

SECTION 10: SUMMARY OF DETAILED AUDIT FINDINGS

Page no.	Finding	Classification					Rating			Number of times reported in previous three years	Status of implementation of previous year(s) recommendation
		Misstatements in financial statements	Misstatements in annual performance report	Non-compliance with legislation	Internal control deficiency	Service delivery	Matters affecting the auditor's report	Other important matters	Administrative matters		
	Predetermined objectives										
	Predetermined objectives: EPWP beneficiaries were not reported on the EPWP third quarter data.		X				X			3	In progress
	Predetermined objectives: Non submission of attendance register		X				X			3	In progress
	Predetermined objectives: Non submission of proof of payment		X				X			3	In progress
	Predetermined objectives: Non submission of ID copies		X				X			3	In progress
	Predetermined objectives: Non submission of disability proof		X				X			1	In progress
	Predetermined objectives: Beneficiaries listed on the EPWP reporting system list not employed on the project		X				X			3	In progress
	Predetermined objectives: EPWP projects were not reported on the EPWP reporting system		X				X			3	In progress
	Predetermined objectives: No reasons were submitted as to why active project was "stopped"		X				X			0	In progress

Page no.	Finding	Classification					Rating			Number of times reported in previous three years	Status of implementation of previous year(s) recommendation
		Misstatements in financial statements	Misstatements in annual performance report	Non-compliance with legislation	Internal control deficiency	Service delivery	Matters affecting the auditor's report	Other important matters	Administrative matters		
	Predetermined objectives: EPWP – Beneficiary's proof of change in banking details were not provided		X				X			0	In progress
	Predetermined objectives: Validity of reported performance information for Programme 5 - Indicator 3 (Percentage of movable assets provided within 60 days after approval by prestige clients)		X					X		3	In progress
	Goods and Services										
	Follow up of state funerals finding raised in 2018/19 audit	X		X			X			1	In progress
	Follow up of state events finding raised in 2018/19 audit	X		X			X			1	In progress
	Goods and Services: Contractors: Invoiced amounts exceed quoted price and Items invoiced but not included on approved quote – State Events	X						X		1	In progress
	Irregular Expenditure										
	Disclosure note not fairly presented pertaining to the Pricewaterhouse Coopers Incorporated (PWC) report on state events	X					X				In progress
	Disclosure note not fairly presented pertaining to the Public Service Commission report on SMS appointments	X					X				In progress
	Non-compliance										

Page no.	Finding	Classification					Rating			Number of times reported in previous three years	Status of implementation of previous year(s) recommendation
		Misstatements in financial statements	Misstatements in annual performance report	Non-compliance with legislation	Internal control deficiency	Service delivery	Matters affecting the auditor's report	Other important matters	Administrative matters		
	Payments not made in 30 days			X				X			In progress
	Employee benefits										
	Disclosed amount incorrectly calculated and presented	X						X		1	In progress
	Procurement and contract management										
	Publish of awards on eTender Publication and Government Tender Bulletin			X				X		0	In progress
	Quotations pre-qualifying criteria			X				X		0	In progress
	Compensation of employees										
	2019/20 HR Plan			X					X	0	In progress
	IT matters										
	INFORMATION TECHNOLOGY GOVERNANCE										
	Vacant positions within information and communication (ICT) division				X			X		4	Not addressed
	Inadequate planning and management processes around Archibus ERP system				X			X		1	Not applicable
	Information Communication Technology projects for 2019/20 were not achieved				X			X		1	Not applicable
	Corporate Governance of Information and Communications Technology Policy & Charter (CGICT) outdated				X			X		1	Not applicable

Page no.	Finding	Classification					Rating			Number of times reported in previous three years	Status of implementation of previous year(s) recommendation
		Misstatements in financial statements	Misstatements in annual performance report	Non-compliance with legislation	Internal control deficiency	Service delivery	Matters affecting the auditor's report	Other important matters	Administrative matters		
	USER ACCESS MANAGEMENT										
	Inadequately implementation of user access management controls around Windows Active Directory (AD)				X			X		3	Not addressed
	Inadequately implementation of user access management controls around EPWP				X			X		2	Not addressed
	Inadequately implementation of user access management controls around Reapatala				X			X		2	Not applicable
	Lack of adequately designed PERSAL user access management policy				X			X		1	Not applicable
	Inadequate implementation of user access management controls around PERSAL application				X			X		1	Not applicable
	Inadequate implementation of user access controls on GIS				X			X		4	Not addressed
	Inadequate implementation of user access management controls on SAGE				X			X		4	Not addressed
	Inadequate implementation of user access management controls on PMIS				X			X		1	Not applicable
	Inadequate implementation of user access management controls on WCS				X			X		1	Not applicable
	Inadequate implementation of user access management controls on Archibus				X			X		1	Not applicable
	Inadequate implementation of user access management controls on WORX4U				X			X		1	Not applicable

Page no.	Finding	Classification					Rating			Number of times reported in previous three years	Status of implementation of previous year(s) recommendation
		Misstatements in financial statements	Misstatements in annual performance report	Non-compliance with legislation	Internal control deficiency	Service delivery	Matters affecting the auditor's report	Other important matters	Administrative matters		
	SECURITY MANAGEMENT										
	Inadequate Security Management controls				X			X		4	Not addressed
	CHANGE MANAGEMENT										
	Inadequate change management process				X				X	4	Not addressed
	Inadequate implementation of change controls around Reapatala and EPWP				X				X	4	Not addressed
	INFORMATION TECHNOLOGY SERVICE CONTINUITY										
	Inadequate IT service continuity controls				X				X	4	Not addressed

DETAILED AUDIT FINDINGS: ANNEXURES A TO C¹

ANNEXURE A: MATTERS AFFECTING THE AUDITOR'S REPORT

Predetermined objectives

1. EPWP – EPWP beneficiaries were not reported on the EPWP Q4 data

Requirements

Public Finance Management Act (PFMA) section 40(3)(a) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Technical indicator description – method of calculation states that: *“A count of the aggregate work opportunities created/reported. Work opportunity is paid work created for an individual on an EPWP project for any period of time. The same person can be employed on different projects and each period of employment will be counted as work opportunity....”*

Nature

During the audit Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported in the EPWP-RS by public bodies*, the following matters were identified at EPWP projects at the various public bodies:

Participants were included on the attendance registers and / or proof of payment; but were not reported on quarter 3 (April 2019 to 30 December 2019) data submitted for audit.

No	Project No	Project Name	Public Body	Sector	Under reported W/O per project
DPWI					
1	80970-EPWP3N	Pretoria Bricklaying Apprenticeship Program	Gauteng: DPWI	Infrastructure Sector	1
2	99121-EPWP3N	SAPS: Salvokop Radio Tech Unit	Gauteng: DPWI	Infrastructure Sector	2
3	90550-EPWP3N	Pretoria High Court	Gauteng: DPWI	Environment and Culture Sector	4
4	98789-EPWP3N	Telkom Towers	Gauteng: DPWI	Infrastructure Sector	5
5	81866-EPWP3N	Momentum Building Health Care Cleaning	Gauteng: DPWI	Environment and Culture Sector	7
6	87763-EPWP3N	Nelspruit RO Gardening	Mpumalanga: DPWI	Environment and Culture Sector	6
7	80999-EPWP3N	Emahlathini and Bothashoop Ports of Entry	Mpumalanga: DPWI	Infrastructure Sector	1
8	19917-EPWP3N	Parliamentary Residential Accommodation	Western Cape: DPWI	Infrastructure Sector	11
9	85725-EPWP3N	Caledon Prison	Western Cape: DPWI	Infrastructure Sector	1
10	64927-EPWP3N	NCOP Building	Western Cape: DPWI	Infrastructure Sector	5
11	65870-EPWP3N	Humewood Military Base	Eastern Cape: DPWI	Infrastructure Sector	1

No	Project No	Project Name	Public Body	Sector	Under reported W/O per project
12	94774-EPWP3N	Queenstown SAPS (General Labour) Maziya General	Eastern Cape: DPWI	Infrastructure Sector	189
13	95941-EPWP3N	Odi Magistrate Court	North West: DPWI	Environment and Culture Sector	2
14	95592-EPWP3N	Mmabatho High Court	North West: DPWI	Infrastructure Sector	1
15	2700-EPWPRS	Bulwer Rehabilitation of old prison	KwaZulu Natal: DPWI	Infrastructure Sector	2
16	2736-EPWPRS	NPA Pietermaritzburg Workshop	KwaZulu Natal: DPWI	Infrastructure Sector	2
17	1090-EPWPRS	Umlazi Magistrate Office	KwaZulu Natal: DPWI	Infrastructure Sector	1
18	4427-EPWPRS	Melmoth SAPS	KwaZulu Natal: DPWI	Infrastructure Sector	1
19	90516-EPWP3N	Plooysburg Police Complex Repair of police station, Married Quarters and bach	Northern Cape: DPWI	Infrastructure Sector	2
20	90517-EPWP3N	Grobleshoop Magistrate's Construction of additional Accommodation	Northern Cape: DPWI	Infrastructure Sector	2
21	95315-EPWP3N	Cleaning and Gardening	Northern Cape: DPWI	Environment and Culture Sector	1
22	93306-EPWP3N	Repair and Renovation Magistrate Court in Victoria West	Northern Cape: DPWI	Infrastructure Sector	3
					250
Other Public bodies					
23	100645-EPWP3M	Taring of internal streets zone S to Q access road	Limpopo: Lepelle-Nkumpi	Infrastructure Sector	5
24	76809-EPWP3M	New indoor sports and recreation	FreeState: Matjhabeng	Infrastructure Sector	4
25	95696-EPWP3M	Nala Refuse Removal	FreeState: Bothaville/ Nala	Environment and Culture Sector	1
26	95782-EPWP3M	Nala Routine Maintenance	FreeState: Bothaville/ Nala	Infrastructure Sector	3
27	96124-EPWP3M	Nala Admin	FreeState: Bothaville/ Nala	Social Sector	1
28	63821-EPWP3M	Routine Horticultural and Gardening Maintenance	Mpumalanga: Nkangala	Environment and Culture Sector	1
29	93336-EPWP3M	ELM Transversal Admin Support Unit	Mpumalanga: Emalahleni (MP)	Social Sector	2
30	96701-EPWP3M	Road Construction and pavements	Western Cape: Bergervier	Infrastructure Sector	2
31	75348-EPWP3M	Safer Community Project	Western Cape: Overberg	Social Sector	3
32	76837-EPWP3M	Beaches Maintenance	Eastern Cape: Nelson Mandela Bay Metro	Social Sector	4
33	88269-EPWP3M	Drilling of Boreholes, Churchill Phase 1	Eastern Cape: Nelson Mandela Bay Metro	Infrastructure Sector	4
34	88284-EPWP3M	South End Museum Trust	Eastern Cape: Nelson Mandela Bay Metro	Environment and Culture Sector	1
35	94216-EPWP3M	Bathurst: Freestone Road	Eastern Cape: Ndlambe	Infrastructure Sector	12
36	83184-EPWP3M	Retained Fire Fighters	Eastern Cape: Ndlambe	Environment and Culture Sector	1
37	97647-EPWP3M	2019/20 Inhouse Project	Gauteng: City of Johannesburg Metro	Social Sector	3
38	77106-EPWP3M	Water Stewards - Ekurhuleni Water Depot	Gauteng: Ekurhuleni Metro	Infrastructure Sector	5

No	Project No	Project Name	Public Body	Sector	Under reported W/O per project
39	91949-EPWP3M	Maintenance of Roads and Storm water	Gauteng: Lesedi/ Heidelberg	Infrastructure Sector	1
40	91955-EPWP3M	Public Service	Gauteng: Lesedi/ Heidelberg	Environment and Culture Sector	1
41	77918-EPWP3M	Mbhashe Street Cleaning	Eastern Cape: Mbhashe	Environment and Culture Sector	10
42	27905-EPWP3M	EThekweni Community Social Support Programme	KwaZulu Natal: eThekweni Metro	Social Sector	2
43	70071-EPWP3M	Upgrading of the Manyavu Community Water Supply	KwaZulu Natal: Umgungundlovu	Infrastructure Sector	1
44	77069-EPWP3M	Non Revenue Water Management	KwaZulu Natal: Umgungundlovu	Infrastructure Sector	7
45	93031-EPWP3M	Operation and Maintenance in Dikgatlong	Northern Cape: Dikgatlong	Infrastructure Sector	2
46	89500-EPWP3M	Cleaning of Stormwater Intakes	Northern Cape: Sol Plaatjie	Infrastructure Sector	32
47	91185-EPWP3M	Refurbishment of Galeshewe Main Outfall Sewer	Northern Cape: Sol Plaatjie	Infrastructure Sector	3
48	57711-EPWP3M	Special Cleaning Team	Northern Cape: Sol Plaatjie	Environment and Culture Sector	61
49	89595-EPWP3M	The construction of the bulk link water infrastruc	Northern Cape: Sol Plaatjie	Infrastructure Sector	17
50	91798-EPWP3M	Maintenance of JB Marks Parks	North West: JB Marks	Environment and Culture Sector	17
51	82992-EPWP3M	Peace Officers (75682)	North West: Mahikeng	Social Sector	1
52	77436-EPWP3M	Librarian Assistants	North West: JB Marks	Social Sector	5
53	77442-EPWP3M	Community Care Giving Project	North West: JB Marks	Social Sector	2
54	95336-EPWP3M	Maintenance of Montshioa Stadium	North West: Mahikeng	Environment and Culture Sector	1
55	95341-EPWP3M	Maintanance of Civic Buidings	North West: Mahikeng	Infrastructure Sector	6
					221

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

Understatement of reported performance for Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported in the EPWP-RS by public bodies*.

Internal control deficiency

Financial and Performance Management

The department did not implement effective controls to reconcile the participants on the attendance registers to the participants reported on the EPWP reporting system.

Beneficiary lists and attendance registers are not regularly reviewed to ensure that all participants are captured on EPWP reporting system.

Recommendation

It is recommended that:

The department should perform frequent, adequate reviews of beneficiary lists and attendance registers from the public bodies to ensure that all participants are captured on EPWP reporting system.

Management should review all EPWP projects reported on the system against the attendance registers, to ensure that all work opportunities created are reported.

Management's response

I am in agreement with the finding for the following reasons [and supply the following/attached information in support of this]:

The participants were not reported by the end of Quarter 3 of 2019/20.

Name: Mr. Devan Pillay
Position: Acting DDG: EPWP
Date: 13/05/2020

Auditor's conclusion

Management comment noted.

This matter was followed up during the final audit and it was confirmed that for some of the participants from the interim audit was reported in Q4. However, the remaining participants (as indicated in the table above) were not reported and validated for Q4, and are thus not reported in the annual performance report; therefore this matter remains and will be reported in the management report.

2. EPWP - Attendance registers were not provided

Requirements

Section 40(a) and (b) of the Public Finance Management Act (PFMA) states that: *“The accounting officer for a department must keep full and proper records of the financial affairs of the department, trading entity or constitutional institution in accordance with any prescribed norms and standards; must prepare financial statements for each financial year in accordance with generally recognized accounting practice...”*

Section 40(3)(a) of the Public Finance Management Act (PFMA) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Section 41 of the Public Finance Management Act (PFMA) furthermore states that *an accounting officer of a department must submit to the relevant Treasury or the Auditor-General such information, returns, documents, explanations and motivations as may be prescribed or as the relevant Treasury or the Auditor-General may require....”*

Paragraph 15(a) to (c) of the Public Auditing Act states that: *“the Auditor-General has at all reasonable times full unrestricted access to Any document, book or written or electronic record or information of the auditee or which reflects or may elucidate the business, financial results, financial position or performance of the auditee; Any of the assets of or under the control of the auditee; or Any staff member or representative of the auditee....”*

Technical indicator description – method of calculation states that: *“A count of the aggregate work opportunities created/reported. Work opportunity is paid work created for an individual on an EPWP project for any period of time. The same person can be employed on different projects and each period of employment will be counted as work opportunity.....”*

The ministerial determination 4: Expanded Public Works Programme dated 04 May 2012 paragraph 12(1)(a) to (e) and 12.2 – Keeping records it states that: *“Every employer must keep a written record of at least the worker’s name and position; copy of an acceptable worker identification; in the case of task-rated worker, the number of tasks completed by the worker; in the case of a time-rated worker, the time worked by the worker; payments made to each worker. The employer must keep this record for a period of at least three years after completion of the EPWP.....”*

Nature

During the audit of Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups*, the following matter was identified at EPWP projects at the various public bodies:

The following participant’s attendance registers were not provided for audit purposes.

