be updated and implemented and the recommendations implemented during the 2012/13 financial year. Some of the said accounts will appear with disguised names but are administrator accounts (e.g. SHOES – Domain admin)

Name: Dintheng Matlala / Phorwane Mphahlele

Position: Director IT Support / Security Manager

Date:

1. **Security Management: The design of the network system security controls was found to be inadequate**

**Audit finding**

The following deviation was noted:

The department has a software solution to ensure that the Windows system is regularly updated with the latest patches and regular activation of the anti-virus scans is taking place. However, the activities or processes that are followed to manage and operate the solutions were not formally documented.

The finding occurred as a result of the fact that:

Over reliance on the software solutions and the auditee does not see the importance of having the documented processes / guidelines as their informal processes / guideline are working well for them.

The impact of the finding:

Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents should they occur. If the security management controls are not securely configured, the application systems that generate the information used to prepare the financial statements are vulnerable to unauthorised access.

**Internal control deficiency**

Leadership

Establish and communicate policies and procedures to enable and support, understanding and execution of internal control objectives, processes and responsibilities

**Recommendation**

The Director Infrastructure and Security Manager should work together with the operational staff to document the current informal processes and guidelines followed to manage the software solutions in place.

**Management response**

I am in agreement with the finding and internal control deficiency: Although these are automated processes which are effective and efficient, to satisfy audit processes, the IT Security procedures document will be updated to include the automated procedures.

Name: Dintheng Matlala / Phorwane Mphahlele

Position: Director: IT Support / Security Manager

Date:

**TRANSVERSAL SYSTEMS USER ACCOUNT MANAGEMENT**

1. **Personnel and Salaries System (PERSAL):User account management procedures not adequately designed**

**Audit finding**

Although “PERSAL user procedures” were documented and approved, the procedure document was found to be inadequately designed as it did not address the following key user account management processes:

a) The review of user access rights on the system to ensure they are in line with their job functions,

b) The review of system controller activities with regard to user account management, and

c) The review of access and logon violations reports.

Furthermore, the above-mentioned key user account management procedures were not performed during the period under review.

The finding occurred as a result of the fact that:

The established processes by management were addressed as part of the job responsibilities of the system controller and were as a result not included as part of the PERSAL user account management procedure document.

The impact of the finding:

Incomprehensive user account management procedures might result in insufficient guidelines to follow when performing reviews on the activities of the System Controller, user access rights and access and logon violations reports. This can also compromise the integrity of data generated by PERSAL.

**Internal control deficiency**

Leadership

Establish and communicate policies and procedures to enable and support, understanding and execution of internal control objectives, processes and responsibilities

**Recommendation**

1. The Director Human Resource Administration should revise the current procedures to incorporate the abovementioned processes
2. The action should be implemented by 30 June 2012.

**Management response**

I am in agreement with the finding and internal control deficiency. The action plan to resolve the finding and action date to be provided.

Name: Ronel Mostert / Ntumisheng Mokgoatjane

Position: Director: Human Resource Administration / PERSAL System Controller

Date:

1. **Personnel and Salaries System: User account management procedures not adequately implemented**

**Audit finding**

The following weaknesses with regard to the implementation of the user account management controls were identified regarding PERSAL:

a) Although reviews were performed to identify and terminate inactive users on the system, these reviews were not adequate to ensure the timely deactivation of users who have left the department.

b) There is no process in place to validate the signatures of the Head of units who have approved requests forms for new user access and/or amendment of user profiles.

c) The following inconsistencies were identified with regard to the completion of user request forms:

1. Five out of 14 “Request for additional PERSAL functions" forms did not include the reason for the request.
2. The approval of the change request was not included on four “Request for additional PERSAL functions" forms.
3. Five out of 14 “Request for additional PERSAL functions" forms did not specify whether the change request was supported or not.

The finding occurred as a result of the fact that:

The Human Resource Administration management team had not ensured that the established controls are adhered to and are adequately mitigating the risk associated with systems access.

