UNITY LIBERTY JUSTICE

Auditor-General
NAMIBIA
Enhancing Transparent Accountability

REPORT OF THE AUDITOR-GENERAL ON THE INFORMATION SYSTEMS OF

OFFICE OF THE VICE PRESIDENT: VETERANS AFFAIRS

FOR THE FINANCIAL YEAR ENDED 31 MARCH 2018

Published by authority

Price (Vat excluded) N$ 68.00
Report no: 46/2019

Republic of Namibia

TO THE HONOURBALE SPEAKER OF THE NATIONAL ASSEMBLY

I have the honour to submit herewith my information systems audit report on the Veteran Administration system, and the general controls regarding the IT environment of the Office of the Vice President: Veterans Affairs for the financial year-ended 2017/2018 in terms of Article 127(2) of the Namibian Constitution. The report is transmitted to the Honourable Minister of Finance in terms of Section 27(1) of the State Finance Act, 1991, (Act 31 of 1991) to be laid upon the Table of the National Assembly in terms of Section 27(4) of the Act.

WINDHOEK, APRIL 2019

JUNIAS ETUNA KANDJEKE
AUDITOR-GENERAL

TABLE OF CONTENTS

GLOSSARY OF TERMS

Application Control Audit Application controls are those controls that pertain to the scope of individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting.

Asset Owner A person or entity that receives the benefit of ownership. Being an actual owner the asset is under the person's or entity's name and they are entitled to any advantage from that.

Brute Force Attack It is a trial and error method used to obtain information, such as, user password or personal identification number

Change Management Is the process, tools and techniques to manage the people side of *change* to achieve the required business outcome. *Change management* incorporates the organizational tools that can be utilized to help individuals make successful personal transitions resulting in the adoption and realization of *change*.

Cryptography Is the process of converting ordinary plain text into meaningless text and vice versa.

Encryption Is the processes of encoding a message or information in such way that only authorised parties can access it and those who are not authorised cannot

General Control Audit Controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications.

Information Assets Is a body of knowledge that is organized and managed as a single entity. Like any other corporate *asset*, an organization's *information assets* have financial value. That value of the *asset* increases in direct relationship to the number of people who are able to make use of the *information*.

IT Governance Is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals. This is achieved by having the right structures and policies in place.

IT Operations Gartner defines **IT operations** as the people and management processes associated with IT service management to deliver the right set of services at the right quality and at competitive costs for customers.

IT Security Is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.

MS SQL Microsoft has developed a database called MS SQL This database are designed to use SQL structured query language with which it Update/ delete information to the database.

Misconfiguration Incorrect or inappropriate configuration

Oracle Database Developed by the Oracle Company. It is a database that is commonly used for running online transaction processing (OLTP), data warehousing (DW) and mixed (OLTP) and (DW) database workload.

Risk Assessment Is a systematic process of evaluating the potential risk that may be involved projected activity or undertaking

Standing Data Information held on a file in a computer for long-term use because it does not often change

Subvention Payment. Monthly grant of money especially from government.

ACRONYMS

CAATS	Computer Assisted Auditing Techniques: the practice of using computers to automate the IT audit processes. CAATs normally includes using basic office productivity software such as spreadsheet, word processors and text editing programs and more advanced software packages involving use statistical analysis and business intelligence tools.
IDI Handbook	International Development Initiative Handbook: developed by a Working Group for IT Audit (WGITA) for SAI's
SAI	Supreme Audit Institution
VAS	Veterans Administration System
VFFMS	Veterans Fund Financial Management system
SLA	Service Level Agreement
UPS	Uninterruptable power supply
CIA	Confidentiality, Integrity and Availability of information systems
IS	Information Systems
IT	Information Technology

EXECUTIVE SUMMARY

I carried out an audit on Information Systems in terms of Section 26(a)(i) of the State Finance Act, 1991 (Act 31 of 1991), which states that the Auditor-General, in his or her discretion, may determine the extent of any investigation, examination and audit. Furthermore, Section 27(3) of the State Finance Act states that the Auditor-General may at any time, if he or she deems it necessary; transmit a special report on any matter connected with the Auditor-General's duties and powers under this Act or any other law to the Minister.

An Information Systems Audit involves collecting, evaluating evidence to determine whether information systems and related resources, adequately safeguards assets, maintain data and system integrity, provides relevant and reliable information, achieve organisational goals effectively, consume resources efficiently, and have effective internal controls that provide reasonable assurance that business, operational and control objectives are met.

The objective of the audit is to determine whether the Office of the Vice President: Veterans Affairs has controls in place that effectively preserves the confidentiality, availability and integrity of information assets.

The audit focused on the following control areas:

- IT General Controls
- Application input controls;
- Database controls; and
- Data Analysis on standing data with CAATS.

The major findings and recommendations identified during the audit are as follows:

IT General Controls

IT Governance

The Office of the Vice President: Veterans Affairs has an inadequate IT Governance in place which could lead to overall objectives of the Office not being met.

It is recommended that the Accounting Officer at the Office of the Vice President: Veterans Affairs should put measures in place that will ensure an adequate IT Governance structure is in place, that enables IT to effectively achieve overall objectives.