No	Project No	Project Name	Public Body	Sector	Number of beneficiaries where attendance were not submitted
	DPWI				

No	Project No	Project Name	Public Body	Sector	Number of beneficiaries where attendance were not submitted
1	98107-EPWP3N	Sibasa Embassy Home Affairs Project	Limpopo: DPWI	Infrastructure Sector	3
2	64927-EPWP3N	NCOP Building	Western Cape: DPWI	Infrastructure Sector	2
3	79047-EPWP3N	Parow Forensic Science Laboratory	Western Cape: DPWI	Infrastructure Sector	1
4	81866-EPWP3N	Momentum Building Health Care Cleaning	Gauteng: DPWI	Environment and Culture Sector	3
					9
		Other Public bodies			
5	76809-EPWP3M	New indoor sports and recreation	Freestate: Matjhabeng	Infrastructure Sector	6
6	63821-EPWP3M	Routine Horticulture and Gardening Maintenance	Mpumalanga: Nkangala	Environment and Culture Sector	1
7	88269-EPWP3M	Drilling of Boreholes, Churchill Phase 1	Eastern Cape: Nelson Mandela Bay Metro	Infrastructure Sector	3
8	94216-EPWP3M	Bathurst: Freestone Road	Eastern Cape: Ndlambe	Infrastructure Sector	6
9	77918-EPWP3M	Mbhashe Street Cleaning	Eastern Cape: Mbhashe	Environment and Culture Sector	42
10	70071-EPWP3M	Upgrading of the Manyavu Community Water Supply	KwaZulu Natal: Umgungundlovu	Infrastructure Sector	16
11	77069-EPWP3M	Non Revenue Water Management	KwaZulu Natal: Umgungundlovu	Infrastructure Sector	80
12	93031-EPWP3M	Operation and Maintenance in Dikgatlong	Northern Cape: Dikgatlong	Infrastructure Sector	2
13	98027-EPWP3M	Bufferzone Bulk Water Supply	Northern Cape: Dikgatlong	Infrastructure Sector	14
14	89500-EPWP3M	Cleaning of Stormwater Intakes	Northern Cape: Sol Plaatje	Infrastructure Sector	13
15	57711-EPWP3M	Special Cleaning Team	Northern Cape: Sol Plaatje	Environment and Culture Sector	4
					187

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

The quarter 3 data reported performance for Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported on the EPWP-RS by public bodies* submitted for audit might be overstated.

Non-compliance with ministerial determination 4: Expanded Public Works Programme dated 04 May 2012.

Limitation of scope in confirming the reported information pertaining to Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported in the EPWP-RS by public bodies*

Internal control deficiency

Financial and Performance Management

The department did not implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting.

EPWP Projects are not adequately reviewed against the supporting documentation to ensure that work opportunities created are supported by valid supporting documentation

Recommendation

It is recommended that:

The department should increase their visibility at the public bodies and adequately review the projects at the public bodies for compliance with the Ministerial Handbook.

The department should follow up on all findings noted by the internal, external auditors and also findings from their visits to public bodies to ensure that corrective measures have been implemented.

The department should also obtain evidence from the public bodies that the corrective measures have been implemented on all other EPWP projects not selected for the audit.

Management response

I **am in agreement** with the finding for the following reasons [and supply the following/attached information in support of this]:

The listed names were participants and the requested documents should be available.

Name: Mr. Devan Pillay
Position: Acting DDG: EPWP
Date: 13/05/2020

Auditor's conclusion

Management comment noted. Follow up was performed during the final audit; however, the outstanding required documentation was not subsequently submitted for audit purposes. The issue raised will therefore be reported in the final management report as scope limitation.

3. EPWP – Proof of payments were not provided/ submitted

Requirements

Section 40(a) and (b) of the Public Finance Management Act (PFMA) states that: *“The accounting officer for a department must keep full and proper records of the financial affairs of the department, trading entity or constitutional institution in accordance with any prescribed norms and standards; must prepare financial statements for each financial year in accordance with generally recognized accounting practice...”*

Section 40(3)(a) of the Public Finance Management Act (PFMA) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Section 41 of the Public Finance Management Act (PFMA) furthermore states that *an accounting officer of a department must submit to the relevant Treasury or the Auditor-General such information, returns, documents, explanations and motivations as may be prescribed or as the relevant Treasury or the Auditor-General may require....”*

Paragraph 15(a) to (c) of the Public Auditing Act states that: *“the Auditor-General has at all reasonable times full unrestricted access to Any document, book or written or electronic record or information of the auditee or which reflects or may elucidate the business, financial results, financial position or performance of the auditee; Any of the assets of or under the control of the auditee; or Any staff member or representative of the auditee....”*

Technical indicator description – method of calculation states that: *“A count of the aggregate work opportunities created/reported. Work opportunity is paid work created for an individual on an EPWP project for any period of time. The same person can be employed on different projects and each period of employment will be counted as work opportunity.....”*

The ministerial determination 4: Expanded Public Works Programme dated 04 May 2012 paragraph 12(1)(a) to (e) and 12.2 – Keeping records it states that: *“Every employer must keep a written record of at least the worker’s name and position; copy of an acceptable worker identification; in the case of task-rated worker, the number of tasks completed by the worker; in the case of a time-rated worker, the time worked by the worker; payments made to each worker. The employer must keep this record for a period of at least three years after completion of the EPWP.....”*

Nature

During the audit of Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups*, the following matter was identified at EPWP projects at the various public bodies:

The following participant’s proof of payments were not provided for audit purposes.

No	Project No	Project Name	Public Body	Sector	Number of work opportunities where proof of payments not provided
DPWI					
1	81866-EPWP3N	Momentum Building Health Care Cleaning	Gauteng: DPWI	Environment and Culture Sector	3
2	95592-EPWP3N	Mmabatho High Court	North West: DPWI	Environment and Culture Sector	10
					13
Other Public bodies					
3	76809-EPWP3M	New indoor sports and recreation	Freestate: Matjhabeng	Infrastructure Sector	11
4	63821-EPWP3M	Routine Horticulture and Gardening Maintenance	Mpumalanga: Nkangala	Environment and Culture Sector	1
5	88269-EPWP3M	Drilling of Boreholes, Churchill Phase 1	Eastern Cape: Nelson Mandela Bay Metro	Infrastructure Sector	3
6	88284-EPWP3M	South End Museum Trust	Eastern Cape: Nelson Mandela Bay Metro	Environment and Culture Sector	5
7	91798-EPWP3M	Maintenance of JB Marks Parks	North West: JB Marks	Environment and Culture Sector	12
8	77918-EPWP3M	Mbhashe Street Cleaning	Eastern Cape: Mbhashe	Environment and Culture Sector	26
9	27905-EPWP3M	eThekweni Community Social Support Programme	KwaZulu Natal: eThekweni Metro	Social Sector	1
10	70071-EPWP3M	Upgrading of the Manyavu Community Water Supply	KwaZulu Natal: Umgungundlovu	Infrastructure Sector	3
11	77069-EPWP3M	Non Revenue Water Management	KwaZulu Natal: Umgungundlovu	Infrastructure Sector	26
12	98027-EPWP3M	Bufferzone Bulk Water Supply	Northern Cape: Dikgatlong	Infrastructure Sector	14
13	89500-EPWP3M	Cleaning of Stormwater Intakes	Northern Cape: Sol Plaatjie	Infrastructure Sector	4
14	57711-EPWP3M	Special Cleaning Team	Northern Cape: Sol Plaatjie	Environment and Culture Sector	6
15	89595-EPWP3M	The construction of the bulk link water infrastruc	Northern Cape: Sol Plaatjie	Infrastructure Sector	7
					119

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

The quarter 3 data reported performance for Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported on the EPWP-RS by public bodies* submitted for audit might be overstated.

Non-compliance with ministerial determination 4: Expanded Public Works Programme dated 04 May 2012.

Limitation of scope in confirming the reported information pertaining to Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported in the EPWP-RS by public bodies*

Internal control deficiency

Financial and Performance Management

The department did not implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting.

EPWP Projects are not adequately reviewed against the supporting documentation to ensure that work opportunities created are supported by valid supporting documentation

Recommendation

It is recommended that:

The department should increase their visibility at the public bodies and adequately review the projects at the public bodies for compliance with the Ministerial Handbook.

The department should follow up on all findings noted by the internal, external auditors and also findings from their visits to public bodies to ensure that corrective measures have been implemented.

The department should also obtain evidence from the public bodies that the corrective measures have been implemented on all other EPWP projects not selected for the audit.

Management response

I am in agreement with the finding for the following reasons [and supply the following/attached information in support of this]:

The listed names were participants and the requested documents should be available.

Name: Mr. Devan Pillay
Position: Acting DDG: EPWP
Date: 13/05/2020

Auditor's conclusion

Management comment noted. Follow up was performed during the final audit; however, the outstanding required documentation was not subsequently submitted for audit purposes. The issue raised will therefore be reported in the final management report as scope limitation.

4. EPWP – ID copies were not provided/ submitted

Requirements

Section 40(a) and (b) of the Public Finance Management Act (PFMA) states that: *“The accounting officer for a department must keep full and proper records of the financial affairs of the department, trading entity or constitutional institution in accordance with any prescribed norms and standards; must prepare financial statements for each financial year in accordance with generally recognized accounting practice...”*

Section 40(3)(a) of the Public Finance Management Act (PFMA) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Section 41 of the Public Finance Management Act (PFMA) furthermore states that *an accounting officer of a department must submit to the relevant Treasury or the Auditor-General such information, returns, documents, explanations and motivations as may be prescribed or as the relevant Treasury or the Auditor-General may require....”*

Paragraph 15(a) to (c) of the Public Auditing Act states that: *“the Auditor-General has at all reasonable times full unrestricted access to Any document, book or written or electronic record or information of the auditee or which reflects or may elucidate the business, financial results, financial position or performance of the auditee; Any of the assets of or under the control of the auditee; or Any staff member or representative of the auditee....”*

Technical indicator description – method of calculation states that: *“A count of the aggregate work opportunities created/reported. Work opportunity is paid work created for an individual on an EPWP project for any period of time. The same person can be employed on different projects and each period of employment will be counted as work opportunity.....”*

The ministerial determination 4: Expanded Public Works Programme dated 04 May 2012 paragraph 12(1)(a) to (e) and 12.2 – Keeping records it states that: *“Every employer must keep a written record of at least the worker’s name and position; copy of an acceptable worker identification; in the case of task-rated worker, the number of tasks completed by the worker; in the case of a time-rated worker, the time worked by the worker; payments made to each worker. The employer must keep this record for a period of at least three years after completion of the EPWP.....”*

Nature

During the audit of Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups*, the following matter was identified at EPWP projects at the various public bodies:

The following participant’s Identity documents were not provided for audit purposes.

No	Project No	Project Name	Public Body	Sector	Number of ids not provided
	Other Public bodies				

No	Project No	Project Name	Public Body	Sector	Number of ids not provided
1	76809-EPWP3M	New indoor sports and recreation	Freestate: Matjhabeng	Infrastructure Sector	3
2	88269-EPWP3M	Drilling of Boreholes, Churchill Phase 1	Eastern Cape: Nelson Mandela Bay Metro	Infrastructure Sector	4
3	77918-EPWP3M	Mbhashe Street Cleaning	Eastern Cape: Mbhashe	Environment and Culture Sector	7
4	89500-EPWP3M	Cleaning of Stormwater Intakes	Northern Cape: Sol Plaatje	Infrastructure Sector	8
5	57711-EPWP3M	Special Cleaning Team	Northern Cape: Sol Plaatje	Environment and Culture Sector	6
6	89595-EPWP3M	The construction of the bulk link water infrastruc	Northern Cape: Sol Plaatje	Infrastructure Sector	12
					40

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

The quarter 3 data reported performance for Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported on the EPWP-RS by public bodies* submitted for audit might be overstated.

Non-compliance with ministerial determination 4: Expanded Public Works Programme dated 04 May 2012.

Limitation of scope in confirming the reported information pertaining to Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported in the EPWP-RS by public bodies*

Internal control deficiency

Financial and Performance Management

The department did not implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting.

EPWP Projects are not adequately reviewed against the supporting documentation to ensure that work opportunities created are supported by valid supporting documentation

Recommendation

It is recommended that:

The department should increase their visibility at the public bodies and adequately review the projects at the public bodies for compliance with the Ministerial Handbook.

The department should follow up on all findings noted by the internal, external auditors and also findings from their visits to public bodies to ensure that corrective measures have been implemented.

The department should also obtain evidence from the public bodies that the corrective measures have been implemented on all other EPWP projects not selected for the audit.

Management response

I **am in agreement** with the finding for the following reasons [and supply the following/attached information in support of this]:

The listed names were participants and the requested documents should be available.

Name: Mr. Devan Pillay
Position: Acting DDG: EPWP
Date: 13/05/2020

Auditor's conclusion

Management comment noted. Follow up was performed during the final audit; however, the outstanding required documentation was not subsequently submitted for audit purposes. The issue raised will therefore be reported in the final management report as scope limitation.

5. EPWP – Reported persons with disability evidence or supporting documentation were not provided

Requirements

Section 40(a) and (b) of the Public Finance Management Act (PFMA) states that: *“The accounting officer for a department must keep full and proper records of the financial affairs of the department, trading entity or constitutional institution in accordance with any prescribed norms and standards; must prepare financial statements for each financial year in accordance with generally recognized accounting practice...”*

Section 40(3)(a) of the Public Finance Management Act (PFMA) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Section 41 of the Public Finance Management Act (PFMA) furthermore states that *an accounting officer of a department must submit to the relevant Treasury or the Auditor-General such information, returns, documents, explanations and motivations as may be prescribed or as the relevant Treasury or the Auditor-General may require....”*

Paragraph 15(a) to (c) of the Public Auditing Act states that: *“the Auditor-General has at all reasonable times full unrestricted access to Any document, book or written or electronic record or information of the auditee or which reflects or may elucidate the business, financial results, financial position or performance of the auditee; Any of the assets of or under the control of the auditee; or Any staff member or representative of the auditee....”*

Technical indicator description – method of calculation states that: *“A count of the aggregate work opportunities created/reported. Work opportunity is paid work created for an individual on an EPWP project for any period of time. The same person can be employed on different projects and each period of employment will be counted as work opportunity.....”*

The ministerial determination 4: Expanded Public Works Programme dated 04 May 2012 paragraph 12(1)(a) to (e) and 12.2 – Keeping records it states that: *“Every employer must keep a written record of at least the worker’s name and position; copy of an acceptable worker identification; in the case of task-rated worker, the number of tasks completed by the worker; in the case of a time-rated worker, the time worked by the worker; payments made to each worker. The employer must keep this record for a period of at least three years after completion of the EPWP.....”*

Nature

During the audit of Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups*, the following matter was identified at EPWP projects at the various public bodies:

The following participant’s proof of disability documents were not provided for audit purposes

No	Project No	Project Name	Public Body	Sector	Number of proof of disability not provided
Other Public bodies					
1	77918-EPWP3M	Mbhashe Street Cleaning	Eastern Cape: Mbhashe	Environment and Culture Sector	1
2	91185-EPWP3M	Refurbishment of Galeshewe Main Outfall Sewer	Northern Cape: Sol Plaatje	Infrastructure Sector	2
					3

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

The quarter 3 data reported performance for Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported on the EPWP-RS by public bodies* submitted for audit might be overstated.

Non-compliance with ministerial determination 4: Expanded Public Works Programme dated 04 May 2012.

Limitation of scope in confirming the reported information pertaining to Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported in the EPWP-RS by public bodies*

Internal control deficiency

Financial and Performance Management

The department did not implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting.

EPWP Projects are not adequately reviewed against the supporting documentation to ensure that work opportunities created are supported by valid supporting documentation

Recommendation

It is recommended that:

The department should increase their visibility at the public bodies and adequately review the projects at the public bodies for compliance with the Ministerial Handbook.