The impact of the finding:

Inadequate control over user account management processes might result in unauthorised activities performed on the system which might negatively compromise the integrity of the system.

**Internal control deficiency**

Financial and Performance Management

Design and implement formal controls over PERSAL to ensure the reliability of the system and the availability, accuracy and protection of information

**Recommendation**

The Director: Human Resource should ensure that the abovementioned processes are adequately implemented and monitored.

**Management response**

I am in agreement with the finding and the internal control deficiency. The action plan and action date to be provided.

Name: Ronel Mostert / Ntumisheng Mokgoatjane

Position: Director: Human Resource Administration / PERSAL System Controller

Date:

1. **Logistical Information System (LOGIS):User account management procedures not adequately designed**

**Audit finding**

The following deviations were noted:

The “Revised Directive user account management” procedure document for LOGIS was reviewed and the following weaknesses were identified with regard to the adequacy and accuracy of the procedure document:

a) The “Registration of user IDs” Procedure outlined under paragraph 2 makes reference to the "LOGIS Service Request" form whereas reference should be made to the "Request to create/maintain security profile on LOGIS" form.

b) The procedure document did not address the requirement that the "Request to create/maintain security profile on LOGIS" forms should be accompanied by the specimen signature forms when a user requests access to the system or requests user profile amendments. Furthermore, the procedure document did not stipulate that only authorised Line Managers who have submitted their specimen signature forms to the LOGIS system controller should approve the request forms.

c) The “Confirmation of existing LOGIS user IDs” procedure outlined under paragraph 16 in the procedure document was not aligned to the current process of confirming the existence of LOGIS user IDs.

d) The “Cancellation of LOGIS user IDs” procedure outlined under paragraph 14 in the procedure document was not aligned with the current process of terminating users on the LOGIS System.

e) The “changing of roles” procedure outlined under paragraph 14 was not clearly defined in the procedure document.

The finding occurred as a result of the fact that:

Management had not been aware of the key processes that should be included in the “Revised Directive user account management” procedure document.

The impact of the finding:

Incomprehensive user account management procedures might result in users not having adequate rules and guidelines to follow when requesting new user access, changes to users’ access, password resets and termination of user access, as a result, the integrity of the system might be compromised.

**Internal control deficiency**

Financial and Performance Management

Design and implement formal controls over LOGIS to ensure the reliability of the system and the availability, accuracy and protection of information

**Recommendation**

1. The Deputy Director: Provisioning should revise the current user account management directive to incorporate the abovementioned processes
2. The action should be implemented by 30 June 2012.

**Management response**

Agree with the finding, the Department will ensure that the LOGIS User Account Management Directive is reviewed and amended in line with what is physically happening on a day to day basis as recommended by Audit General

Name:Mr Lesole Matsotso / Annetjie Erlank

Position: Deputy Director: Provisioning / LOGIS System Controller

Action date: 30 June 2012

Auditor’s conclusion

Management comments are noted; however, the corrective actions agreed upon by management will be assessed after three months, or as per due date.

1. **Logistical Information System (LOGIS): User account management procedures not adequately implemented**

**Audit finding**

The following weaknesses were identified with regard to the management of user accounts on LOGIS:

a) Although management monitors the activities of the system controller by reviewing completed user request forms before the system controller creates new users and/or amends user profiles on the system, this review was found to be inadequate as it did not provide reasonable assurance that valid user creations and user profile changes were processed on the application system as per the request forms..

b) It was established during the review that "Request to create/maintain security profile on LOGIS" form is used to request new user access and user profile amendments. The following weaknesses were identified with regard to the completion of the forms:

1. The “create security profile on LOGIS” option was not selected on thirteen of the fifteen “Request to create/maintain security profile on LOGIS" forms; as a result, it was not clear whether the request forms were for new user access or user profile amendments. Furthermore, the “maintain security profile on LOGIS” option was not selected on seven of the seven "Request to create/maintain security profile on LOGIS" forms for user profile amendments.
2. The User ID (VBM) number was not indicated on one of seven "Request to create/maintain security profile on LOGIS" form (for user profile changes), and two “Reset” forms.
3. The “nature of the resetting” section was not completed on one of fifteen “Reset” form for user ID (VBM) number: 554.

c) There were nineteen inactive users on the system who had last logged onto the application in 2009 and 2010.

d) Twenty users had not logged onto the system since they were created.

e) It was further established that access and logon violation reports were not requested and reviewed by the System Controller.