IT operations

The Office of the Vice President: Veterans Affairs does not have formally documented policies and procedures in place to manage the different operations of the IT function. This could lead to the following control weaknesses:

- Inconsistent practices on how operations are done;
- Errors due to a lack of knowledge; and
- Inability to enforce employee accountability.

It is recommended that the Office of the Vice President: Veterans Affairs should formally document policies and procedures to manage the different operations of the IT function.

IT security

Information Security Risk Assessment

The Office of the Vice President: Veterans Affairs did not conduct an information security risk assessment for the IT environment, which includes the infrastructure, applications and databases. This could lead to the following control weaknesses:

- The Office of the Vice President: Veterans Affairs might not be aware of the threats to its information resources and vulnerabilities; and
- The current risk mitigation strategies in place may be ineffective in dealing with the actual risks the Office of the Vice President: Veterans Affairs might be facing.

It is recommended that the Office of the Vice President: Veterans Affairs should conduct an information security risk assessment for the IT environment, which includes the infrastructure, applications and databases.

Access control

The Office of the Vice President: Veterans Affairs also did not consistently apply access control procedures. This could result in inappropriate access privileges, which are unidentified and not changed accordingly.

It is recommended that the Office of the Vice President: Veterans Affairs should consistently apply access control procedures to avoid the risk of inappropriate access privileges.

Change management

The Office of the Vice President: Veterans Affairs does not have controls and procedures in place to ensure that changes to the IT environment are established, implemented and managed effectively. This could lead to the following control weaknesses:

- Unauthorised changes can be made to the system resulting into fraud or user requirements not met; and
- System disruption if changes are not tested.

It is recommended that the Office of the Vice President: Veterans Affairs should put controls and procedures in place that will ensure that changes to the IT environment are adequately managed.

Business Continuity and disaster recovery

The Office of the Vice President: Veterans Affairs does not have controls in place to ensure uninterrupted operation or minimum disruption in case of an emergency or disaster.

It is recommended that the Office of the Vice President: Veterans Affairs should put controls in place to ensure that when emergencies or disasters occur, the Office of the Vice President: Veterans Affairs' operations can continue uninterrupted or with minimum disruption.

Outsourcing of IT functions

The Office of the Vice President: Veterans Affairs does not have adequate controls to ensure that IT services are provided efficiently and effectively by service providers and that, information security risks have been considered. This could lead to the Office of the Vice President: Veterans Affairs not receiving timely and quality services.

It is recommended that the Office of the Vice President: Veterans Affairs should put controls in place that will ensure that IT services are provided efficiently and effectively by service providers and considers information security risks.

Microsoft SQL (VAS) and Oracle (VFFMS) databases

Policies and Database Management Documentation

The Office of the Vice President: Veterans Affairs does not have policies and procedures that guide the management and operation of SQL and Oracle databases. This might result in the databases configured incorrectly and insecurely.

It is recommended that the Office of the Vice President: Veterans Affairs should develop policies and procedures that will guide the management and operation of the SQL and Oracle databases to ensure that the databases are configured correctly and securely.

Password Management

The audit found that password policy configurations are not adequate. The specifics of this finding have been communicated to the Office of the Vice President: Veterans Affairs There is a risk that passwords are prone to brute force attacks, which may eventually be broken, leaving user accounts compromised.

It is recommended that the Office of the Vice President: Veterans Affairs should ensure all password configurations on the databases maintain a secure environment and are within the guidelines of best practice

Management of Access Privileges

The Office of the Vice President: Veterans Affairs has not securely configured privileges on the Oracle database. Default public privileges have been granted access to tables/objects/packages they are not supposed to have access to. This might result in unauthorized access to the application and information.

It is recommended that the Office of the Vice President: Veterans Affairs should securely configure privileges on the Oracle database to avoid the risk of unauthorized access to the application and information.

Logging and Review of Database User Activities

The Office of the Vice President: Veterans Affairs does not have logs enabled for the oracle database. This could result in the non-tracking of changes/activities that were done on the database.

It is recommended that the Office of the Vice President: Veterans Affairs should enable logs for the oracle database to timely track changes that were performed on the database.

Application input controls

Information for Registration of Veterans & Dependents

The Office of the Vice President: Veterans Affairs did not ensure that the veterans application form is captured with an identity document (ID) number as a mandatory field on the VAS. This led to duplications, which might result in overpayments and possible fraudulent activities.

It is recommended that the Office of the Vice President: Veterans Affairs should create a mandatory field for the ID's of veterans on the VAS to avoid the risks of overpayments to veterans and possible fraudulent activities.

Data Analysis on standing data with CAATS

Completeness of Systems Data

The audit revealed payment batches paid for October 2016 as reflected on the bank statements, could not be found on the VAS system. Upon further investigation, it was noted that these batches were reused from September 2016 and were not actually generated by the VAS system. If payment batches can be reused, instead of being generated by the VAS system, it causes the VAS to be understated and provides an opportunity for making and concealing unauthorized transactions. The audit also found duplicated profiles where payments had been made were deleted from the VAS system. This affects the integrity of database of the system.