The department should follow up on all findings noted by the internal, external auditors and also findings from their visits to public bodies to ensure that corrective measures have been implemented.

The department should also obtain evidence from the public bodies that the corrective measures have been implemented on all other EPWP projects not selected for the audit.

Management response

I **am in agreement** with the finding for the following reasons [and supply the following/attached information in support of this]:

The listed names were participants and the requested documents should be available.

Name: Mr. Devan Pillay
Position: Acting DDG: EPWP
Date: 13/05/2020

Auditor's conclusion

Management comment noted. Follow up was performed during the final audit; however, the outstanding required documentation was not subsequently submitted for audit purposes. The issues raised will therefore be reported in the final management report as scope limitation.

6. EPWP – Participants listed/ reported on project list were not employed on the project

Requirements

Public Finance Management Act (PFMA) section 40(3)(a) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Technical indicator description – method of calculation states that: *“A count of the aggregate work opportunities created/reported. Work opportunity is paid work created for an individual on an EPWP project for any period of time. The same person can be employed on different projects and each period of employment will be counted as work opportunity.....”*

Nature

During the audit of Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups* at the various public bodies, the participants listed below were reported as participants on the EPWP reporting system for the project; including with number of days worked. However, during the audit of the project it was noted that the participants did not work on the project as attendance register and proof of payment could not be obtained.

No	Project No	Project Name	Public Body	Sector	Participants did not worked on project
DPWI					
1	5478-EPWPRS	Masonic Grove Building Refurbishment	KwaZulu Natal: DPWI	Infrastructure Sector	1
2	90517-EPWP3N	Grobleshoop Magistrate's Construction of additional Accommodation	Northern Cape: DPWI	Infrastructure Sector	2
					3
Other Public bodies					
3	77106-EPWP3M	Water Stewards - Ekurhuleni Water Depot	Gauteng: Ekurhuleni Metro	Infrastructure Sector	5
4	70071-EPWP3M	Upgrading of the Manyavu Community Water Supply	KwaZulu Natal: Umgungundlovu	Infrastructure Sector	15
					20

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

The quarter 3 data reported performance for Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported on the EPWP-RS by public bodies* submitted for audit might be overstated.

Internal control deficiency

Financial and Performance Management

The department did not implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting

Beneficiary lists and attendance registers are not regularly reviewed to ensure that participants as per the attendance registers agree to the beneficiary list reported on the EPWP reporting system.

Recommendation

It is recommended that:

The department should perform frequent and adequate reviews of the beneficiary lists and attendance registers to ensure that the number days of participants worked and reported is accurate and valid.

Management response

I **am in agreement** with the finding for the following reasons [and supply the following/attached information in support of this]:

No proof has been submitted that the participants were employed on the project.

Name: Mr. Devan Pillay
Position: Acting DDG: EPWP
Date: 13/05/2020

Auditor's conclusion

Management comment noted.

This matter was followed up during the final audit and confirmed that the participants are still being reported on the Q4 data, therefor this matter will be reported in the management report as an over-reporting of participants.

7. EPWP – EPWP projects were not reported on the EPWP reporting system

Requirements

Public Finance Management Act (PFMA) section 40(3)(a) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Technical indicator description – method of calculation states that: *“A count of the aggregate work opportunities created/reported. Work opportunity is paid work created for an individual on an EPWP project for any period of time. The same person can be employed on different projects and each period of employment will be counted as work opportunity.....”*

Nature

During the audit of EPWP projects at the Lepelle-Nkumpi Local Municipality, the under-mentioned project was not reported on the quarter 3 EPWP reporting system as at 31 December 2019.

No	Project No	Project Name	Public Body	Sector	Beneficiaries not reported for project
	Other Public bodies				
1	100645-EPWP3M	Taring of internal streets zone S to Q access road	Limpopo: Lepelle-Nkumpi	Infrastructure Sector	16

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

Work opportunities created for the financial year could be understated.

Internal control deficiency

Financial and Performance Management

The department did not implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting

Project lists are not regularly reviewed, validated and reported on the National Department of Public Works and Expanded Public Works Programs (EPWP) project list to ensure that all participants are captured on EPWP reporting system.

Recommendation

It is recommended that:

The department should perform adequate and frequent reviews of project lists and it must be reviewed by the senior officials to ensure that all the projects are captured on EPWP reporting system.

Management response

I am in agreement with the finding for the following reasons [and supply the following/attached information in support of this]:

No acceptable reason for the underreporting was provided by the municipality.

The municipality uses the data capturing services of the Limpopo Department of Public Works, Roads and Infrastructure. The department did not capture the project in time for the Quarter 3 report as the project documents were submitted late and had errors.

It remains the responsibility of the municipality to ensure that the data is captured timely and that proper documentation is submitted for the purposes of capturing

Name: Mr. Devan Pillay
Position: DDG: EPWP
Date: 23/03/2020

Auditor's conclusion

Management comment noted.

This matter was followed up during the final audit. The project was reported on the Q4 validated data; however not all the participants were reported on the Q4 validated data.

The matter will be reported in the final management report.

8. No reasons were submitted as to why active project was “stopped”

Requirements

Section 40(a) and (b) of the Public Finance Management Act (PFMA) states that: *“The accounting officer for a department must keep full and proper records of the financial affairs of the department, trading entity or constitutional institution in accordance with any prescribed norms and standards; must prepare financial statements for each financial year in accordance with generally recognized accounting practice...”*

Section 40(3)(a) of the Public Finance Management Act (PFMA) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Section 41 of the Public Finance Management Act (PFMA) furthermore states that *an accounting officer of a department must submit to the relevant Treasury or the Auditor-General such information, returns, documents, explanations and motivations as may be prescribed or as the relevant Treasury or the Auditor-General may require....”*

Paragraph 15(a) to (c) of the Public Auditing Act states that: *“the Auditor-General has at all reasonable times full unrestricted access to Any document, book or written or electronic record or information of the auditee or which reflects or may elucidate the business, financial results, financial position or performance of the auditee; Any of the assets of or under the control of the auditee; or Any staff member or representative of the auditee....”*

Technical indicator description – method of calculation states that: *“A count of the aggregate work opportunities created/reported. Work opportunity is paid work created for an individual on an EPWP project for any period of time. The same person can be employed on different projects and each period of employment will be counted as work opportunity.....”*

The ministerial determination 4: Expanded Public Works Programme dated 04 May 2012 paragraph 12(1)(a) to (e) and 12.2 – Keeping records it states that: *“Every employer must keep a written record of at least the worker’s name and position; copy of an acceptable worker identification; in the case of task-rated worker, the number of tasks completed by the worker; in the case of a time-rated worker, the time worked by the worker; payments made to each worker. The employer must keep this record for a period of at least three years after completion of the EPWP.....”*

Nature

No documentation or reasons was submitted to explain as to why the project 70071-EPWP3M (Upgrading of the Manyavu Community Water Supply Sc) was temporary “stopped” by the municipality, therefore no physical verification of participants were performed.

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

The quarter 3 data reported performance for Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported on the EPWP-RS by public bodies* submitted for audit might be overstated.

Non-compliance with ministerial determination 4: Expanded Public Works Programme dated 04 May 2012.

Limitation of scope in confirming the reported information pertaining to Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported in the EPWP-RS by public bodies*

Internal control deficiency

Financial and Performance Management

The department did not implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting.

EPWP Projects are not adequately reviewed against the supporting documentation to ensure that work opportunities created are supported by valid supporting documentation

Recommendation

It is recommended that:

The department should increase their visibility at the public bodies and adequately review the projects at the public bodies for compliance with the Ministerial Handbook.

The department should follow up on all findings noted by the internal, external auditors and also findings from their visits to public bodies to ensure that corrective measures have been implemented.

The department should also obtain evidence from the public bodies that the corrective measures have been implemented on all other EPWP projects not selected for the audit.

Management response

I am in agreement with the finding for the following reasons [and supply the following/attached information in support of this]:

Documentation or reasons as to why the project 70071-EPWP3M was temporary stopped by the municipality should be available.

Name: Mr. Devan Pillay
Position: Acting DDG: EPWP
Date: 13/05/2020

Auditor's conclusion

Management comment noted. The matters raised will be reported in the management report as no supporting documentation were submitted for audit purposes.

DRAFT

9. EPWP – Beneficiary's proof of change in banking details were not provided

Requirements

Section 40(a) and (b) of the Public Finance Management Act (PFMA) states that: *"The accounting officer for a department must keep full and proper records of the financial affairs of the department, trading entity or constitutional institution in accordance with any prescribed norms and standards; must prepare financial statements for each financial year in accordance with generally recognized accounting practice..."*

Section 40(3)(a) of the Public Finance Management Act (PFMA) states that: *"The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned...."*

Section 41 of the Public Finance Management Act (PFMA) furthermore states that *an accounting officer of a department must submit to the relevant Treasury or the Auditor-General such information, returns, documents, explanations and motivations as may be prescribed or as the relevant Treasury or the Auditor-General may require...."*

Paragraph 15(a) to (c) of the Public Auditing Act states that: *"the Auditor-General has at all reasonable times full unrestricted access to Any document, book or written or electronic record or information of the auditee or which reflects or may elucidate the business, financial results, financial position or performance of the auditee; Any of the assets of or under the control of the auditee; or Any staff member or representative of the auditee...."*

Technical indicator description – method of calculation states that: *"A count of the aggregate work opportunities created/reported. Work opportunity is paid work created for an individual on an EPWP project for any period of time. The same person can be employed on different projects and each period of employment will be counted as work opportunity....."*

The ministerial determination 4: Expanded Public Works Programme dated 04 May 2012 paragraph 12(1)(a) to (e) and 12.2 – Keeping records it states that: *"Every employer must keep a written record of at least the worker's name and position; copy of an acceptable worker identification; in the case of task-rated worker, the number of tasks completed by the worker; in the case of a time-rated worker, the time worked by the worker; payments made to each worker. The employer must keep this record for a period of at least three years after completion of the EPWP....."*

Nature

During the audit of EPWP project at the Mafikeng Local Municipality, the following beneficiary's proof of change in banking details were not provided for audit purposes.

No	Project No	Project Name	Public Body	Sector	Banking details not submitted
Other Public bodies					
1	75688-EPWP3M	Meter Reading within Mahikeng and Mmabatho	North West: Mahikeng	Social Sector	4

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

The quarter 3 data reported performance for Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported on the EPWP-RS by public bodies* submitted for audit might be overstated.

Non-compliance with ministerial determination 4: Expanded Public Works Programme dated 04 May 2012.

Limitation of scope in confirming the reported information pertaining to Indicator 3.1 *Number of work opportunities reported in the EPWP-RS by public bodies* and Indicator 3.2 *Percentage EPWP participation among designated groups reported in the EPWP-RS by public bodies*

Internal control deficiency

Financial and Performance Management

The department did not implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting.

EPWP Projects are not adequately reviewed against the supporting documentation to ensure that work opportunities created are supported by valid supporting documentation

Recommendation

It is recommended that:

The department should increase their visibility at the public bodies and adequately review the projects at the public bodies for compliance with the Ministerial Handbook.

The department should follow up on all findings noted by the internal, external auditors and also findings from their visits to public bodies to ensure that corrective measures have been implemented.

The department should also obtain evidence from the public bodies that the corrective measures have been implemented on all other EPWP projects not selected for the audit.

Management response

I **am in agreement** with the finding for the following reasons [and supply the following/attached information in support of this]:

The listed names were participants and the requested documents should be available.

Name: Mr. Devan Pillay
Position: Acting DDG: EPWP
Date: 06/04/2020

Auditor's conclusion

Management comment noted. The matters raised will be reported in the final management report as no supporting documentation were submitted for audit purposes.

DRAFT

10. EPWP – DPWI Regional Office – Participants listed/ reported on project list as people with disability without the relevant supporting documentation.

Requirements

Public Finance Management Act (PFMA) section 40(3)(a) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Technical indicator description – method of calculation states that: *“The work opportunities reported by public bodies are disaggregated into women, youth and people with disability. Percentage calculation of Number of work opportunities reported for people with disability / Total number of work opportunities reported. ...”*

Nature

During the audit of Indicator 3.2 *Percentage EPWP participation among designated groups* at the DPWI Regional Office, the participant listed below was reported as a person with disability on the EPWP reporting system for the project; including with number of days worked. However, during the audit of the project it was noted that no evidence could not be obtained to substantiate the disability reporting.

No	Name	Surname	ID	Project Code	Project Name	Sector
1	Nwabisa Primrose	Holani	8909180981080	97023-EPWP3N	KWT Magistrate Office General Labour (Blue Disa)	Infrastructure Sector

Impact of the finding

Non-compliance with PFMA section 40(3) (a)

The quarter 3 data reported performance for Indicator 3.2 *Percentage EPWP participation among designated groups reported on the EPWP-RS by public bodies* submitted for audit might be overstated.

Internal control deficiency

Financial and Performance Management

The department did not implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting

Beneficiary lists and disability declaration documents are not regularly reviewed to ensure that participants as per the disability declaration documents agree to the people with disability information reported on the EPWP reporting system.

Recommendation

It is recommended that:

The department should perform frequent and adequate reviews of the beneficiary lists along with the disability declaration documents to ensure, that participants with disability are reported accurately and is valid.

Management response

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

Description	Response	
Corrective action to be taken		
Does the finding affect an amount disclosed in the financial statements	Yes	No
If yes, what corrections will be made to the population		
If yes, the process followed to correct the population, including the internal controls put in place to ensure that the misstatement does not recur in future.		
If yes and the population was adjusted, the proposed adjusting journal entries to correct the population, with the supporting documentation.		
Acknowledgement that additional audit costs will be incurred in order to audit the proposed adjustments and that the financial statements will not be adjusted if material misstatements still exist. (Under these circumstances the misstatements identified originally will be reported by the auditor.)	Yes	No
If yes and no corrections will be made, the reason why such a conclusion has been reached should be indicated.		
Position of official responsible to take corrective actions		
Estimated completion date for corrective action		
Does management agree with the root cause indicated	Yes	No
If management does not agree with the root cause indicated, please provide the root cause according to management.		
Does management agree with the internal control deficiencies indicated	Yes	No
If management does not agree with the internal control deficiency indicated, please provide the internal control deficiency according to management.	<ul style="list-style-type: none"> 	

Name:
Position:
Date:

Auditor's conclusion

DRAFT

Goods and Services

11. Follow up of state funerals finding raised in 2018/19 audit

Requirements

Public Finance Management Act paragraph 38(1)(a)(i) states that *“The accounting officer for a department must ensure that the department has and maintains effective, efficient and transparent systems of financial and risk management and internal control”*

Section 38(1)(b)(i) of the Public Finance Management Act states that *“The accounting officer for a department is responsible for the effective, efficient, economical and transparent use of the resources of the department, trading entity or constitutional institution...”*

Public Finance Management Act paragraph 38(1)(c)(ii) states that *“The accounting officer for a department must take effective and appropriate steps to prevent unauthorized, irregular and fruitless and wasteful expenditure and losses resulting from criminal conduct”*

Treasury Regulation (TR) 8.1.1 states that *“The accounting officer of an institution must ensure that internal procedures and internal control measures are in place for payment approval and processing. These internal controls should provide reasonable assurance that all expenditure is necessary...”*

Treasury Regulation paragraph 8.2.1 states that *“An official of an institution may not spend or commit public money except with the approval (Either in writing or duly authorised electronic means) of the accounting officer or a properly delegated or authorised officer.”*

Treasury Regulation 8.2.2 states that *“Before approving expenditure or incurring a commitment to spend, the delegated or authorised official must ensure compliance with any limitations or condition attached to the delegation or authorisation.”*

Nature

During the 2018/19 financial period, findings were raised with respect to state funerals (COFF 7 of 2018/19), wherein we noted weaknesses in the contract management processes. These weaknesses resulted in payments made on those contracts being in excess of the amounts required as per the pricing schedule that was submitted by the supplier during the tender process. In other instances, the invoice that was submitted by the supplier for payment purposes included items that were not initially quoted as per pricing schedule which was submitted by the supplier during the tender process.

Management agreed with the findings, and committed to conducting a forensic investigation into the funerals to determine the cause, extent and responsibility for the irregularity.