The finding occurred as a result of the fact that:

The position of the Assistant Director had been vacant for 15 months; this resulted in an administrative burden.

The impact of the finding:

Inadequate control over user account management processes might result in unauthorised activities performed on the system which might negatively compromise the integrity of the system.

**Internal control deficiency**

Leadership

Implement effective HR management to ensure that adequate and sufficiently skilled resources are in place and that performance is monitored

**Recommendation**

The Deputy Director: Provisioning should ensure that the abovementioned user account management processes are adequately implemented.

**Management response**

Agree with the finding, the Department has subsequently appointed an Assistant Director as a System Controller of which the position was vacant for 15 months which resulted in an administrative burden. The newly appointed Assistant Director will now start overseeing all the relevant LOGIS Management reports as well as the activities of the Sub System Controller both administratively and systematically on an on regular basis as recommended by Audit General.

Name:Mr Lesole Matsotso / Annetjie Erlank

Position: Deputy Director: Provisioning / LOGIS System Controller

Action date: 30 June 2012

Auditor’s conclusion

Management comments are noted; however, the corrective actions agreed upon by management will be assessed after three months, or as per due date.

**INFORMATION TECHNOLOGY/BUSINESS APPLICATION SYSTEMS**

1. **Information technology/business application systems: The design of the Works Control and Property Management Information Systems user access management was found to be inadequate**

**Audit finding**

The following deviations were noted:

The Works Control System (WCS) and Property Management Information System (PMIS) user access management process is managed centrally at DPW national offices. All the new user requests are logged at SITA via Action Request System (ARS) and assigned to the DPW System Administrators for action.

The Information Service (IS) Procedure Manual document is utilised by the department for the management of user access on WCS and PMIS.

This procedure manual document was evaluated and the following weaknesses were again identified and reported last year:

a) Although, user termination forms were included as part of the procedure manual document, the use of such forms was not explained.

b) There is built-in control (i.e. a capturer cannot be an approver/authoriser) to ensure that users’ access rights on the systems are in line with their job functions. However, the procedure manual does not explain the process of how the control is handled.

c) The review of the audit trails are performed weekly to ensure that users and System Administrator’s functions on the system are in line with their job functions. However, the procedure manual does not explain how this control is handled.

d) The logon and access violations reviews are included with the review of audit trails on a weekly basis. However, it was found that the audit trails does not include the logon and access violations. Additionally, the procedure manual does not explain how this control is handled.

The finding occurred as a result of the fact that:

Although business users and the IS team was complying with the established user access management processes, the IS team commitment to review and update the procedure manual was however not implemented.

The impact of the finding:

Lack of consistent and clearly documented user account management standards and procedures could lead to unauthorised access to the financial data which could negatively impact the presentation of financial information.

**Internal control deficiency**

Leadership

Establish and communicate policies and procedures to enable and support, understanding and execution of internal control objectives, processes and responsibilities

**Recommendation**

1. The Director Applications with support from System Administrators should review and update the Information Service Manual to address the above weaknesses.
2. Once updated, the manual should be implemented and communicated to all affected stakeholders.

**Management response**

I am in agreement with the finding and internal control deficiency: The procedures of user account management are being followed properly however; the procedure manual will be updated to feature details as per recommendation.

Name: Kobedi Matsafu / Mmaphefo Motlou / Lettie Mohlamonyane]

Position: Director Applications / System Administrators

Date:

1. **Information technology/business application systems: The design of the IE-Works user access management was found to be inadequate**

**Audit finding**

The following deviations were noted:

The IE-Works user access management process is managed centrally at DPW national offices. All the requests are directed to the System Administrator. The System Administrator receiving the requests is responsible for addressing them.