It is recommended that the Office of the Vice President: Veterans Affairs do not reuse previously generated batches for making payments. All payments made should be generated from the VAS system. Information that has transaction information attached to it should not be deleted from the system. Possible duplicate profiles should be investigated and disabled.

The comprehensive findings root causes, recommendations and overall conclusion are detailed in the body of the report in chapter two (2).

CHAPTER 1 - INTRODUCTION

1.1 BACKGROUND

The Office of the Vice President: Veterans Affairs of Veterans Affairs was established to oversee payments which veterans are entitled to receive due to the role they played in the liberation struggle. The Veterans Act, 2002 (Act No 9 of 2002) makes provision for payment of either a once-off lump sum, provision of a payment towards a project, monthly payments payable to veterans or their dependents or a token of appreciation. There is an established board known as the Veterans Board whose main objective is to administer the Veterans Fund. A registered veteran is, subject to the provisions of this Act, entitled to receive assistance from the Fund if he or she satisfies the Board that he or she is a person who is not employed, or if employed, receives income, which is less than the prescribed amount.

1.2 MOTIVATION

Financial audits highlighted some reconciliation problems between the Veterans Administration System (VAS) and the Veterans Fund Financial Management System (VFFMS) of the Office of the Vice President: Veterans Affairs. These audits concluded that it could be due to system problems. An Information Systems audit was therefore required to investigate the possible causes. A Compliance audit was also conducted to evaluate if veterans are administered according to the Veterans Act. The Information Systems audit assisted with obtaining audit evidence of risk materialisation where possible non-compliance issues were identified.

1.3 MANAGEMENT'S RESPONSIBILITY

Management is responsible for the establishment and maintenance of internal controls necessary to ensure Confidentiality, Integrity and Availability of information and systems. Management should also provide reasonable assurance that adopted policies and prescribed procedures are adhered to and errors and irregularities, including fraud and illegal acts are prevented.

1.4 AUDITOR'S RESPONSIBILITY

My responsibility is to conclude on the effectiveness of design and/or operation of control procedures of these information systems based on the audit. The audit was conducted in accordance with International Standards for Supreme Audit Institutions (ISSAI) and other international standards of best practice. These standards require that I comply with ethical requirements and plan and perform the audit to gain assurance that effectiveness of the IT system and related controls is maintained.

The audit involves performing procedures to obtain sufficient and appropriate audit evidence on the effectiveness of information system controls. The extent of the audit procedures are dependent on the auditor's professional judgement, including the assessment of the information system's risks. The audit evidence obtained is sufficient and appropriate to provide a basis for the audit conclusion.

1.5 AUDIT TECHNIQUES AND CRITERIA

The audit techniques applied during the Information Systems audit were as follows:

- Gain an understanding of the IT environment and mapping system description and walkthrough;
- Conduct risk assessment to identify risks, the lack of controls and adequacy thereof to recommend mitigation measures;
- Conduct Oracle and MS SQL database audits to ascertain the adequacy of the security settings and parameters;
- Verify the quality and accuracy of Master data on the Veteran Administration system (VAS) by using Computer Assisted Audit Techniques (CAATS) to compare the Veteran Administration system with the information of Home Affairs.

The audit was based on the following best practice frameworks and guidance standards:

- ISSAI 5300 – International Standards of Supreme Audit Institutions;
- ISO 27001/2 – Information Security Management & Controls;
- COBIT 5 – Framework for the Governance and Management of IT; and
- ISACA standards – Information Systems Audit & Control Association - International professional organization for information governance, control, security and audit professionals.

CHAPTER 2 – KEY AUDIT FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSE

2.1 IT GENERAL CONTROLS

According to ISSAI 5300 and ISACA standards, the objective of IT general controls (ITGC) audit is to determine whether the computer controls effectively support the confidentiality, integrity and availability of information systems. These controls include controls over the information technology (IT) environment, computer operations, access to programs and data, program development and program changes. The audit focused on the following areas:

- IT Governance
- IT Operations
- IT Security
- Change Management
- Business continuity and disaster recovery
- Outsourcing of IT Functions

2.1.1 IT GOVERNANCE

IT Governance means putting structures around how the Office of the Vice President: Veterans Affairs aligns IT strategy with their strategic plan. It is essential for efficient operations, the creation of added value and effective risk management.

Criteria:

Principle 2 in ISO 38500 states that, *"The organization's business strategy takes into account the current and future capabilities of IT satisfy the current and ongoing needs of the organisation's business strategy"*.

Principle 3 in ISO 38500 states, *"IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and long term"*.

The Office of the Vice President: Veterans Affairs does not have an adequate IT governance structure in place which could lead to overall objectives of the Office of the Vice President : Veterans Affairs not being met. The root causes are as follows:

- The Office of the Vice President: Veterans Affairs does not have an adequate IT Strategy or strategic plan in place, which serves to guide its IT functions; neither do they have an IT steering committee in place.
- No evidence was provided to ensure IT investments are optimally used, allocated and prioritised according to the Office of the Vice President: Veterans Affairs' objectives.