During the follow up conducted during interim audit in the current year, we noted that the investigation was conducted by PwC, and confirmed the matters initially identified by the auditors. The information confirmed the following discrepancies:

1. The prices that were charged on the invoice were different from the prices that were quoted on the pricing schedule that was submitted by the supplier during the tender process.

2. The prices that were charged on the invoice were different from the prices that were quoted by the supplier prior to the event.
3. Quantities on the invoice differed from the quantities agreed to on the quotation, with no evidence of additional items being requested by the department.

Invoiced amounts exceed pricing schedule price

When comparing the invoice with the approved pricing schedule differences were identified as indicated on the table below:

Event	Supplier	Difference identified (Rand)	VAT (Rand)	TOTAL (Rand)
State Funeral for Mama Winnie Madikizela Mandela	Crocia Events	2 115 055,74	317 258,36	2 432 314,10
State Funeral for Zola Skweyiya	Crocia Events	4 713 764,76	1 905 576,00	2 808 188,76
State Funeral for Billy Modise	Crocia Events	79 100,00	11 865,00	90 965,00
TOTAL				5 331 467,86

Invoiced amounts exceed quoted price

Furthermore, it was noted that there were additional items and amounts that were included on the invoice and paid for, which did not appear on the approved pricing schedule submitted by the supplier. These items were included in the quotation provided by the supplier prior to the event, however the prices quoted in the quotation differed from the prices charged per the invoice. Of specific concern was the fact that the initial quotation included Management Fees as an item in the funerals for Mandela and Skweyiya, which was not included on as a separate item on the final invoice. However, the quotation total and the invoice total was identical, even though management fees were removed from the invoice. The differences identified in the pricing between the items on the invoice and the quotation are indicated in the table below.

Event	Supplier	Difference identified (Rand)	VAT (Rand)	TOTAL (Rand)
State Funeral for Mama Winnie Madikizela Mandela	Crocia Events	1 768 441,14	265 266,17	2 033 707,31
State Funeral for Zola Skweyiya	Crocia Events	420 223,04	63 033,46	483 256,50
TOTAL				2 516 963,81

Invoiced quantities exceed quoted quantities

Event	Supplier	Difference identified (Rand)	VAT (Rand)	TOTAL (Rand)
State Funeral for Mama Winnie Madikizela Mandela	Crocia Events	309 750,00	46 462,50	356 212,50

Refer to the annexures for detailed calculations.

Impact

Non – compliance with Treasury Regulation paragraph 8.1.1, 8.2.1 and 8.2.2 resulting in irregular expenditure.

A financial loss of R7 848 431,67 as a result of price variances.

A possible financial loss of R356 212,50 as a result of variance in quantity between invoice and quotation for which there was no documented evidence of services being requested or received.

Internal control deficiency

Financial and performance management

Management did not review and monitor compliance with applicable laws and regulations as a result, irregular expenditure was incurred.

Internal procedures and internal control measures in place for the approval and processing of payments were not adequate, or were not implemented.

Management did not implement controls over reconciling quotations received from suppliers and invoices submitted for payment.

Recommendation

It is recommended that:

Management must determine the total financial losses which were suffered by the department as a result of the above-mentioned irregularities. The workings must be submitted to the AGSA.

The expenditure must be included in the irregular expenditure register.

Management must revisit the population for expenditure relating to state events and determine if there are more misstatements and update the irregular expenditure register. The workings must be submitted to the AGSA.

Management must develop or enhance compliance procedures to ensure compliance with all prescribed laws and regulations. In addition, such procedures include enhancement of compliance checklists already developed.

Management response:

Management conducted the investigation with regard to the said three funerals. The investigation revealed the following with regard to the irregularities with respect to each funeral:

State Funerals				
Nature of transaction		Madikizela-Mandela	Dr Skweyiya	Amb Modise
Payment date		25-May-18	24-May-18	14-Aug-18
Total Invoice (excl 15% VAT)		31 071 161,61	25 189 383,80	9 948 401,60
Deviations not approved		17 899 174,15	6 108 830,00	5 540 725,00
Variations not approved		8 399 566,06	14 762 023,80	826 070,00
Irreconcilable items		29 400,00	3 500,00	402 000,00

Sub-total		26 328 140,21	20 874 353,80	6 768 795,00
VAT @ 15%	15%	3 949 221,03	3 131 153,07	1 015 319,25
Total		30 277 361,24	24 005 506,87	7 784 114,25
Unapproved Management fee		4 052 760,21	3 285 571,80	-

The Department has further opened a case with the SA Police Services for civil recovery against Crocia Events as recommended by the investigation report. The case number is CAS793/2020 opened at Pretoria Central Police Station. Furthermore, the investigation report recommended disciplinary actions against the responsible officials and this is also being implemented by management.

Description	Response	
Does the finding result in a financial loss to the department?	Yes	No
	X	
If yes, please indicate the financial loss amount.	R7,740,332.01 (excl VAT)	
If no, please indicate reasons why there is no financial loss		
Corrective action to be taken	Review all payments made on state events (funeral and state visits). Disciplinary actions will be taken against employees found to have caused the department any financial loss. Civil and criminal actions will be instituted against any service providers found for wrongdoing.	
Does the finding affect an amount disclosed in the financial statements	Yes	No
	X	
If yes, what corrections will be made to the population	Review all payments made on state events (funeral and state visits) and disclose the amount appropriately in the disclosure notes.	
If yes, the process followed to correct the population, including the internal controls put in place to ensure that the misstatement does not recur in future.	Procurement in Prestige on state events will be subject to review of SCM processes before any appointment.	
If yes and the population was adjusted, the proposed adjusting journal entries to correct the population, with the supporting documentation.		
Acknowledgement that additional audit costs will be incurred in order to audit the proposed adjustments and that the financial statements will not be adjusted if material misstatements still exist. (Under these circumstances the misstatements identified originally will be reported by the auditor.)	Yes	No
	X	
If yes and no corrections will be made, the reason why such a conclusion has been reached should be indicated.		
Position of official responsible to take corrective actions		
Estimated completion date for corrective action	31 December 2020	
Does management agree with the root cause indicated	Yes	No
	X	

Description	Response	
If management does not agree with the root cause indicated, please provide the root cause according to management.		
Does management agree with the internal control deficiencies indicated	Yes	No
	X	
If management does not agree with the internal control deficiency indicated, please provide the internal control deficiency according to management.		

Name: Lesetja Toona

Position: Director

Date: 01/09/2020

Auditor's conclusion

Management's comment noted, and cognizance is taken of the fact that management agrees with the finding. The amended annual financial statements will be reviewed to confirm the required disclosures are adequately made. Follow up will be performed in the following period to confirm that the required consequence management has been performed.

12. Follow up of state events finding raised in 2018/19 audit

Requirement

Public Finance Management Act paragraph 38(1)(a)(i) states that *“The accounting officer for a department must ensure that the department has and maintains effective, efficient and transparent systems of financial and risk management and internal control”*

Section 38(1)(b)(i) of the Public Finance Management Act states that *“The accounting officer for a department is responsible for the effective, efficient, economical and transparent use of the resources of the department, trading entity or constitutional institution...”*

Public Finance Management Act paragraph 38(1)(c)(ii) states that *“The accounting officer for a department must take effective and appropriate steps to prevent unauthorized, irregular and fruitless and wasteful expenditure and losses resulting from criminal conduct”*

Treasury Regulation (TR) 8.1.1 states that *“The accounting officer of an institution must ensure that internal procedures and internal control measures are in place for payment approval and processing. These internal controls should provide reasonable assurance that all expenditure is necessary...”*

Treasury Regulation paragraph 8.2.1 states that *“An official of an institution may not spend or commit public money except with the approval (Either in writing or duly authorised electronic means) of the accounting officer or a properly delegated or authorised officer.”*

Treasury Regulation 8.2.2 states that *“Before approving expenditure or incurring a commitment to spend, the delegated or authorised official must ensure compliance with any limitations or condition attached to the delegation or authorisation.”*

Nature

During the 2018/19 financial period, findings were raised with respect to state events (COFF 18 of 2018/19), wherein we noted weaknesses in the contract management processes. These weaknesses resulted in payments made on those contracts being in excess of the amounts required as per the pricing schedule that was submitted by the supplier during the tender process. In other instances, the invoice that was submitted by the supplier for payment purposes included items that were not initially quoted as per pricing schedule which was submitted by the supplier during the tender process.

Management agreed with the findings, and committed on reviewing the business process, structures and controls in events management section together with the provisioning section which create an order number. Furthermore, further meetings were held with management to discuss these matters, and management indicated the scope of the current forensic investigation into state funerals will be extended to include these findings to determine the cause, extent and responsibility for the irregularity.

During the follow up conducted during interim audit in the current year, we noted that the investigation was conducted, however it excluded these findings. The audit work we performed confirmed the following discrepancy:

The prices that were charged on the invoice were different from the prices that were quoted on the pricing schedule that was submitted by the supplier during the tender process.

Invoiced amounts exceed pricing schedule price

When comparing the invoice with the approved pricing schedule differences were identified as indicated on the table below:

Event	Supplier	Payment Batch Number	Difference identified (Rand)	VAT (Rand)	TOTAL (Rand)
State Funeral for Mama Veronica Sobukwe	Crocia Events	2419110	108 100	16 215	124 315
State Funeral for M Mtshali	Crocia Events	2420349	322 770	48 416	371 186
					495 501
BRICS Summit	Side Production	2418760	44 430	6 664	51 094
China State Visit	Side Production	2417704	545 835	81 875	627 710
Ghana State Visit	Side Production	2416023	127 850	19 178	147 028
					825 832
TOTAL					1 321 333

Refer to the annexures for detailed calculations.

Impact

Non – compliance with Treasury Regulation paragraph 8.1.1, 8.2.1 and 8.2.2 resulting in irregular expenditure.

A financial loss of R1 304 222 due to price variances.

Internal control deficiency*Financial and performance management*

Management did not review and monitor compliance with applicable laws and regulations. As a result, irregular expenditure was incurred.

Internal procedures and internal control measures in place for the approval and processing of payments were not adequate, or were not implemented.

Management did not implement controls over reconciling quotations received from suppliers and invoices submitted for payment.

Recommendation

It is recommended that:

Management must determine the total financial losses which were suffered by the department as a result of the above-mentioned irregularities. The workings must be submitted to the AGSA.

The expenditure must be included in the irregular expenditure register.

Management must revisit the population for expenditure relating to state events and determine if there are more misstatements and update the irregular expenditure register. The workings must be submitted to the AGSA.

Management must develop or enhance compliance procedures to ensure compliance with all prescribed laws and regulations. In addition, such procedures include enhancement of compliance checklists already developed.

Management response:

Management takes note of the audit finding. While management has conducted investigation on state funerals that we identified by the audit team, management has since identified the need to review all payments that were made with regard to state funerals. The amount of the finding will be disclosed as irregular expenditure. Furthermore, it is uncertain at this stage if the transactions will or have resulted in financial loss until the investigations are concluded and finalized.

Description	Response	
	Yes	No
Does the finding result in a financial loss to the department?		
If yes, please indicate the financial loss amount.		
If no, please indicate reasons why there is no financial loss		
Corrective action to be taken	Review all payments made on state events (funeral and state visits). Disciplinary actions will be taken against employees found to have caused the department any financial loss. Civil and criminal actions will be instituted against any service providers found for wrongdoing.	
Does the finding affect an amount disclosed in the financial statements	Yes	No
	X	
If yes, what corrections will be made to the population	Review all payments made on state events (funeral and state visits) and disclose the amount appropriately in the disclosure notes.	
If yes, the process followed to correct the population, including the internal controls put in place to ensure that the misstatement does not recur in future.	Procurement in Prestige on state events will be subject to review of SCM processes before any appointment.	
If yes and the population was adjusted, the proposed adjusting journal entries to correct the population, with the supporting documentation.		
Acknowledgement that additional audit costs will be incurred in order to audit the proposed adjustments and that the financial statements will not be adjusted if material misstatements still exist. (Under these circumstances the misstatements identified originally will be reported by the auditor.)	Yes	No
	X	

Description	Response	
If yes and no corrections will be made, the reason why such a conclusion has been reached should be indicated.		
Position of official responsible to take corrective actions		
Estimated completion date for corrective action	31 December 2020	
Does management agree with the root cause indicated	Yes	No
	X	
If management does not agree with the root cause indicated, please provide the root cause according to management.		
Does management agree with the internal control deficiencies indicated	Yes	No
	X	
If management does not agree with the internal control deficiency indicated, please provide the internal control deficiency according to management.		

Name: Lesetja Toona

Position: Director

Date: 01/09/2020

Auditor's conclusion

Management's comment noted, and cognizance is taken of the fact that management agrees with the finding, and will review all payments made in respect of state events and state funerals.

The amended annual financial statements will be reviewed to confirm the required disclosures are adequately made. Follow up will be performed in the following period to confirm that the required steps in terms of consequence management have been performed.

13. Contractors (State Events): Invoiced amounts exceed quoted price and Items invoiced but not included on approved quote

Requirements

Public Finance Management Act paragraph 38(1)(a)(i) states that *“The accounting officer for a department must ensure that the department has and maintains effective, efficient and transparent systems of financial and risk management and internal control...”*

Public Finance Management Act paragraph 38(1)(c)(ii) states that *“The accounting officer for a department must take effective and appropriate steps to prevent unauthorized, irregular and fruitless and wasteful expenditure and losses resulting from criminal conduct...”*

Treasury Regulation paragraph 8.2.1 states that *“An official of an institution may not spend or commit public money except with the approval (Either in writing or duly authorised electronic means) of the accounting officer or a properly delegated or authorised officer.”*

Treasury Regulation 8.2.2 states that *“Before approving expenditure or incurring a commitment to spend, the delegated or authorised official must ensure compliance with any limitations or condition attached to the delegation or authorisation.”*

Nature

During the 2017/18 financial period, the department embarked on a tender process in order to appoint a service provider which would provide services related to state events. The bidders were required to quote prices per item on a specified list of items. The contract period was for 24 months, and explicitly required that prices be fixed for this term (as per terms of reference). Crocia Events was awarded the tender, and was thus the supplier for state funerals during the year under review.

An internal memorandum was then sent to the National Adjudication Bid Committee (NABC) by the project manager on 20 March 2019 requesting to use the current funeral term contract of Crocia Events to provide infrastructure for the SADC Solidarity Conference. NABC approved the internal memo on 20 March 2019 to utilise the funeral term contract for the state event noting to the project manager that the service must also be delivered at the same rates as approved in the current funeral term contract.

During the audit of Goods and Services (Contractors) and Contract Management we noted the following discrepancies:

The prices that were charged on the invoice were different from the prices that were quoted on the pricing schedule that was submitted by the supplier during the tender process

The invoice that was submitted by the supplier for payment purposes included items that were not initially quoted as per pricing schedule (Quotation) which was submitted by the supplier during the tender process;

Invoiced amounts exceed quoted price

Even though the NBAC approval stated that the service must be delivered at the same rates as approved in the current funeral term contract, when comparing the invoice with the approved pricing schedule differences were identified as indicated on the table below:

Event	Supplier	Difference identified (Rand)	VAT (Rand)	TOTAL (Rand)
SADC Solidarity Conference	Crocia Events	17 400,00	2 610,00	20 010,00
				20 010,00

Items invoiced but not included on approved quote

Furthermore, it was noted that there was no approval of variation for additional items and amounts that were included on the invoice and paid for, which did not appear on the approved pricing schedule submitted by the supplier, as indicated on the table below:

Event	Supplier	Difference identified (Rand)	VAT (Rand)	TOTAL (Rand)
SADC Solidarity Conference	Crocia Events	277 377,00	41 607,00	318 984,00
				318 984,00

Please refer to Annexure A for detailed calculations.

Impact

Non – compliance with Treasury Regulation paragraph 8.2.1 and Treasury regulation 8.2.2 resulting in irregular expenditure of R338 994.

Internal control deficiency

Financial and performance management

Management did not review and monitor compliance with applicable laws and regulations. As a result, irregular expenditure was incurred.

Management did not implement controls over reconciling quotations received from suppliers and invoices submitted for payment.

Recommendation

It is recommended that:

Management must develop or enhance compliance procedures to ensure compliance with all prescribed laws and regulations. In addition, such procedures include enhancement of compliance checklists already developed.