The IS Procedure Manual document is utilised by the department for the management of user access on IE-Works. This procedure manual document was evaluated and the following weaknesses were again identified as reported last year:

a) The IE-Works new user registration form is included in the procedure manual. However, the process of registering new users was not documented in the procedure manual.

b) The IE-Works new user registration form makes provision for changes to user profiles and user account passwords. However, these processes were not documented in the procedure manual.

c) Although, user termination forms were included as part of the procedure manual document, the use of such forms was not explained.

d) There is built-in control to ensure that users’ access rights on the system are in line with their job functions. However, the procedure manual does not explain how the control is handled.

e) The review of audit trails is performed weekly to ensure that users and System Administrator’s functions are in line with their job functions. However, the procedure manual does not indicate how the auditee reviews this control.

f) The logon and access violations reviews are included with the review of audit trails on a weekly basis. However, it was found that the audit trails does not include the logon and access violations. Additionally, the IS procedure manual does not explain the process of handling logon and access violation reviews.

The finding occurred as a result of the fact that:

Although the IS team was practicing the processes of user access management. The team did not implement their commitment to review and update the procedure manual.

The impact of the finding:

Lack of consistent and clearly documented user account management standards and procedures could lead to unauthorised access to the financial data which could negatively impact the presentation of financial information.

**Internal control deficiency**

Leadership

Establish and communicate policies and procedures to enable and support, understanding and execution of internal control objectives, processes and responsibilities

**Recommendation**

1. The Director Applications with support from System Administrator should review and update the Information Service Manual to address the above weaknesses.
2. Once updated, the manual should be implemented and communicated to all affected stakeholders.

**Management response**

I am in agreement with the finding and internal control deficiency: The procedures of user account management are being followed properly however; the procedure manual will be updated to feature details as per recommendation.

Name: Kobedi Matsafu / Mmaphefo Motlou / Lettie Mohlamonyane]

Position: Director Applications / System Administrators

Date:

**INFORMATION TECHNOLOGY SERVICE CONTINUITY**

1. **Information technology service continuity: The Disaster Recovery Plan had not been implemented**

**Audit finding**

The following deviations were noted:

Although the department had established and approved a Disaster Recovery Plan (DRP), the plan was not implemented, since key personnel responsible for various disaster recovery processes were not yet trained and the plan was not tested for the period under review.

These matters were reported in the prior year and since then; management was only able to address the off-site storage issue.

The finding occurred as a result of the fact that:

The DRP is currently in the process of being updated to be aligned with the current IT infrastructure of the department. Due to the lack of capacity implement the DRP, management has decided to outsource the revision and updating of the DRP to consultants. This process is currently underway.

The impact of the finding:

Inadequate implementation of a DRP could lead to the department being unable to recover or successfully restore lost data from the backup media.

**Internal control deficiency**

Financial and Performance Management

Design and implement formal controls over IT systems to ensure the reliability of the systems and the availability, accuracy and protection of information

**Recommendation**

1. The Acting Chief Director and the Director: IT Support should ensure that the process to revise and update the DRP in line with the department’s infrastructure is expedited and implemented.
2. The identified key personnel responsible to activate this plan during a disaster situation should be trained and the plan must be tested at least annually. It would be ideal if the recommendation is implemented by 31 August 2012. Furthermore, currently being done should be closely monitored to ensure that the completion date of the DRP does not deviate from the date outlined in the action plan.

**Management response**

I am in agreement with the finding and internal control deficiency/I am not in agreement with the finding/internal control deficiency for the following reasons [and supply the following/attached information in support of this]: The DRP document has been updated, however relevant stakeholders have not been trained and the necessary equipment has not been procured due to financial constraints during the 2011/112 financial year. Management is in the process of procuring the relevant hardware which should be in place by the end of the 2012/13 financial year.

Name: Dintheng Matlala

Position: Acting Director: IT Support

Date:

1. **Information technology service continuity: The design of the backup strategy process was found to be inadequate**

**Audit finding**

The following deviations were noted:

It was established during the review that the Sithabile backup solution was still in the project phase, however, the solution had been implemented as it was utilised to backup IE-Works, File and Exchange servers.