It is recommended that the Office of the Vice President : Veterans Affairs should:

- Develop an IT strategy or strategic plan that is derived from and aligned to the Office of the Vice President: Veterans Affairs' overall strategy and establish an IT steering committee that will direct the execution of the IT strategy.
- Ensure that there should be an IT Investment strategy.

Management Response

In response to the draft report, the Accounting Officer indicated that: "Recommendations are noted."

2.1.2 IT OPERATIONS

Managing IT Operations ensures that adequate controls for computer operations have been established, system/application processing is appropriately authorized and scheduled and deviations from scheduled processing are identified and resolved.

Documented Operating Procedures

Criteria

Section A.12.1.1 of ISO 27001 states that, "*operating procedures shall be documented and made available to all users who need them*".

There are no documented policies and procedures to guide and manage the different operations of the IT function. This could lead to the following:

- Inconsistent practices on how operations are done;
- Errors due to a lack of knowledge; and
- Inability to enforce employee accountability.

It is recommended that the Office of the Vice President: Veterans Affairs should develop and implement policies and procedures to manage operations of the IT functions.

Management Response

In response to the draft report, the Accounting Officer indicated that: "Recommendation taken into account."

Segregation of Incompatible Duties

Criteria

Section A.6.1.2 of ISO 27001 states that, *"conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets"*.

The duties of IT staff are not adequately segregated. The audit found validation and approval of transactions in the VAS can be done by the same person or in some cases it is not indicated on the transaction information extracted from the system's database. who validated and who approved.

It is recommended that the Office of the Vice President: Veterans Affairs should ensure compensating controls are put in place to mitigate the issue of segregation of duties. These controls include management supervision and close monitoring of system logs on activities of IT staff where duties are not appropriately segregated.

It is also recommended that the system be configured to register and record who has done what on the system in this case verification and approval, based on the profile of the individual logged on the system at the time. The system user should not be given the option to complete the "validate by" and "approved by" fields on the system.

Management Response

In response to the draft report the Accounting Officer indicated that: "A System Administrator at Grade 9 level with three support staff heads the IT subdivision in Veterans Affairs. Two of these are at the level of Computer Technician and one Analyst Programmer hence the difficulty in segregating duties. The IT staff complement does not have a Database Administrator, as it is a specialised skill and none of the IT staff is trained in the area. The IT staff does only IT administration on the database and application but SILNAM IT Solutions performs all complex administrative duties on the database. Recommendation considered and segregation of duties will strictly be implemented on the VAS."

Logging and Review of User Activities

Criteria

Section A.12.4.1 of ISO 27001 states that, "*Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed*".

Audit logging is not enabled for the VFFMS application database and the logs on the Operating system and VAS system are not reviewed to detect inappropriate activities. This could lead to inappropriate access and unauthorised activities not timely detected.

It is recommended that the Office of the Vice President: Veterans Affairs should ascertain that all the activities are logged and these logs are secure and regularly reviewed.

Management Response

In response to the draft report, the Accounting Officer indicated that: "Recommendation noted. Alerts will be created to notify management of malicious activities happening in the systems. VAS and VFFMS will have to be modified to create alerts when users try to perform actions they are not supposed to. Extensive research will be required in this regard and system developers will be engaged."

2.1.3 IT SECURITY

This area covers the logical and physical access to an organisation's IT resources and data centre. The objective is to restrict access to company data and programs by means of preventing unauthorized access or changes, including prevention of unintentional errors and fraud by employees and/or intruders.

Information Security Risk Assessment

Criteria:

Section 8.2 of the ISO 27001 requires that the Office of the Vice President: Veterans Affairs should perform an information security risk assessment at planned intervals or when significant changes occur or are proposed.

Information security risk assessment has not been done for the IT environment, which includes the infrastructure, applications and databases. This could lead to the Office of the Vice President: Veterans Affairs being unaware of the threats to their information resources and the vulnerabilities.

It is recommended that the Office of the Vice President: Veterans Affairs carry out risk assessments or general security assessments. It should include internal and external threats that are specific to the Office of the Vice President: Veterans Affairs, and the risk mitigation measures selected should adequately control the risks.

Management Response

In response to the draft report the Accounting Officer indicated that: "All aspects of Information security to be addressed through the planned project on security evaluation. Upon signing of non-disclosure agreement, service providers will do a Penetration test on the network, report findings and recommend possible solutions to address security threats and vulnerabilities."

User Access Provisioning

Criteria:

Section A.9.2.2 of ISO 27001 states that, *"A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services".*

Section A.9.2.5 of ISO 27001 states *"Assets owners shall review users 'access rights at regular intervals".*

The user access provisioning process is working, but it is not consistently applied. This could lead to excess privileges being granted to users. In addition, no evidence could be obtained to indicate that divisional heads review user access rights. This could lead to inappropriate access privileges remaining unidentified and unchanged.

It is recommended that the Office of the Vice President: Veterans Affairs should consistently use the formal procedures that are in place for granting user access to all systems and resources. Access requests should be documented, authorized and filed by the IT sub-division. Furthermore, access rights should be granted according to user responsibilities. Divisional heads should review access rights at regular intervals to ensure they remain accurate.