The accounting officer must investigate the reasons for irregular expenditure and confirm if it was deliberate. The expenditure must be included in the irregular expenditure register

Management must revisit the population for expenditure relating to state events and determine if there are more misstatements and update the register. The workings must be submitted to the AGSA.

Management response:

Auditor's conclusion

Irregular Expenditure

14. Disclosure note not fairly presented – PWC Report on state events

Requirements

Public Finance Management Act paragraph 38(1)(a)(i) states that *“The accounting officer for a department must ensure that the department has and maintains effective, efficient and transparent systems of financial and risk management and internal control...”*

Section 38(1) (b) (i) of the Public Finance Management Act states that *“The accounting officer for a department is responsible for the effective, efficient, economical and transparent use of the resources of the department, trading entity or constitutional institution...”*

Section 40 of the Public Finance Management Act (PFMA) states that: *“The accounting officer for a department – (a) must keep full and proper records of the financial affairs of the department, in accordance with any prescribed norms and standards...”*

Chapter 3, Paragraph 11 of Modified Cash Standard states that: *“Financial statements shall present fairly the financial position, financial performance and cash flows of a department. Fair presentation requires the faithful representation of the effects of transactions, other events and conditions in accordance with the definitions and recognition criteria for assets, liabilities, revenue and expenses set out in the Standard. The application of the Standard with additional disclosures when necessary is presumed to result in financial statements that achieve fair presentation...”*

Irregular expenditure framework para 8 states that *“For a department to incur irregular expenditure, the non-compliance must be linked to a financial transaction. Although a transaction may trigger irregular expenditure, a department will only record irregular expenditure when a payment pertaining to the non-compliance is actually made (i.e. when the expenditure is recognized in accordance with the Modified Cash Standards) ...”*

Irregular expenditure framework para 16 states that *“If a transaction has been processed in contravention of legislation and the same transaction has a financial implication (payment was made or a liability was recognised in the books), it must be recorded as irregular expenditure...”*

Irregular expenditure framework para 22 and 24 states that *“The accounting officer must conduct a determination test or analyse the particulars of non-compliance in order to establish the facts and losses, if any, related to the transaction. The determination test must be instituted within 30 days from the date that the irregular expenditure was reported to the accounting officer or accounting authority...”*

Irregular expenditure framework para 82 states that *“The accounting officer must ensure that only confirmed irregular expenditure is disclosed in the main note to the annual financial statements...”*

Irregular expenditure framework para 82 states that *“Irregular expenditure not confirmed or in the process of determination or investigation must be disclosed in the sub-note to the annual financial statements related to irregular expenditure...”*

Nature

During the audit of irregular expenditure, the following was noted with respect to note 25 to the financial statement *“At the end of the previous financial year, management had identified potential irregular expenditure amounting to R43 million relating to state events under the Prestige portfolio. Appropriate disclosures will be made once the outcome of the investigations has been finalised...”*

Follow up was conducted during interim audit in the current year, we noted that the investigation was conducted by Pricewaterhouse Coopers Incorporated (PWC). A copy of the investigation report was submitted to AGSA and confirmed that the investigation was finalized and approved by Minister P. de Lille on 28 January 2020.

The information disclosed on note 25 is therefore incorrect as the investigation was finalised and confirmed irregular expenditure, therefore it should have been disclosed in the main note to the annual financial statement.

Impact

Non-compliance with Public Finance Management Act (PFMA)

Irregular expenditure disclosure note is not fairly presented in line with MCS Chapter 3.

Non-compliance with National Treasury Instruction No. 1 of 2018/19

Internal control deficiency

Financial and performance management

Management did not implement a proper financial and reporting system to enable proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting.

Lack of proper review of financial statements submitted for audit to ensure that they are accurate and complete.

Recommendation

It is recommended that:

Management should conduct reviews on completed investigations and determined non-compliance resulting to irregular expenditure to ensure that the annual financial statements and supporting schedules (Irregular expenditure register) are updated with accurate and complete amounts.

Management must develop or enhance compliance procedures to ensure compliance with all prescribed laws and regulations. In addition, such procedures include enhancement of compliance checklists already developed.

Management response:

Management takes note of the audit finding. It must be noted by the audit team that when the annual financial statements were prepared and submitted to the audit team for auditing on 31 July 2020, there was lack of clarity with regard to the status of the investigation report. That clarity was obtained after the disclosure note was prepared and submitted as part of the annual financial statements. The irregular expenditure disclosure note will be updated as per the response to Coff 7.

Name: Lesetja Toona

Position: Director

Date: 01/09/2020

Auditor's conclusion

Management's comment noted, and cognizance is taken of the fact that management agrees with the finding. The amended annual financial statements will be reviewed to confirm the required disclosures are adequately made.

15. Disclosure note not fairly presented – PSC report on SMS appointments

Requirements

Public Finance Management Act paragraph 38(1)(a)(i) states that *“The accounting officer for a department must ensure that the department has and maintains effective, efficient and transparent systems of financial and risk management and internal control...”*

Section 38(1) (b) (i) of the Public Finance Management Act states that *“The accounting officer for a department is responsible for the effective, efficient, economical and transparent use of the resources of the department, trading entity or constitutional institution...”*

Section 40 (a) of the Public Finance Management Act (PFMA) states that: *“The accounting officer for a department must keep full and proper records of the financial affairs of the department, in accordance with any prescribed norms and standards...”*

Section 11 (2) (a) and (b) of the Public Service Act states that: *“In the making of any appointment in terms of section 9 in the public service all persons who applied and qualify for the appointment concerned shall be considered; and the evaluation of persons shall be based on training, skills, competence, knowledge and the need to redress, in accordance with the Employment Equity Act, 1998 (Act No. 55 of 1998), the imbalances of the past to achieve a public service broadly representative of the South African people, including representation according to race, gender and disability.”*

Regulation 67(9) of the Public Service Regulations, 2016 states that: *“Before making a decision on an appointment or the filling of a post, an executive authority shall satisfy herself or himself that the candidate qualifies in all respects for the post and that his or her claims in his or her application for the post have been verified as directed by the Minister; and record that verification in writing.”*

Chapter 3, Paragraph 11 of Modified Cash Standard states that: *“Financial statements shall present fairly the financial position, financial performance and cash flows of a department. Fair presentation requires the faithful representation of the effects of transactions, other events and conditions in accordance with the definitions and recognition criteria for assets, liabilities, revenue and expenses set out in the Standard. The application of the Standard with additional disclosures when necessary is presumed to result in financial statements that achieve fair presentation...”*

Irregular expenditure framework para 8 states that *“For a department to incur irregular expenditure, the non-compliance must be linked to a financial transaction. Although a transaction may trigger irregular expenditure, a department will only record irregular expenditure when a payment pertaining to the non-compliance is actually made (i.e. when the expenditure is recognized in accordance with the Modified Cash Standards) ...”*

Irregular expenditure framework para 16 states that *“If a transaction has been processed in contravention of legislation and the same transaction has a financial implication (payment was made or a liability was recognised in the books), it must be recorded as irregular expenditure...”*

Irregular expenditure framework para 22 and 24 states that *“The accounting officer must conduct a determination test or analyse the particulars of non-compliance in order to establish the facts and losses, if any, related to the transaction. The determination test must be instituted*

within 30 days from the date that the irregular expenditure was reported to the accounting officer or accounting authority...

Irregular expenditure framework para 82 states that *“The accounting officer must ensure that only confirmed irregular expenditure is disclosed in the main note to the annual financial statements...”*

Nature

An investigation was conducted by the Public Service Commission on the appointment of senior management officials for the department and the trading entity from the period of 1 April 2017 to 31 March 2018. The finalised report was received by the then Minister of Public Works on 8 February 2019. The investigation confirmed numerous irregularities in the appointments made during the period, as summarized in the annexure to this finding.

During the audit of irregular expenditure (disclosure note 25), it was noted that the expenditure incurred on the irregular appointments of the identified officials were not disclosed for the current financial year.

Impact

Non-compliance with Public Finance Management Act (PFMA).

Non-compliance with the Public Service Act and Regulations which resulted in the irregular expenditure been identified.

Irregular expenditure disclosure note is not fairly presented in line with MCS Chapter 3.

Irregular expenditure is understated by R5 815 938,00 for the current year under review and R6 767 478,00 for the prior year

Internal control deficiency

Financial and performance management

Management did not implement a proper financial and reporting system to enable proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support financial and performance reporting.

Lack of proper review of financial statements submitted for audit to ensure that they are accurate and complete.

Recommendation

It is recommended that:

Management should conduct reviews on completed investigations and determined non-compliance resulting in irregular expenditure to ensure that the annual financial statements and supporting schedules (Irregular expenditure register) are updated with accurate and complete amounts.

Management must develop or enhance compliance procedures to ensure compliance with all prescribed laws and regulations. In addition, such procedures include enhancement of compliance checklists already developed.

Management response:

Management acknowledges the audit finding and wishes to respond as thus:

- a. The Public Service Commission investigation was ordered by Executive Authority of DPWI through the assistance of Minister Public Service & Administration in order to determine if the appointments made by DPWI in 2017-2018 financial were effected in compliance with public service prescripts.
- b. Following this investigation, the PSC made findings to the effect that the appointments of twelve SMS members by DPWI were effected without following the public service prescripts based on various reasons. Further to this, the report recommended corrective action of amongst others, taking disciplinary actions against the panel members and the approving authority and to approach the Court to review and set aside the appointments in terms Section 5 (7) (a) of the Public Service Act of 1994 as amended.
- c. As a result thereof, the Executive Authority accepted the findings and recommendations and proceeded to instruct the Department to prefer charges against the panel members and approving authorities, and to institute Labour Court application to review and set-aside the irregular appointments of the relevant twelve employees.
- d. Disciplinary actions taken against the fourteen panel members are currently underway with all of them defending the charges preferred by the employer whilst the Labour Court application has been served and it is only being opposed by one of the twelve employees and it is currently pending allocation of date of hearing by Registrar.
- e. Furthermore, the eleven employees have also filed a review application in the Labour Court to review and set aside the PSC report, however, the DPWI filed its opposing papers and the application is still pending.
- f. Until the disciplinary actions and Labour Court reviews are heard and concluded successfully in favour of the employer, it will be premature for DPWI to disclose the expenditure in the financial statement as irregular, resulting in irregular expenditure. Management will make a narrative note in the disclosure and provide regular updates to AGSA until finalization of the processes where the status of the expenditure will be clearly determined.
- g. In view of the above, the AGSA's findings that the DPWI should have disclosed the expenditure resulting from this appointments as irregular expenditure may be premature since the relevant forums processing the findings and recommendations are still pending. Should management accept the findings of AGSA now and it is then determined later that the appointments were not irregularly effected then the Department will be prejudiced.
- h. It is therefore our view that the AGSA should consider Management's response that any conclusion that the resulting appointments have resulted in irregular expenditure be suspended pending the finalization of the pending disciplinary action and the Labour Court applications which will provide clear certainty.

- i. The Irregular Expenditure Framework issued by National Treasury does not make provision for instances where the actual report and its finding are being challenged. Only confirmed irregular expenditure must be disclosed in the annual financial statements, and disciplinary actions instituted against the employees found to have caused the irregular expenditure. At the moment the findings of the report are being challenged, as elucidated above, at various forum and the Department will only make a final determination once there is certainty as to the findings, which give rise, in this instance, to the appointment being regarded as irregular expenditure.

Name: Lesetja Toona

Position: Director

Date: 14 September 2020

Auditor's conclusion

Managements comment noted. We take cognizance of the following:

- the department (represented by Executive Authority) accepted the findings and recommendations
- the department has approached the court to set-aside the irregular appointments of the relevant twelve employees
- disciplinary actions taken against the fourteen panel members are currently underway

It is thus clear that there is no disagreement from the department with the findings contained in the report of the Public Service Commission.

Irregular expenditure Framework 2019-20: par 77 – **Reporting in the note to the annual Financial statement** include the following table:

Description	Transgression took place in the current financial year	Transgression took place in the previous financial year
ASSESSMENT		
Alleged transaction related to irregular expenditure was identified and in the process of confirmation	No disclosure in the irregular expenditure note	No disclosure in the irregular expenditure note
DETERMINATION		
Alleged transaction was confirmed as irregular expenditure; and Further determination to identify facts and losses related to the transaction	Disclose amount(s) of irregular expenditure confirmed in the irregular expenditure note; and Disclose progress of irregular expenditure in the sub-note Irregular Expenditure under Determination Include supplementary disclosure on disciplinary steps taken	Disclose amount(s) of irregular expenditure confirmed in the irregular expenditure note; and Disclose progress of irregular expenditure in the sub-note Irregular Expenditure under Determination Include supplementary disclosure on disciplinary steps taken

The fact that the Executive Authority accepted the findings and recommendations and proceeded to instruct the Department to take disciplinary actions against the fourteen panel members provides proof that there is agreement with the non-compliances identified by the PSC. Any salary expenditure payments made contrary to the provisions of PSA 11(2) and PSR, 2016 - Reg 67(9) will result into irregular expenditure. Considering the reporting guidance included the Irregular expenditure framework, the process is at the determination

stage as the alleged transaction was confirmed as irregular expenditure and further determination to identify facts and losses related to the transaction is in progress. Therefore, the department needs to:

1. Disclose amount(s) of irregular expenditure confirmed in the irregular expenditure note; and
2. Disclose progress of irregular expenditure in the sub-note Irregular Expenditure under Determination
3. Include supplementary disclosure on disciplinary steps taken.

The auditors have also verified the non-compliance and confirmed there was a payment of salaries. Therefore irregular expenditure has been incurred. The outcome of the disciplinary actions or the Labour court application will not change the fact that there were non-compliances and subsequently salaries paid which lead to irregular expenditure.

The finding therefore remains, and the matter will be included in the final management report as an issue relating to the completeness of disclosure relating to Irregular Expenditure (disclosure note 25).

ANNEXURE B: OTHER IMPORTANT MATTERS

Predetermined objectives

16. Predetermined objectives: Validity of reported performance information for Programme 5 - Indicator 3 (Percentage of movable assets provided within 60 days after approval by prestige clients)

Requirements

Public Finance Management Act (PFMA) section 40(3)(a) states that: *“The annual report and audited financial statements referred to in subsection (1)(d) must fairly present the state of affairs of the department, trading entity or constitutional institution, its business, its financial results, its performance against predetermined objectives and its financial position as at the end of the financial year concerned....”*

Nature

During the walkthrough of Programme 5: Indicator 3 (Percentage of movable assets requests provided within 60 days after approval by prestige client), the undermentioned request was incorrectly included in the Q1 supporting schedules as “provided within 60 days”.

Indicator 5.3-Percentage of movable assets requests provided within 60 days after approval by prestige clients				
No	Prestige client	Date of request	Date of delivery	Number of days lapsed
1	Union Buildings Cabinet room : 2 high back chairs	28-Sep-18	17-May-19	230

Impact of the finding

The reported performance information as contained in the Annual Performance Report may not be valid and accurate.

Internal control deficiency

Financial and performance management

Management did not prepare regular, accurate and complete financial and performance reports that are supported and evidenced by reliable information.

Recommendation

It is recommended that:

The department should implement processes to ensure that actual achievements reported on the quarterly reports and ultimately the annual performance report is valid and supported by sufficient and appropriate portfolio of evidence.

Management response

I am in agreement with the finding for the following reasons. This is incorrectly included in the Performance indicator

Before inputs submitted to M& E will be checked and verified the validity

Chief Director will be responsible for ensuring the correctness

The action will be completed before year end the 31/03/2020

The Root causes of the audit finding was due to the mistakenly stated on the schedule due to the delivery date.

Name: M Sazona

Position: Chief Director: Prestige

Date: 24/02/2020

Auditor's conclusion

Management comment noted. The matter will be reported in the management report. This matter will also be followed up during the final audit confirming the annual performance report information.

Non – compliance with legislation

17. Payments not made within 30 days

Requirements

Public Finance Management Act (PFMA) section 38(1)(f) state that: *“The accounting officer for a department, trading entity or constitutional institution must settle all contractual obligations and pay all money owing, including inter-governmental claims, within the prescribed or agreed period.”*

Treasury Regulation 8.2.3 requires that: *“Unless determined otherwise in a contract or other agreement, all payments due to creditors must be settled within 30 days from receipt of an invoice or, in the case of civil claims, from the date of settlement or court judgment.”*

Instruction note 34 of National Treasury dated 30 November 2011 state that:

“4.1. The accounting officer’s responsibility [in terms of section 38(1)(f)] to settle all contractual obligations and to pay all money owing, including intergovernmental claims, within the prescribed (30 days) or agreed period is hereby re-iterated.4.