The following shortcomings were identified with regard to the Sithabile backup process:

a) Quantum DXi3500 backup tool has been installed at fourteen DPW remote offices. Each site makes a backup of its data directly to the DXi3500 backup tool and replicates its data to the DX7500 backup tool located at SITA (to maintain a central backup copy for recovery). However, it was established during the review that the regional offices cannot replicate their data to the Quantum.

b) Data on the Quantum DXi7500 was not backed up to the tapes as not all the regions were able to replicate their data to the Quantum DXi7500.

The finding occurred as a result of the finding:

The drivers of the DXi3500 Virtual Tape Libraries located at the regions were not functioning properly. This resulted in the regions not being able to replicate their data to the DXi7500 Virtual Tape Library.

The impact of the finding:

Inadequate implementation of a backup strategy process could lead to the department not being able to recover or successfully restore lost data from the backup media following a disastrous event.

**Internal control deficiency**

Financial and Performance Management

Design and implement formal controls over IT systems to ensure the reliability of the systems and the availability, accuracy and protection of information

**Recommendation**

1. As was previously recommended, the Acting Chief Director IS with the assistance on the Director IT Support should ensure that the DRP once implemented takes into account the backup technology deployed. This will guarantee some recovery from the backed up media should a disaster or disruption occur.
2. Furthermore the IS management team are advised to examine the extent of the replication problem and address it with the service provider.
3. The recommendation should be implemented by 31 August 2012.

**Management response**

I am not in agreement with the finding/internal control deficiency for the following reasons [and supply the following/attached information in support of this]: The DXI devices are functioning properly, however, due to bandwidth limitations, the regional DXI are unable to synchronise data to Head Office. Management is in the process of establishing a managed service for the DXI where in dedicated data lines will be utilized to synchronise data from the regional DXI to head office and subsequently to the Offsite storage

Name: Dintheng Matlala

Position: Acting Director: IT Support

Date:

1. **IT Service Continuity: Inadequate backup solution for PMIS**

**Audit finding**

The following deviation was noted:

The PMIS transactional information has increased over the years and the backup solution that was initially used is no longer adequate to ensure that complete backups are made.

The following are the issues that are rendering the backup solution inadequate:

a) Backups are not verified due to the volumes of data being backed up and the media used which is no longer practical to use, i.e. there is approximately 130GB of data to be backed up using 24GB DDS tapes which translate to approximately 6 tapes being used for one set of backup.

b) Data backup restores are not performed due to the system resources required to do this.

c) The latest backup software solutions cannot be used as it will not function in sync with the old PMIS infrastructure which renders the current manual backup processes inefficient.

Impact of the finding:

Without an adequate backup solution for PMIS, the resumption of operations in the event of a disruption might be prolonged due to critical data not being recovered from the backup media.

**Internal control deficiency**

Leadership:

Oversight responsibility regarding reporting and compliance

The role of the IS steering committee to help the IS management team to implement solutions that the department will derive value from was lacking as the department continued to pay for services in terms of the existing SLA with SITA even though they were not guaranteed availability of PMIS should anything happen.

Financial and performance management:

Control over IT systems to ensure the reliability of the system and the availability, accuracy and protection of information

There is lack of forward planning and decision making by the department’s management team as there seems to be no policy for optimising IT technology at the department.

**Recommendation**

1. The Head of Property Management unit together with the IS management team should meet and decide on the migration plan to ensure successful migration of PMIS to a new environment.
2. It is recommended that the recommendation is implemented by 31 August 2012.

**Management response**

I am in agreement with the finding and internal control deficiency.

The PMIS environment is extremely old and we hope that we migrate sooner to the IE-Works environment to solve most problems posed by the old PMIS environment.

The Date for migration to the new server is set for 20 July 2012 and the back- up issues will be resolved.

Name: Kobedi Matsafu

Position: Director: IT Applications

Action date: 31 August 2012