Management Response

In response to the draft report, the Accounting Officer indicated that: "The user Access requests for VFFMS are made by relevant functional units (heads) to the Deputy Director for General Services who then directs IT subdivision on the requests. However, the recommendation is noted to ensure that the formal procedures are put in place for granting user access to the systems as well as revoking access when users leave the organisation or when roles change should be put in place".

User Access De-provisioning

Criteria:

Section A 9.2.1 of ISO 27001 states that, *"A Formal User registration and deregistration process shall be implemented to enable assignment of access rights"*.

In addition, Section A9.2.6 states that, *"The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment contract or agreement, or adjusted upon change."*

No formal user deregistration procedure could be obtained during the audit that guides the Office of the Vice President: Veterans Affairs when employees are terminated or when their responsibilities change. This could lead to unauthorised access to information system resources and facilities.

It is recommended that the Office of the Vice President : Veterans Affairs should establish a user de-provisioning procedure where IT is formally notified by Human Resources or Divisional Heads when an employee has left the organisation so their access to systems is removed. This procedure should be documented, authorized and kept in files by the IT sub-division.

Management Response

In response to the draft report, the Accounting Officer indicated that: "IT deactivates all user accounts and revokes all access as per the information provided by Human resources or subdivision heads. However, a de-provisioning procedure as per the recommendation will be put in place and implemented to ensure that all employees leaving the organisation are communicated accordingly to IT sub-division by Human Resource subdivision for their access to systems to be removed."

Encryption of Sensitive Information

Criteria:

Section A.10.1 of ISO 27001 states that, *"To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and /or integrity of information".* Implementation guidance in ISO 27002 requires the use of encryption for protection of information transported by mobile or removable media devices or across communication

The Office of the Vice President: Veterans Affairs did not put controls in place to ensure that information transferred across the network is encrypted. This could lead to possible manipulation of information before it is processed for payment. Specifics of this finding have been communicated with Office of the Vice President: Veterans Affairs.

It is recommended that the Office of the Vice President : Veterans Affairs should ensure that information sent to finance for processing cannot be modified in any way once they are generated by the VAS system.

Management Response

In response to the draft report, the Accounting Officer indicated that: "Veterans Affairs to meet with Service provider to advice on an appropriate encryption type."

Physical Access and Environmental Controls

Criteria:

Section A.11.1.2 of ISO 27001 states that *"Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access".*

In addition, Implementation guidance part (c) states, *"a physical log book or electronic audit trail of all access should be securely maintained and monitored".*

Access to the data centre is restricted but there is no record kept of who goes in the server room, what times and record of work done. This could lead to no accountability among the IT personnel that have access to the data centre.

Section A.11.2.2 of ISO 27001 states that *"Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities"*.

In addition, Section A.11.2.4 states that *"Equipment shall be corrected maintained to ensure its continued availability and integrity"*

There is environmental equipment in place for fire and temperature controls. However, there is no backup power supply and no maintenance schedules in place to ensure the equipment is regularly maintained. This could compromise availability and integrity of information systems assets.

It is recommended that the Office of the Vice President: Veterans Affairs should ensure the following:

- A logbook must be kept for all access to the server room (data centre);
- Remote access to the data centre (TeamViewer) should be logged and monitored;
- There is Uninterruptible Power Supply (UPS) to ensure continued operations in case of power outages; and
- There are written down scheduled maintenance procedures for the environmental equipment and a log available for all maintenance done.

Management Response

In response to the draft report, the Accounting Officer indicated that: "The data centre remains locked and the key remains in possession of the System Administrator. Work on the access control has started but only the east and west lobbies have been fitted with card readers. The remaining compartments including the server room are to be addressed in the 2019/2020 financial year.

In the absence of the access control at the server room, the office has implemented mechanisms of handing over in absence of System Administrator to ensure accountability.

The recommendation is noted and the office will make budgetary provision to acquire uninterruptible power supplies as part of the upgrade of the data centre".

`

2.1.4 CHANGE MANAGEMENT

The objective of change management in an organization is to ensure adequate controls for program changes have been established. This ensures that new systems/applications and changes to existing systems/applications are authorized, tested, approved, properly implemented and documented.

Criteria

Process BAI06 of COBIT5 states that the Office of the Vice president: Veterans Affairs should *"Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation".*

There are no controls and procedures in place to ensure that changes to the IT environment are established, implemented and managed effectively. This could lead to unauthorised changes to application system programs causing system malfunction. The root causes are as follows:

- Change requests are not documented and authorized;
- Programmers have access to the production environment but their access is not monitored.
- Changes made to applications/systems are not adequately tested and signed off before being placed into a production environment;
- When changes are made, there are no procedures in place to ensure reverting to old versions if required. Upgrades or changes to the system may be unsuccessful, and without procedures to rollback to previous working versions, the Office of the Vice President: Veterans Affairs may be stuck with a system that does not work or may not be in a position to recover with integrity of information intact;
- There are no procedures in place that require tracking of progress of changes to the system; and

- The Office of the Vice President: Veterans Affairs does not carry out routine reviews/audits of changes made to the systems to ensure they have been approved and documentation changes made accordingly.