4.2. Within thirty days (30) days from the date of this Instruction Note, all departments are required to have in place systems (processes and procedures) that will enable the tracking of each invoice received from the various service providers.”

4.3. The system referred to in paragraph 4.2 above may either be manual or electronic in nature and such a system must also be able to track progress with the processing of each invoice.”

4.4. At any given time, such a system must be able to provide information related to the date on which an invoice was received, the date on which it was paid and the time period between the date of receipt and the date of payment, if the invoice was indeed paid.”

Nature

The following payments were not made within 30 days from the date of receipt of the invoice:

No	Supplier name	Payment number	Amount	Date of receipt of invoice (Registry stamp)	Payment date	Number of day in which payment is made from receipt of invoice
1.	KWANTU INFORMATION TECHNOLOGY	PM-157226 - OR-062568	99 475,00	2019/06/12	2019/08/06	55
2.	PROPERTY MANAGEMENT TRADING ENTITY	2424121	758 979,20	2019/04/02	2019/05/03	31

Impact

The aforementioned findings may result in:

Non-compliance with Section 38 of the Public Finance Management Act

Non-compliance with Treasury Regulations 8.2.3

Non-compliance with Instruction Note 34 of National Treasury

Internal control deficiency

Leadership

Management does not effectively establish and communicate policies and procedures to enable and support understanding and execution of internal control objectives, processes and responsibilities

Monitoring controls did not ensure that creditors were paid within the required 30 days of receipt of the invoice.

Recommendation

Payments should be processed in a speedy manner without compromising internal controls.

The entity should ensure that the implementation and roll out of the invoice tracking system occurs timeously.

Management response

Management agrees with the finding. Late payments are mainly due to late submission of invoices to finance for processing. Finance continues to follow up on long outstanding invoices. The Department has since strengthened consequence management process.

Name: Azwihangwisi Negota

Position: Director

Date: 15 September 2020

Auditor's conclusion

Management comment noted, and cognizance is taken of the fact that management agrees with the finding. The non-compliance will be included in the final management report.

Employee Benefits – Performance award

18. Performance award (Employee Benefits) – Disclosed amount incorrectly calculated and presented

Requirements

Section 40 (a) of the Public Finance Management Act (PFMA) states that: “The accounting officer for a department must keep full and proper records of the financial affairs of the department, in accordance with any prescribed norms and standards...”

Section 73(3) of the Public Service Regulations (PSR) states that: “The Minister shall from time to time determine a percentage of a department’s remuneration budget that shall not be exceeded for the purpose of granting performance rewards.”

Department of Public Service and Administration (DPSA) Circular 1 of 2019 paragraph 5 states that: “However, where there is a reduction in the limit as set by the MPSA from time to time, each department will have to, accordingly pro rata, adjust its Incentive Scheme, to tally with the quantum generated by the percentage of their remuneration budget as determined by the MPSA. This ceiling as determined by the MPSA **may not be exceeded** under any circumstances. No deviation in this regard will be considered by the MPSA.”

DPSA Circular 1 of 2019 paragraph 9 states that: “It is for the above reasons, that the MPSA has approved the **decremental adjustment of the percentage that can be allocated from the remuneration budget for the payment of performance bonuses**, as tabulated below, for ALL categories of employees, which is also applicable to members of the SMS.”

DPSA Circular 1 of 2019 paragraph 10 states that: “This means that the maximum percentage for a budgeted provisioning for performance rewards is set out as follows for the indicated financial years:

Financial Year	Maximum % of Remuneration Budget
2018-19	1.5%
2019-20	0.75%
2020-21	0.5%
2021-22	0%
Post 2022	To be determined based on the Comprehensive Review of ALL PMDSs for ALL categories of Employees

DPSA Circular 1 of 2019 paragraph 16 states that: “Departments are hereby instructed to hereby amend their internal administrative policies to be aligned to the revised directive, which is elucidated in this circular.”

DPSA Circular 1 of 2019 paragraph 17 states that: “Departments must ensure that all employees in their respective departments are informed accordingly to the contents of this circular.”

Chapter 3, Paragraph 11 of Modified Cash Standard states that: “Financial statements shall present fairly the financial position, financial performance and cash flows of a department. Fair presentation requires the faithful representation of the effects of transactions, other events and conditions in accordance with the definitions and recognition criteria for assets, liabilities,

revenue and expenses set out in the Standard. The application of the Standard with additional disclosures when necessary is presumed to result in financial statements that achieve fair presentation...”

Nature

During the audit of performance awards as disclosed in employee benefits (disclosure note 22), it was noted that the incorrect percentage (1.5%) was used to calculate the current year amount instead of the approved percentage (0.75%) as per DPISA Circular 1.

The use of the incorrect percentage resulted in the overstatement of performance award amount and the total employee benefit disclosure note.

Disclosure item in Employee Benefits note (Note 22)	Compensation of employees - 2019/20 Appropriation	Department's calculation		Auditors calculation		Difference identified (Rand)
		% used	Amount disclosed	% used	Amount calculated	
Performance awards	557 826 000	1.5%	8 367 390	0.75%	4 183 695	4 183 695

Impact

Non-compliance with Public Finance Management Act (PFMA).

Non-compliance with the Public Service Regulations and DPISA Circular 1 of 2019 which resulted in the overstatement of performance awards been identified.

Performance awards in the employee benefits disclosure note is not fairly presented in line with MCS Chapter 3.

Performance awards in the employee benefits disclosure note is overstated by R4 183 695,00 for the current year under review.

Internal control deficiency

Financial and performance management

Management did not review and monitor compliance with applicable laws and regulations.

Lack of proper review of financial statements submitted for audit to ensure that they are accurate and complete.

Recommendation

It is recommended that:

Management should conduct reviews to ensure that the annual financial statements and supporting schedules are updated with accurate and complete amounts.

Management must develop or enhance compliance procedures to ensure compliance with all prescribed laws and regulations. In addition, such procedures include enhancement of compliance checklists already developed.

Management response:

The department is in agreement with the findings that Employee benefit amount disclosed in the annual financial statements was overstated as result of incorrect percentage used to calculate the performance award amount. The financial statements are amended, refer to the attached adjusted note.

Description	Response	
Does the finding result in a financial loss to the department?	Yes	No
		X
If yes, please indicate the financial loss amount.	N/A	
If no, please indicate reasons why there is no financial loss	The disclosure in question is a provision to the financial statements (Employees Benefits) and does not equate to outflow of cash or assets of the department as at reporting date.	
Corrective action to be taken	Rectified the percentage and updated the Employee benefit note.	
Does the finding affect an amount disclosed in the financial statements	Yes	No
	x	
If yes, what corrections will be made to the population	Adjust the note with the correct amount.	
If yes, the process followed to correct the population, including the internal controls put in place to ensure that the misstatement does not recur in future.	Recalculate the provision using the correct 0.75% prescribed on DPISA Circular 1 of 2019 and adjust the disclosure.	
If yes and the population was adjusted, the proposed adjusting journal entries to correct the population, with the supporting documentation.	See attached Annexure A	
Acknowledgement that additional audit costs will be incurred in order to audit the proposed adjustments and that the financial statements will not be adjusted if material misstatements still exist. (Under these circumstances the misstatements identified originally will be reported by the auditor.)	Yes	No
		x
If yes and no corrections will be made, the reason why such a conclusion has been reached should be indicated.	N/A	
Position of official responsible to take corrective actions	D: Financial Accounting	
Estimated completion date for corrective action	Done	
Does management agree with the root cause indicated	Yes	No
		x

Description	Response	
If management does not agree with the root cause indicated, please provide the root cause according to management.	Management omission.	
Does management agree with the internal control deficiencies indicated	Yes	No
		x
If management does not agree with the internal control deficiency indicated, please provide the internal control deficiency according to management.	Oversight	

Name: Azwihangwisi Negota

Position: Director

Date: 15 September 2020

Auditor's conclusion

Management's comments noted, and cognizance is taken of the fact that management agreed with the finding and will make amendments to the final AFS. The proposed amendment has been inspected, and is in line with our expectation. The misstatement portion finding will be resolved when the final AFS are received, and the amendment is confirmed, however the finding will remain as an internal control deficiency.

Procurement and Contract Management

19. Publish of awards on eTender Publication and Government Tender Bulletin

Requirements

Public Auditing Act paragraph 15 (a) to (c) states that: *"The Auditor-General has at all reasonable times full unrestricted access to any document, book or written or electronic record or information of the auditee or which reflects or may elucidate the business, financial results, financial position or performance of the auditee; any of the assets of or under the control of the auditee; or any staff member or representative of the auditee."*

Public Finance Management Act paragraph 38(1)(a)(i) and (iii) states that *"The accounting officer for a department must ensure that the department has and maintains effective, efficient and transparent systems of financial and risk management and internal control; and an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost effective;..."*

Public Finance Management Act paragraph 38 (1)(c)(ii) states that *"The accounting officer for a department must take effective and appropriate steps to prevent unauthorized, irregular and fruitless and wasteful expenditure and losses resulting from criminal conduct"*

Public Finance Management Act paragraph 40(a) and (b) states that *"The accounting officer for a department must keep full and proper records of the financial affairs of the department in accordance with any prescribed norms and standards; must prepare financial statements for each financial year in accordance with generally recognized accounting practice..."*

Treasury regulation 16A6.3 (d) states that *"awards are published in the Government Tender Bulletin and other media by which the bids were advertised."*

National Treasury Instruction No 1 of 2015/16 paragraph 4.1 and 4.2 states that *"The Accounting Officers of PFMA compliant institutions must through the relevant treasury publish the awards of all advertised competitive bids on the eTender Publication Portal by taking cognisance of the requirements in paragraph 4.2"*

PFMA compliant institutions must submit the following information on successful bids to the relevant treasury's eTender Publication Administrator within seven (7) working days of awarding the bids:

- a) Contract description and bid number*
- b) Names of the successful bidder(s) and preference points claimed*
- c) Contract price(s), if possible and*
- d) contract period"*

Nature

During the audit of supply chain management, it was noted that the following contracts were awarded through a tender process, however the awards for these tenders were not advertised in the Government Tender Bulletin and eTender Publication Portal as required Treasury regulation 16A6.3 and National Treasury Instruction No 1 of 2015/16.

No	Tender number	Project Description	Supplier Name	Award Contract Value	Payment to date
1	CPTSC01/19	CPT: Parliamentary Villages: Transportation of MPs & Sessional Officials	Springbok Atlas	9 969 620,00	0
2	CPTSC04/19	CPT: Maintenance & Conservation of Rhodes Collection at Groote Schuur House/ Museum	DK Conservators Pty Ltd	893 037,00	0
3	CPTSC06/19	CPT: Parliamentary Precinct: Infrastructure Requirement - Feb 2020 SONA	C-Squared Group	795 782,00	795 782,00
4	CPTSC05/19	CPT: Parliamentary Precinct: Internal Deep Cleaning - Feb 2020 SONA	Greystone Trading 389 t/a Pronto Kleen	660 331,00	660 331,00
5	CPTSC28/18	CPT: Parliamentary Precinct: Infrastructure Requirement - May 2019 SONA	C-Squared Consumer	330 000,00	330 000,00
Total					1 786 113,00

Impact of the finding

Non-compliance with the Preferential Procurement Regulation, 2017

Misstatement of irregular expenditure for the amount paid to date

Internal control deficiency

Leadership

Management did not exercise oversight responsibility regarding financial and performance reporting and compliance and related internal controls.

Financial and Performance Management

Reviewing and monitoring of compliance with applicable laws and regulations is insufficient and not properly monitored.

Recommendation

It is recommended that:

Management must develop or enhance compliance procedures to ensure compliance with all prescribed laws and regulations. In addition, such procedures include enhancement of compliance checklists already developed.

The accounting officer should investigate the reasons for the irregular expenditure and confirm if it was deliberate. The expenditure should be included in the irregular expenditure register.

Management response

Management is in agreement with the finding. It must be clarified that these tenders were advertised on the Tender Bulletin and the eTender Portal. However, the awards of these tender were only advertised on the Departmental website and this was due to budget constraints. We since started reviewed this process and awards are advertised as required. All the necessary SCM processes were adhered to therefor these transactions do not constitute Irregular Expenditure.

Name : D. Magida
Position: Assistant Director
Date: 18/03/2020

Auditor's response

Management comments are noted. After consideration of the alternate procedures done by the department to ensure that the these tenders were advertised, we have obtained sufficient appropriate evidence that the process followed was fair, equitable and transparent, and the finding with respect to irregular expenditure is resolved. However the finding remains and will be reported in the final management report as non-compliance with Treasury Regulation 16A6.3 and Treasury Instruction No.1 of 2015/16.

20. Quotations pre-qualifying criteria

Requirements

Public Finance Management Act paragraph 38(1)(a)(i) and (iii) states that *"The accounting officer for a department must ensure that the department has and maintains effective, efficient and transparent systems of financial and risk management and internal control; and an appropriate procurement and provisioning system which is fair, equitable, transparent, competitive and cost effective;..."*

Public Finance Management Act paragraph 38 (1)(c)(ii) states that *"The accounting officer for a department must take effective and appropriate steps to prevent unauthorized, irregular and fruitless and wasteful expenditure and losses resulting from criminal conduct"*

Treasury regulation 16A6.4 states that *"If in a specific case it is impractical to invite competitive bids, the accounting officer may procure the required goods or services by other means, provided that the reasons for deviating from inviting competitive bids must be recorded and approved by the accounting officer."*

In terms of Preferential Procurement Regulation 2017 paragraph 4 (2) states that: *"A tender that fails to meet any pre-qualifying criteria stipulated in the tender document is an unacceptable tender."*

Practice Note 3 of 2016/17 paragraph 8.1, 8.2 and 8.4 states that *"The Accounting Officer must only deviate from inviting competitive bids in cases of emergency and sole supplier status; An emergency procurement may occur when there is a serious and unexpected situation that poses an immediate risk to health, life, property or environment which calls an agency to action and there is insufficient time to invite competitive bids and the Accounting officer must invite as many suppliers as possible and select the preferred supplier using the competitive bid committee system."*

Nature

An internal memorandum was approved by the acting Regional Manager to deviate from inviting suppliers on Central Supplier Database (CSD) as there is no commodity on the CSD for this service due to having a limited number of suppliers with the required security clearance certificate to be providing this service. A nominated procedure was then followed to identify seven (7) suppliers whom the department has previously worked with for providing speed crowd security fence and are security cleared.

Notice and Invitation for Quotation; PA-03 (GS) was sent to the nominated suppliers with a pre-qualifying criteria of level 1 B-BBEE status level of contributor. In performing the audit procedures, it was found that the winning supplier Pantsula CC was a level 2 B-BBEE contributor, which should have not been evaluated further as they did not meet the pre-qualifying criteria.

RFQ #	Commodity / Short Description	Supplier	BBBEE LEVEL	Amount
7884	Prestige: SONA 2020: S&D speed fencing	Pantsula CC	Level 2	361 806,00

Impact of the finding

Non-compliance with the Preferential Procurement Regulation, 2017

Misstatement of irregular expenditure for the amount paid to date of R 361 806.00

Internal control deficiency

Leadership

Management did not exercise oversight responsibility regarding financial and performance reporting and compliance and related internal controls.

Financial and Performance Management

Reviewing and monitoring of compliance with applicable laws and regulations is insufficient and not properly monitored.

Recommendation

It is recommended that management must develop or enhance compliance procedures to ensure compliance with all prescribed laws and regulations. In addition, such procedures include enhancement of compliance checklists already developed.

The accounting officer should investigate the reasons for the irregular expenditure and confirm if it was deliberate. The expenditure should be included in the irregular expenditure register.

Management response

Management is not in agreement with the finding as the nominated procedure for procurement was followed, where the issue of Pre-Qualification criteria is not applicable. In this case the standard PA-03(GS) form was used which is a standard form for invitation of quotations, all prospective bidders were invited and evaluated accordingly, without any prejudice.