It is recommended that the Office of the Vice President: Veterans Affairs should develop and implement the change management process, policy and procedures, which should include the following:

- Documenting change requests and ensuring they are authorised before any changes are made to information systems assets. Also, change requests documentations should be accompanied by evidence of due diligence carried out on the impact of changes to the current environment;
- Programmers access to the production environment should be monitored;
- Testing of changes should be done in a separate testing environment and signed off before changes are effected.
- Backup and rollback procedures considered before changes are made to systems;
- Documentation on changes should be completed and retained to ensure tracking and reviews are done to ensure changes are carried out as required; and
- The Office of the Vice President: Veterans Affairs should review or audit all changes made to information systems assets.

Management Response

In response to the draft report, the Accounting Officer indicated that: "At this stage there are no documented change management procedures, the office documents every server restart and users are notified of downtime in advance."

2.1.5 BUSINESS CONTINUITY AND DISASTER RECOVERY

Business continuity would ensure that normal business operations could continue following a disaster or a complete system failure. There should be plans and procedures in place to provide for the recovery of files, address disaster recovery, and identify critical processing (data).

Criteria

Section A17.1.1 of ISO 27001 states that the Office of the Vice President shall determine its requirements for information security and continuity of information security management in adverse situations, e.g. during crisis or disaster."

In addition, Section A17.1.2 states that the Office of the Vice President : Veterans Affairs shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

There are inadequate controls in place to ensure the Office of the Vice President: Veterans Affairs can continue with uninterrupted operation or minimum disruption in case of an emergency or disaster. This could lead to the Office of the Vice President: Veterans Affairs not being able to continue with daily operations.

The root causes are as follows:

- No controls are in place to ensure that critical Ministerial functions are identified and prioritized in business continuity planning and disaster recovery;
- There is no approved disaster recovery policy and plan that would guide the overall IT disaster recovery processes in the IT environment; and
- No backup and retention strategy is in place and controls are not adequate to ensure backups are performed, verified and checked for successful completion.

It is recommended that the Office of the Vice President: Veterans Affairs should develop and implement a comprehensive business continuity plan that incorporates disaster recovery plan for the IT environment. The following key features should be part of these plans and procedures:

- Conducting a Business Impact Assessment on which the business continuity and disaster recovery planning will be based on;
- Business continuity and disaster recovery policies;

- Backup procedures that are formally documented and approved. A log should be maintained for backup activities and this should be reviewed to ensure the backup procedures execute successfully and any errors are resolved;
- Establishing the team that will be involved in the disaster recovery activities during development of the disaster recovery plans;
- Establishing emergency processing priorities for critical business systems, that are approved by management;
- Once the business continuity and disaster re7covery procedures are developed, they should be tested regularly. Backups should also be tested regularly to ensure information from them can be successfully recovered when need arises; and
- The security of information maintained at the offsite location should be similar to security maintained at the Office of the Vice President: Veterans Affairs.

Management Response

In response to the draft report, the Accounting Officer indicated that: "It is also worth mentioning that Veterans Affairs has dedicated sufficient storage space for its backup in the upgraded data centre. The IT staff will test the backup to assess the possibilities of recovery in case of a disaster."

The upgrade of the data centre is still ongoing therefor there is no complete documentation of details and configurations. Documentation will only be available after 15 February 2019 when project is expected to reach completion.

There have been delays in the process due to the fact that all elevated functions that require administrative privileges are isolated to OPM Administrators so IT are limited in terms of flexibility.

2.1.6 OUTSOURCING OF IT SERVICES

The objective is to ensure that outsourced critical business services are provided by reliable service providers and that information security risks have been considered.

Criteria

Process APO10 of the COBIT 5 requires that, the Office of the Vice President: Veterans Affairs manage IT-related services provided by all types of suppliers to meet enterprise requirements, including, management of contracts, and reviewing and monitoring of supplier performance for effectiveness.

There are no adequate controls to ensure that IT services (Functional support services, Technical support services and training services on VFFMS as well as Telephonic services) are being provided effectively by service providers and that information security risks such as, leakage of confidential information have been considered.

The root causes are as follows:

- There are no established and documented policies and procedures that are followed when outsourcing IT services to third parties;
- Inadequate management of service providers. During the audit, it was established that the Service Level Agreement (SLA) for Telecom was expired and the one for Silnam was drafted but not signed.
- There are non-disclosure agreement phrases on the SLA. However, there are no adequate controls in place to ensure security is not tampered with during outsourcing of IT services; and
- Business continuity and disaster recovery requirements for the outsourced services are not defined in the SLAs.

It is recommended for the Office of the Vice President : Veterans Affairs should make the following provisions during the outsourcing of IT services to third parties:

- Developing a comprehensive policy and procedures as part of an overall IT/Security policy that guide the outsourcing of IT services;
- All outsourced services should have valid SLAs agreed and signed by both parties. The SLAs should include details on how performance will be monitored and implications of non-performance. Management should receive and review reports on the performance of service providers; and

- Business continuity and disaster recovery requirements for outsourced services should be specified in the Disaster recovery plans and they should be agreed to with the service provider in the initial contracts and SLA.

Management Response

In response to the draft report, the Accounting Officer indicated that: "Recommendations noted and will be implemented accordingly."

2.2 AUDIT FINDINGS – MICROSOFT SQL (VAS) AND ORACLE (VFFMS) DATABASES

The Office of the Vice President: Veteran Affairs has two main systems with separate databases. The Veterans Administration System uses the MS SQL Database and the Veterans Fund Financial Management Systems uses an Oracle database. The audit focused on evaluating the adequacy of security configurations on the databases that ensure Confidentiality, Integrity and Availability of the information is not comprised.

2.2.1 MICROSOFT SQL (VAS) DATABASE

Policies and Database Management Documentation

Criteria

Section 5.1.1 of ISO 27002:2013 states that, *"a set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties"*.

The Office of the Vice President: Veterans Affairs does not have policies in place that guides the security of the database.

It is recommended that the database security guidelines be included in the overall IT security policy for the Office of the Vice President: Veterans Affairs.

Management Response

In response to the draft report, the Accounting Officer indicated that: "Recommendations noted and will be implemented accordingly."

Password Management

Criteria

Section 9.4.3 of ISO 27002:2013 states that, *"password management systems should be interactive and should ensure quality passwords"*. In addition, implementation guidance (e) requires that regular password changes should be enforced.

The audit found that password policy configurations are not adequate. The specifics of this finding have been communicated to the Office of the Vice President: Veterans Affairs. There is a risk that passwords are prone to brute force attacks, which may eventually be broken, leaving user accounts compromised.

It is recommended that the Office of the Vice President: Veterans Affairs should ensure all the password configurations on the databases maintain a secure environment and are within the guidelines of best practice.

Management Response

In response to the draft report, the Accounting Officer indicated that: "The auditor's recommended best practice configurations will be assessed to determine if they are applicable to our environment."

Logging and Review of Database User Activities

Criteria

Section 12.4.1 of ISO 27002:2013 states that, *"event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed"*.

Database audit logs are not reviewed. This could lead to inappropriate system activities not discovered timely, before they have a major impact on system and information integrity.

It is recommended that audit logs be regularly reviewed by senior personnel or management.

Management Response

In response to the draft report, the Accounting Officer indicated that: "The Office have taken note of the audit recommendations. Audit logs will be provided to senior personnel and/ management for review on a regular basis."

2.2.2 ORACLE DATABASE

Policies and Database Management Documentation

Criteria

Section 5.1.1 of ISO 27002:2013 states that, *"a set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties".*

In addition, Section 12.1.1 of ISO 27002:2013 states that, *"operating procedures should be documented and made available to all users who need them"*

The Office of the Vice President: Veterans Affairs does not have policies and system documentation that guides the security, management and operation of the database.

It is recommended that the Office of the Vice President: Veterans Affairs should:

- Develop database security procedures/guidelines and include them in the overall IT Security policy for the Office of the Vice President: Veterans Affairs.
- Ensure documented procedures are available for IT staff for daily operation and maintenance of the database. This documentation should be approved and maintained, with any changes made to the database reflected in the documentation.

Management Response

In response to the draft report, the Accounting Officer indicated that: "Recommendations noted and will be implemented accordingly."

Management of Access Privileges

Criteria:

Section 9.2.3 of ISO 27002:2013 states that, *"the allocation and use of privileged access rights should be restricted and controlled".*

The Office of the Vice President: Veterans Affairs has not securely configured privileges on the Oracle database. PUBLIC [1]privileges have been granted access to tables/objects/packages they are not supposed to have access to. This might result in unauthorized access to the application and information.

It is recommended that the Office of the Vice President: Veterans Affairs should securely configure the Oracle database by removing public, system and role privileges that have been identified and reported in the audit.

Management Response

In response to the draft report, the Accounting Officer indicated that: "Service provider will be engaged for modifications as per recommendations."

Logging and Review of User Activities

Criteria:

Section 12.4.1 of ISO 27002:2013 states that, "Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed".

[1] When a database user is created, it is granted a pre-defined role with permissions (functions, procedures and packages).

Event logs are not enabled for the Oracle database, and therefore reviews are not done. This could result in the non-tracking of changes/activities that were done on the database.

It is recommended that the Office of the Vice President : Veterans Affairs should ensure the database critical events are logged and reviewed regularly

Management Response

In response to the draft report, the Accounting Officer indicated that: "Veterans Affairs will engage the Service provider for modifications as per recommendations."

2.3 APPLICATION INPUT CONTROLS ON VAS

Auditing the input of application controls evaluates whether data is captured accurately, reliably and completely accepted by the application in a timely manner.