Name: Karen Blaine
Position: Assistant Director
Date: 23/03/2020

Auditors conclusion

Managements comments are noted, however in inviting prospective bidders PA-03 Notice and Invitation for Quotation stated that a pre-qualifying criteria would be applicable. Furthermore, there is no evidence that the DPWI had attempted to notify prospective bidders that the pre-qualifying criteria appearing on the invite was not applicable.

Furthermore, the quotations were evaluated using PPR 2017 as outlined in the PA-03. Price and BBBEE certificates or sworn affidavit was used and this further indicates that management initial intention were to use PPR 2017 guidelines thus even pre-qualifying criteria was applicable on the PA-03. Therefore, the finding remains and will be reported in the final management report.

ANNEXURE C: ADMINISTRATIVE MATTERS

Compensation of employees

21. 2019/20 HR Plan

Requirements

Section 7 (3)(b) of the Public Service Act (PSA) requires that *“A head of department shall be responsible for the efficient management and administration of his or her department, including the effective utilisation and training of staff, the maintenance of discipline, the promotion of sound labour relations and the proper use and care of State property, and he or she shall perform the functions that may be prescribed.”*

Section 25 (2)(d) of the Public Service Regulations, 2016 (PSR) requires that *“Based on the strategic plan of the department, an executive authority shall engage in human resource planning in accordance with regulation 26 to meet the resulting human resource needs.”*

Section 26 (1) of the PSR requires that *“An executive authority shall prepare and implement a human resource plan for his or her department.”*

Nature

The previous approved departmental Human Resource (HR) Plan was for the MTEF period 2016-2019, hence a new HR plan needed to be approved for the 2019/20 financial year.

The 2019/20 HR Plan was requested per Request for Information no. 3 dated 5 December 2019 and Communication of Finding 1 dated 7 February 2020 and could not be submitted as it was not finalised, approved and implemented for the 2019/20 financial year.

The department indicated on their response that it will only be approved by 31 March 2020 after the finalization of the development of the 5 year strategic plan of the Department, the National Macro Organization of Government as part of the sixth administration and the reorganization of the Department.

No exemption was requested or obtained from National Treasury or the Department of Public Service and Administration for not complying with the PSA and PSR.

Impact

This results in non-compliance with PSA 7(3)(b); PSR 25(2)(d) and 26(1).

Internal control deficiency

Financial and performance management:

Review and monitor compliance with applicable laws and regulations

Management did not review and monitor compliance with applicable laws and regulations, as a result the 2019/20 HR Plan is not timeously finalised, approved and implemented for the 2019/20 financial year.

Recommendation

It is recommended that:

Management must develop or enhance compliance procedures to ensure compliance with all prescribed laws and regulations. In addition, timeously requesting exemption from the relevant authority for not complying with any laws and regulations when circumstances are outside of their control.

Management response:

Management is partly not in agreement with the finding.

The Department has an approved HR plan for period 2019-2022 which was submitted to the Auditor General of South Africa (A copy of the HR plan is attached hereto). The Department notes and is in agreement that the HR Plan was only approved 03 March 2019. The coming in of the sixth administration in May 2019, after the national elections, resulted in the reconfiguration of Ministries and Departments referred to as National Macro Organization of Government. The finalization of National Macro Organization of Government was considered very critical to HR plan as it was to provide information on the newly reconfigured Department of Public Works and Infrastructure in relation to added Infrastructure function hence the delays in the finalization of related plans. The NMOG processes were scheduled for completion by 31 December 2019. The DPSA was accordingly informed of the delay and reasons thereof. However it should be mentioned that the Annual HR plan implementation report for the 2019/20 financial year is only due for submission at the DPSA on 30 June 2020. During June 2019, the department submitted the Annual HR implementation report for the 2018/19 financial year.

Name: TB Hlatshwayo
Position: CD: HRM
Date: 11/05/2020

Auditor's conclusion

Management comment noted and that the finalization of National Macro Organization of Government for the newly reconfigured Department of Public Works and Infrastructure delayed the finalisation of related plans.

However no exemption was obtained or received and the HR plan for 2019 to 2022 was only signed by the DG on the 9 March 2020 which resulted in the 2019/20 HR Plan not being timeously finalised, approved and implemented for the 2019/20 financial year therefore this matter will be reported in the management report as an administrative matter.

FINDINGS RELATING TO THE INFORMATION SYSTEMS AUDIT

1. INFORMATION TECHNOLOGY GOVERNANCE

1.1 Vacant positions within information and communication (ICT) division

Management should establish Information and ICT organisational structure that reflects business needs. In addition, put a process in place for periodically reviewing the ICT organisational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances.

Audit Finding

As previously reported, it was noted that there was an established and approved ICT department organisational structure in 2016. However, the following listed positions were still vacant:

- Chief Information Officer (CIO)
- Deputy Project Manager (ICT)

Risk

The inadequate staffing of the ICT division may result in inefficient service delivery and lack of segregation of duties within the ICT function which might lead to integrity of data being compromised.

Internal control deficiency

Leadership: Information technology governance framework

Moratorium placed on recruitment processes by the Department of Public Service and Administration (DPSA) in order to revise the organisational structure.

The new Minister requested a re-evaluation of the organisational structure to be align to the new mandate of DPWI.

Recommendation

It is noted that Human Resource Management is a function managed outside of ICT however, the Chief Information Officer should ensure that there is a process in place for periodically reviewing the ICT organisational structure to adjust staffing requirements and sourcing strategies to meet expected objectives of the department and changing circumstances.

The impact of vacant key positions on service continuity should be a matter regularly tabled at established governance structures.

Management response

Management comment on audit finding:

The DPW organisational structure was approved in 2016. The approved organisational structure proposed additional positions for ICT. The implementation of the newly approved

organisational structure had to be done within the allocated budget ceilings. As a result, and after a thorough prioritisation process not all positions as approved in the organisational structure were activated in the PERSAL post establishment. All the positions identified with the exception of Chief Information Officer and Deputy Project Manager are not funded and therefore not activated for filling on the post establishment. The other positions were contracted through service providers as consultants.		
Management comment on internal control deficiencies: In terms Management Agrees		
Management comment on recommendation: Management Agrees. In this regards ICT completed its structure review and engaged HR to fill the proposed vacant posts which were regarded as priority		
Remedial action:		
What actions will be taken: ICT Structure review	By whom: Bheki Zwane Position: Act: CIO	By when: 30 April 2020
Memo to HR for the filling of posts	Bheki Zwane	31 May 2020
Advertising and filling of CIO and Deputy Project Manager	Bheki Zwane	25 February 2021

Auditor's conclusion

Management comments are noted and corrective actions will be evaluated in next audit cycle.

1.2 Inadequate planning and management processes around Archibus ERP system

A project management framework should be in place to ensure that the scope defined and boundaries of managing projects, as well as the method to be adopted and applied to each project undertaken follow a consistent approach.

Audit finding

During the audit, we noted that the department was in the process of implementing its Enterprise Resource Planning (ERP) system (Archibus-Sage) which was meant to manage the operational aspects of asset management and to provide a platform on which financial transactions take place.

The project was conceptualised or considered in August 2015. The duration on the initial project plan was to be completed within 10 months, starting in 01 August 2015 to 30 May 2016. Our analysis of the 2019/20 payment schedules indicated that different service providers were paid from 01 August 2015 to date a total amount of R36 203 008. However, the following weaknesses were noted:

- A draft business case supporting the ERP system (Archibus-Sage) project was provided.
- The project was running behind schedule, as result the status indicated that only three (3) out of eight (8) planned modules had gone live.

Risk

A business case articulates the business problem requirement or needs being addressed by implementing the system. The lack of a formally documented business case may result in scope creep and a non-value adding investment that does not meet business needs nor yields efficiency improvements resulting in wasteful expenditure. Furthermore, the delay in finalizing the project may attract more costs and the solutions or modules being introduced may longer be relevant or may fail to support business needs due the time lag it takes to implement the full project.

Internal control deficiency

Leadership: Information technology framework

The Lack of consequences for poor management of ICT contracts and service level agreements (SLAs). This attributed to the timing it took to implement the project due to the department changing service providers.

Recommendation

Management should ensure that the draft business case supporting the ERP system project is approved by the relevant approval structures to ensure that it supports and is aligned to the business plan.

Management should consider monitoring of the project costs centrally in order to track spending overall and ensure that overruns are mitigated.

Management should continue to monitor all the critical success factors and risks identified ensuring that resolutions are prioritised. This will ensure the project is managed successful and that deliverables are achieved within planned timeliness and budget.

Management response

Management comment on audit finding: Management agrees with the finding. A draft business case was developed for the ERP system. The business case is being reviewed given the current status and will be submitted for approval.		
Management comment on internal control deficiencies: Management notes the control deficiency.		
Management comment on recommendation: Management notes the recommendation.		
Remedial action: Review and submit business case for approval.		
What actions will be taken: Review and submit business case for approval.	By whom: Bheki Zwane Position: Act: CIO	By when: September 2020

Auditor's conclusion

Management comments are noted and corrective actions will be evaluated in next audit cycle.

1.3 Information Communication Technology projects for 2019/20 were not achieved

Audit finding

During the audit it was established that Department of Public Works Infrastructure (DPWI) had developed and approved the 2019/20 Annual Performance Plan which detailed the “key performance indicators (KPIs)” to be implemented. However, the following ICT projects were not achieved:

Project Title	Budget	Target achieved (Yes/No)	Stage/Process
1. Backup and Recovery	R30m	No	Procurement
2. Laptop Tracking	R10m	No	Procurement
3. EPWP reporting system SLA	R2m	No	Procurement
4. Technical support and WCS & PMIS support	R45m	No	Procurement
5. ESRI GIS licensing	R8m	No	Procurement
6. Enterprise security solution	R30m	No	Initiating

Failure to achieve set ICT goals may hinder the progress in implementation of the APP and ICT may fall short in aligning to the organisational strategy.

Internal control deficiency

Leadership: Information technology governance framework

ICT did not meet set targets due to the following:

Dependencies on other parties which were not initially taken into account when committing to the KPIs.

Delays in procurement by the department.

Recommendation

The Acting Chief Information Officer should ensure that:

All KPIs are developed with an understanding of dependencies on other parties to ensure set target are realistic in order to be achieved

He continues to monitor implementation of all KPIs on a monthly basis and reasons or root causes for failure to implement should be clearly documented

Management response

Management comment on audit findings:
Management comment on internal control deficiencies:
Management comment on recommendations:

Remedial actions:		
What actions will be taken:	• By whom:	• By when:

Auditor's conclusions

DRAFT

1.4 Corporate Governance of Information and Communications Technology Policy & Charter (CGICT) outdated

Audit Finding

The Corporate Governance of Information and Communications Technology Policy & Charter (CGICT) was drafted and approved in July 2014. Review of the Charter was not conducted during the period under review.

Inadequate or irregular review of CGICT may result in business not able to understand and manage all significant ICT risks and ICT enabled business projects to ensure ICT value, improve service delivery and the achievement of business objectives.

Internal control deficiency

Leadership: IT Governance

Root cause to be provided by auditee

Recommendation

The acting Chief Information Officer should ensure that the CGICT is reviewed to ensure that it is relevant to the organization's environment and approved by the relevant business structures to ensure compliance with the adopted business wide framework.

The established structures as per the charter should operate as stipulated on the charter.

Management response

Management comment on audit findings:		
Management comment on internal control deficiencies:		
Management comment on recommendations:		
Remedial actions:		
What actions will be taken:	By whom:	By when:

Auditor's conclusions

2. USER ACCESS MANAGEMENT

2.1 Inadequately implementation of user access management controls around Windows Active Directory (AD)

A sound and formally approved user access management policy ensures that users have rules and procedures to follow in order to minimise the risk of errors, fraud and the loss of confidentiality, integrity and availability of data.

Audit Finding

The Consolidated Information and Communication Technology Policy included user access management and it was noted that the policy does not explicitly indicate the systems and/or applications that are covered by the policy.

Furthermore, as previously reported in 2018/19 it was noted that the current policy was still in draft and does not provide adequate guidance on the process to follow when performing the below user access management activities:

- User account termination
- User transfer requests
- Monitoring of system controller actions on application security level (creation of IDs, user ID maintenance, allocating functions to users etc.)
- Periodic reviews of access and logon violation

The controls for monitoring and reviewing of system administrator activities was implemented and performed, however the control was not adequately performed as the review reports did not detail administrator activities performed such as user creation, user ID maintenance, allocation of functions and deletion of user accounts.

System generated list of users who requested password resets during the period was not provided, consequently we were unable to assess whether the control around password resets was effectively implemented.

As previously reported on 2017-18 and 2018-19, the following system accounts exist and were not assigned to any specific user furthermore Administrator account was not renamed:

- SQL2016Admin
- SQLADMIN
- SVC-Autodesk
- SVC_SageRT
- SASAdmin
- MomService
- Maps
- Faxadmin
- Administrator

Risk

Without an adequately designed user account management procedure, there will be inconsistencies in processes followed for termination, monitoring of system controller actions and access and logon violation.

Inadequate reviews of system controller activities might result in unauthorised system activities such as creating of unauthorised user accounts, deleting or modifying information and unauthorised attempts to access the system may not be timely detected and resolved.

Inadequate controls around the resetting of user passwords might result in unauthorised users being granted access to the system.

If user accounts are not linked to a specific user, it would make impossible to apportion accountability in the event when unauthorised or fraudulent transactions are processed. These could negatively impact data integrity of information systems.

Internal control deficiency

Financial and performance management: Formal controls over IT Systems

Lack of consequence management for not resolving prior audit finding.

Recommendation

Management should:

Ensure that the Consolidated Information and Communication Technology Policy is reviewed and approved to include all processes related to user access management.

Regular review and monitoring of audit trails which details activities of privileged users / administrators on the system should be duly conducted and signed off by management as evidence of review.

All password resets should be logged/recorded and authorized prior to system administrator resetting the user's password on the systems and evidence thereof should be retained for audit purposes

That they review the list of user-ids on the AD to ensure that each user-id is linked to a specific user and that key system accounts are renamed so that they remain protected.

Management response

Management comment on audit finding: Management agrees.		
Management comment on internal control deficiencies: On policy review all systems will be indicated. The user access management activities will also be amended accordingly. The accounts specified have been linked to users and PoE is attached.		
Management comment on recommendation: It's noted that recommendations were made before policy approval and they will be considered when review takes place.		
Remedial action: All identified deficiencies will be attended as per action plan below.		
What actions will be taken: Update the procedure in line with the process.	By whom: Pakiso Mphuthi Position: Security Manager	By when: 31 October 2020

Auditor's conclusion

Management comments are noted and corrective actions will be evaluated in next audit cycle.

DRAFT

2.2 Inadequately implementation of user access management controls around EPWP

User access controls ensures that only valid and authorized users are allowed access to initiate and approve transactions on the system and that user access is adequately segregated when transactions are captured and approved.

Audit finding

The following deficiencies were noted with regards to the administration of user access controls on the EPWP system:

Evidence of review performed to monitor user's access rights was not adequate as it did not entail users access furthermore there was no evidence indicating that the report/list was reviewed to ensure that the functions allocated to the users commensurate with their job responsibilities.

Evidence of review performed to monitor activities performed system was not adequate as the audit logs did not detail activities performed by system controller such as user creation, user ID maintenance, allocation of functions, password resetting and termination of user accounts, furthermore there was no evidence indicating the logs were reviewed.

System was configured to log failed logon attempts however there was no evidence indicating that the logs were analysed and reviewed on an interval basis and malicious trends or activities such as brute force attack are followed up.

Due to lack of system generated list indicating when user access was modified on the EPWP application system, testing could not be performed to determine if controls in place had been adequately implemented.

Risk

Failure to perform user access reviews might result in employees being granted excessive rights that would allow them to perform inappropriate activities on the applications such as fraud.

Inadequate reviews of system controller activities might result in unauthorised system activities such as creating of unauthorised user accounts, deleting or modifying information and unauthorised attempts to access the system may not be timely detected and resolved.

Without monitoring of access and logon violations, it may be difficult to assess the effectiveness of the security controls. Attempts to breach security may remain undetected, enabling knowledge of security loopholes to be exploited for malicious purposes.

Failure to ensure that adequate audit logs are designed and implemented for user account access amendments on the system could result in unauthorized access modification going undetected. This might lead to unauthorized access to systems which could potentially compromise data integrity.