<u>Information for Registration of Veterans & Dependents</u>

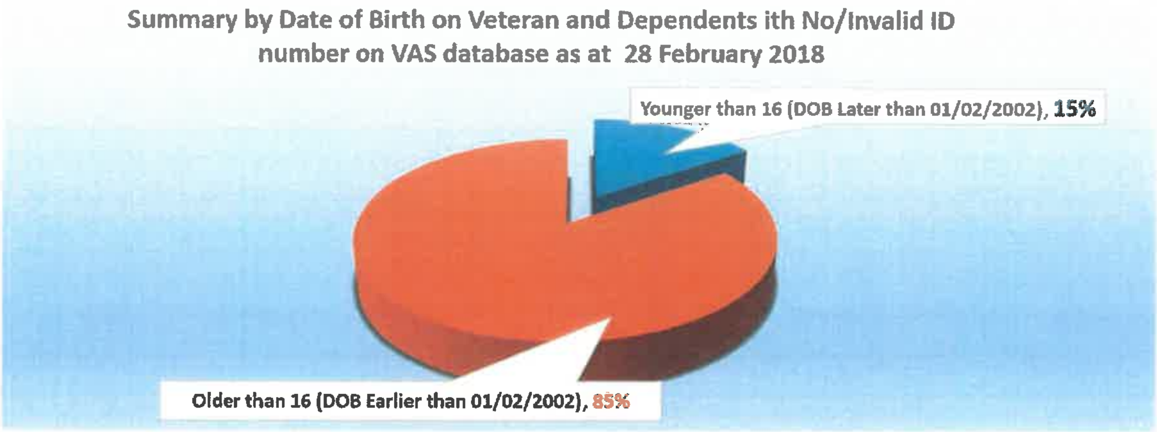
Criteria:

Subsection 1 of section 28 of the Veterans Act, 2008 (Act no 2 of 2008) states that "a person who wishes to be registered as a veteran or dependent of a living or deceased veteran must, in the prescribed form and manner, Apply to the Board for registration".

This is detailed in Form VA1 Regulation 2 that Namibian ID, Namibian Birth Certificate, Marriage Certificate and Death Certificate must be provided. This information must be captured on the Veteran Administration system.

The audit found that "ID number field" is not validated as mandatory on the VAS.

This led to 5643/69949 entries on database captured with no/invalid ID number and 273-duplicated veteran's profiles being created, which resulted in possible double payments.



The picture above indicates that only 869/5643 entries on the database has been younger than 16 years, which means that 4774 are eligible to apply for a Namibian ID, but was not captured on the VAS system. The information stated is as at 28 February 2018 from the VAS database.

It is recommended that the Office of the Vice President: Veterans Affairs should make the Identity Document field on the System a mandatory for Veterans only and dependents older than 16 years of age. This is to ensure that all Veterans captured on the system have Identity Numbers to identify themselves to prevent ghost and duplicate veterans.

Management Response

In response to the draft report, the Accounting Officer indicated that: "Veterans Affairs concurs with recommendation to make the ID number field as mandatory on VAS for 16 years and older applicants. For dependant beneficiaries under the age of 16 years old, a condition will be set on VAS as a "trigger" to automatically suspend the benefit thus allowing the beneficiary who has reached the age of 16 years old to acquire a national ID".

2.4 DATA ANALYSIS ON STANDING DATA USING CAATS

Completeness of Systems Data

Criteria:

Appendix A in Section 4 of ISSAI5300 stipulates that gap detection must be carried out to ascertain completeness in numerical data, which is expected to have sequential numbering. This would identify deleted processed transactions or information related to them on the VAS.

The audit revealed that three (3) payment batches to the value of N$ 26 402 150 that had been paid for October 2016 as reflected on the Bank Statements, could not be found on the VAS system. Upon further investigation, it was noted that the batches for September 2016 were reused and not actually generated by the VAS system. If payment batches can be reused, instead of being generated by the VAS system, it causes the VAS to be understated and provides an opportunity for making and concealing unauthorised transactions.

The audit also found that seven (7) duplicated profiles where payments had been made were deleted from the VAS system. This affects the integrity of the system database and also creates an opportunity for making and concealing unauthorised transactions.

It is recommended that the Office of the Vice President: Veterans Affairs do not reuse previously generated batches for making payments. All payments made should be generated from the VAS system.

Information that has transaction information attached to it should not be deleted from the system. Possible duplicate profiles should be investigated and disabled.

Management Response

In response to the draft report, the Accounting Officer indicated that: "The audit finding on three (3) payment batches is confirmed and the implication of reusing payment batches noted.

Veteran Affairs will strictly adhere to the recommendation by audit not to reuse the payment data and also not to manually create batch numbers for payment purposes.

On the deletion of information that has transaction attached to it, Veteran Affairs acknowledges the findings and further states that this happened from 2013 when Veteran Affairs started updating banking details on VAS. After it was detected, VAS was programmed not to accept duplicate account numbers.

CHAPTER 3 - CONCLUSION

3.1 ACKNOWLEDGEMENT

The assistance and cooperation of the management and staff of the Office of the Vice President: Veterans Affairs during the audit engagement is highly appreciated.

3.2 OVERALL AUDIT CONCLUSION

In my opinion based on the significance of the findings discussed in the chapter 2 of this report, I conclude that the Office of the Vice President: Veterans Affairs does not have sufficient controls to effectively preserve the Confidentiality, Availability and Integrity of information assets.

WINDHOEK, APRIL 2019

JUNIAS ETUNA KANDJEKE
AUDITOR-GENERAL