Internal control deficiency

Financial and performance management: Formal controls over IT Systems

Management did not in all instances implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support Information Systems Audit reporting

Reviews were not performed due to system limitation on EPWP version 1, and new version will be implemented during EPWP Phase 4 in 2020/21 financial year to address the audit findings

Failure by management in ensuring that application systems in use is configured to log user account access amendments on the system.

Recommendation

Management should:

Ensure that an individual is identified and allocated the roles to facilitate information systems audit request. This resource will be able to direct the RFIs to the relevant officials, track turnaround time, verify the evidence submitted and ensure that management comments are submitted at the correct level.

Communicate their minimum security requirements on new version to record user's access rights and actions performed by the system controller, furthermore reviews should have been performed and signed off as evidence of review.

Consider updating the systems to include information on changes to user access rights. Alternatively, administrator logs should be made available.

Management response

Management comment on audit findings: Management agrees with the finding. User role modifications are currently managed outside the system. Upon receipt of such request, approval is granted after verification and confirmations had been made. EPWP has considered implementing a system generated log that will track modifications made in granting user role changes.		
Management comment on internal control deficiencies: The feature could not be implemented due to the lack of a contract in the previous financial year.		
Management comment on recommendations: The system will be updated to include information on changes to user access rights. Alternatively administrator logs will be made available.		
Remedial actions: The log will be implemented by the end of August.		
What actions will be taken: The log will be implemented by the end of August 2020.	By whom: Ms T Maluleke (DD: Data Management) Ms Carmen-Joy Abrahams (Acting DDG: EPWP)	By when: August 2020 27 July 2020

Auditor's conclusions

Management responses are noted; however, the corrective actions agreed upon by management will be followed-up in the next audit cycle.

2.3 Inadequately implementation of user access management controls around Reapatala

A sound and formally approved user access management policy ensures that users have rules and procedures to follow in order to minimise the risk of errors, fraud and the loss of confidentiality, integrity and availability of data.

Audit finding

The following deficiencies were noted with regards to the administration of user access controls on the Reapatala system:

Although the policy on user access management is included in the Consolidated Information and Communication Technology Policy, it was noted that the policy does not explicitly indicate the systems and/or applications that are covered by the policy. Furthermore, as previously reported it was noted that the current policy was still in draft and does not provide adequate guidance on the process to follow when performing the following user access management activities:

- User account termination.
- User transfer requests.
- Monitoring of system controller actions on application security level (creation of IDs, user ID maintenance, allocating functions to users etc.)
- Periodic reviews of access and logon violation

Testing of change of existing access/access modification on Reapatala could not be assessed as, a system generated list of all user access modification performed during the period under review was not provided for audit purpose.

System generated list of users who requested password resets during the period was not provided, consequently we were unable to assess whether the control around password resets was effectively implemented.

Evidence of review performed on user access rights to ensure that they are in line with user's job responsibilities was no provided for audit purpose.

Although the control for monitoring and reviewing of activities performed by the system administrators was implemented and performed under the audit review period, however the control was not adequately performed as the review report did not include admin activities performed on the system such creation of IDs, user ID maintenance, allocating functions to users, removal on user ID etc.

There was no process to monitor and review logon and access violation, due to system limitation

Users who had their employment terminated by HR were still active on the system. The details of the accounts are listed in the table below:

Name	username	Resigned date	Last logon date
Kidwell	Kidwell.Mokadi@dpw.gov.za	20191231	08/18/2017 13:47:55
mcebisi	mcebisi.hawu@dpw.gov.za	20191231	11/18/2019 14:24:52
phindile	phindile.khoza@dpw.gov.za	20191115	06/10/2019 14:00:38
Fellen	Fellen.Makwetsa@dpw.gov.za	20191231	05/15/2018 10:32:07
buyisile	buyisile.shabalala@dpw.gov.za	20191231	09/13/2017 12:28:44
liboetso	liboetso.mothelesi@dpw.gov.za	20191231	01/14/2020 14:43:48
siboniso	siboniso.miya@dpw.gov.za	20191231	12/23/2019 12:18:43
sarah	sarah.mabuela@dpw.gov.za	20191231	12/03/2019 09:54:50
Mahlogonolo	Mahlogonolo.Makwela@dpw.gov.za	20191231	09/17/2019 12:07:01
Xola	Xola.Bokoloshe@dpw.gov.za	20191231	11/08/2017 11:02:07
lydia	lydia.mwelase@dpw.gov.za	20191231	11/06/2019 10:05:39
Charmaine	Charmaine.Kok@dpw.gov.za	20190531	02/18/2019 10:42:53
Emmanuel	Emmanuel.Jiyane@dpw.gov.za	20191231	10/02/2018 10:53:59
tebogo	tebogo.legoabe@dpw.gov.za	20191231	12/19/2019 11:52:16
shirly	Shirly.Kgampe@dpw.gov.za	20191231	11/13/2019 07:41:28
Lerroy	Lerroy.Fenyane@dpw.gov.za	20191231	10/30/2018 11:19:45
Bakhaliphicebo	Bakhaliphicebo.Nakedi@dpw.gov.za	20191231	11/08/2019 10:41:10
Thokoza ni	Thokoza ni.Zulu@dpw.gov.za	20190731	08/27/2019 14:04:06

Risk

Without an adequately designed user account management procedure, there will be inconsistencies in processes followed for termination, monitoring of system controller actions and access and logon violation.

If functions granted to a specific user are not recorded and authorised, this can result in users having access rights which are in excess of what is required to perform their job responsibilities. This increases the chances of fraud being committed or unauthorised amendments being made.

Inadequate controls around the resetting of user passwords might result in unauthorised users being granted access to the system

Failure to perform user access reviews might result in employees being granted excessive rights that would allow them to perform inappropriate activities on the applications such as fraud.

Inadequate reviews of system controller activities might result in unauthorised system activities such as creating of unauthorised user accounts, deleting or modifying information and unauthorised attempts to access the system may not be timely detected and resolved.

Without monitoring of access and logon violations, it may be difficult to assess the effectiveness of the security controls. Attempts to breach security may remain undetected, enabling knowledge of security loopholes to be exploited for malicious purposes.

If accounts of users who left the department are not terminated in a timely manner on the network; such accounts may be used by perpetrators to gain access to the system and process illegal/unauthorised activities.

Internal control deficiency

Financial and performance management: Control over IT Systems

Management did not in all instances implement proper record keeping in a timely manner to ensure that complete, relevant and accurate information is accessible and available to support Information Systems Audit reporting

System limitation, there is no functionality for logging failed login attempts on Reapatala.

HR/user's supervisors did not timely communicate users who had left the department to the system controllers.

Recommendation

Management should ensure that an individual is identified and allocated the roles to facilitate information systems audit request. This resource will be able to direct the RFIs to the relevant officials, tract turnaround time, verify the evidence submitted and ensure that management comments are submitted at the correct level.

Regular review and monitoring of audit trails which details activities of privileged users / administrators on the system should be duly conducted and signed off by management as evidence of review.

Management should communicate their minimum security requirements to record access and logon violations on the system to the service provider and verifications should be performed by ICT to ensure that the controls on the system allows for /is conducive to the effective implementation of logging access and logon violations.

HR/user's supervisor's should communicate in time of any users who leave the department to ensure that the access controls that were put in place to safe guard the department are working as intended to.

Management response

Management comment on the audit finding: Management does not agree.		
Management comment on internal control deficiencies: <ul style="list-style-type: none"> All requests for profile/ access change are processed, administered and managed by business. The system cannot currently provide requested report. Reapatala authenticates through AD and as such all requests for password reset are done at AD and not on Reapatala. Reapatala only manages the user profile and not the user account. Reapatala provides a report on the system which is accessible by all line managers to make it easy to download the report, review users under their supervision and submit to ICT for change of profile where necessary. In terms of termination of employment, that termination of account will be managed through AD. Currently Reapatala does not log what the administrators do but only what functions they access on the system. The system does not currently log logon violations thus the requested information could not be provided. To avoid duplication of efforts, termination of user account is managed at AD level. This is done to maintain a single point of entry in terms of authentication on Reapatala. If a user is terminated then the account will then be terminated at AD thus also voiding the user's ability to logon to Reapatala. 		
Management comment on recommendation: <ul style="list-style-type: none"> Officials from Finance, Khutso Lefutla, Relebohile Ramphekwa and Lapologang Koikanyang are the select system controllers to assist as indicated. HR and Line function must communicate timeously to ICT so that we can act faster in deactivating user accounts of officials whose employment has been terminated as this is next to impossible for ICT to manage this process. 		
Remedial action:		
What actions will be taken:	By whom:	By when:
Management to provide more add on ability to enable review of admin activities such as such creation of IDs, user ID maintenance, allocating functions to users, removal on user ID.	Khathu Nekhumbe	31 December 2020
Add process to monitor and review logon and access violation	Khathu Nekhumbe	31 March 2021
Review User Policy to specify line function responsibility in terms of user access review	Pakiso Mphuthi	31 March 2021

Auditor's conclusion

We wish to confirm that management did not provide the auditors with audit evidence to confirm that the reviews of user access rights were performed for the current period of audit, thus the finding remains.

Management response regarding implementing process of review of admin activities, logon and access violation and review of the policy was noted, the corrective actions agreed upon by management will be followed-up in the next audit cycle.

2.4 Lack of adequately designed PERSAL user access management policy

A sound and formally approved user access management policy ensures that users have rules and procedures to follow in order to minimise the risk of errors, fraud and the loss of confidentiality, integrity and availability of data.

Audit finding

Although PERSAL User Account Management procedure was developed, however it was noted that the procedure was still in draft.

Risk

Without an approved user account management procedure, there will be inconsistencies in processes followed for monitoring of system controller actions, user account administration, access rights as well as access and logon violations. This weakness could compromise the integrity of data and ultimately financial statements. Furthermore, failure to perform user reviews might result in employees being granted excessive rights that would allow them to perform inappropriate activities on the applications such as fraud being committed on the systems.

Internal control deficiency

Financial and performance management: Control over IT Systems

Management to provide Internal control deficiency

Recommendation

Management should priorities the process of approving PERSAL User Account Management procedure

Management response

Management comment on the audit finding:

I do not agree with the finding. PERSAL is a transverse system and is maintained by National Treasury through SITA. The functions and responsibilities of the PERSAL Controller as well as the Personnel Controller and the Salary Controller is prescribed. When a new function is created by SITA on the PERSAL System the function is automatically given to the PERSAL Controller. The PERSAL Controller must then assign it to the Personnel or the Salary Controller or both depending on whether HR or Finance will use the function. The User Account Management Guide in use is aligned to the functions and protocols as required by PERSAL. Each Controller also has a work plan that underpins the key responsibilities of the position they occupy. Controllers are evaluated every 6 months in line with PMDS. The Personnel Controller and the Salary Controller is assessed by the PERSAL Controller and the PERSAL Controller by the Director: Human Resource Administration. Attached is copy of the draft document to replace the current PERSAL User Account Management Policy.

The User Profiles are updated on an annual basis and this ensures that employees access commensurate with their job responsibilities. On an annual basis the PERSAL Controller forwards to all the PERSAL Users a request for confirmation of Users Functions aligned to the functions they perform. Attached is the example of the request that was forwarded 1 April 2019. Any User who did not comply with the deadline is not allowed access until a request signed by the Supervisor is forwarded to confirm that User must have access to the system and they did not comply with the due date. Attached is also the latest request that was circulated for 2020.

The PERSAL System was updated to include a screen with an indemnity clause in terms of confidentiality of information on the system as well as access details that each user must confirm every time the user signs on the system.

PERSAL Users have two IDs on the system when signing on the first ID is the Complete User ID (means the ID allocated to a User, in order to log on to the mainframe which houses PERSAL) if captured correctly the User must then access the second screen through the PERSAL User ID (means the ID allocated to a User, to log on to the PERSAL System). Each User ID requires a password to be captured before access is granted. The system requires automatically that the User change their password every month.

If the User is revoked on the first ID, the Complete User ID he/she completes a reset form that is checked and signed by the Controller and forwarded to PERSAL User Support through the SITA Logic Centre to reset the password. If the User is revoked on the second ID the PERSAL User ID the Controller resets the User. Users who frequently revoke themselves are followed up by the Controller. If a User does not use the System in a month, he/she is automatically revoked on the System and must approach the Controller for access. Users that do not utilise the System in three months are not allowed to request for reset without explanation and recommendation of the Supervisor of the User.

Management comment on internal control deficiencies:

I do not agree with the finding. The User Profiles are updated on an annual basis and this ensures that employees access commensurate with their job responsibilities. On an annual basis the PERSAL Controller forwards to all the PERSAL Users a request for confirmation of Users Functions aligned to the functions they perform. Attached is the example of the request that was forwarded 1 April 2019. Any User who did not comply with the deadline is not allowed access until a request signed by the Supervisor is forwarded to confirm that User must have access to the system and they did not comply with the due date. Attached is also the latest request that was circulated for 2020.

Management comment on recommendation:

Management comment on the audit finding:

I do not agree with the finding. PERSAL is a transverse system and is maintained by National Treasury through SITA. The functions and responsibilities of the PERSAL Controller as well as the Personnel Controller and the Salary Controller is prescribed. When a new function is created by SITA on the PERSAL System the function is automatically given to the PERSAL Controller. The PERSAL Controller must then assign it to the Personnel or the Salary Controller or both depending on whether HR or Finance will use the function. The User

Account Management Guide in use is aligned to the functions and protocols as required by PERSAL. Each Controller also has a work plan that underpins the key responsibilities of the position they occupy. Controllers are evaluated every 6 months in line with PMDS. The Personnel Controller and the Salary Controller is assessed by the PERSAL Controller and the PERSAL Controller by the Director: Human Resource Administration. Attached is copy of the draft document to replace the current PERSAL User Account Management Policy.

The User Profiles are updated on an annual basis and this ensures that employees access commensurate with their job responsibilities. On an annual basis the PERSAL Controller forwards to all the PERSAL Users a request for confirmation of Users Functions aligned to the functions they perform. Attached is the example of the request that was forwarded 1 April 2019. Any User who did not comply with the deadline is not allowed access until a request signed by the Supervisor is forwarded to confirm that User must have access to the system and they did not comply with the due date. Attached is also the latest request that was circulated for 2020.

The PERSAL System was updated to include a screen with an indemnity clause in terms of confidentiality of information on the system as well as access details that each user must confirm every time the user signs on the system.

PERSAL Users have two IDs on the system when signing on the first ID is the Complete User ID (means the ID allocated to a User, in order to log on to the mainframe which houses PERSAL) if captured correctly the User must then access the second screen through the PERSAL User ID (means the ID allocated to a User, to log on to the PERSAL System). Each User ID requires a password to be captured before access is granted. The system requires automatically that the User change their password every month.

If the User is revoked on the first ID, the Complete User ID he/she completes a reset form that is checked and signed by the Controller and forwarded to PERSAL User Support through the SITA Logic Centre to reset the password. If the User is revoked on the second ID, the PERSAL User ID the Controller resets the User. Users who frequently revoke themselves are followed up by the Controller. If a User does not use the System in a month, he/she is automatically revoked on the System and must approach the Controller for access. Users that do not utilise the System in three months are not allowed to request for reset without explanation and recommendation of the Supervisor of the User.

Remedial action:

What actions will be taken:	By whom:	By when:
Draft User Account Management Guidelines must be submitted for signature	DD: PERSAL and Payroll	31 August 2020

Auditor's conclusion

Management responses are noted; however, the corrective actions agreed upon by management to submit Draft User Account Management Guidelines for signature/approval will be followed-up in the next audit cycle.

2.5 Inadequate implementation of user access management controls around PERSAL application

Audit finding

In the absence of a guiding PERSAL user access management policy, the following controls relating to the administration of user access on the PERSAL system were found to be inadequate:

There were no reviews of the logon and access violation performed for the current period of audit.

Evidence of review performed to monitor activities performed by the system controllers was not adequate as the review report include access allocated to system control and did not outline activities performed by the system controller such as user creation, user ID maintenance, allocation of functions and deletion of user accounts.

Evidence of password requests for the selected sample could not be provided to validate that there was formal request and authorisation prior to unlocking user's account of PERSAL. Refer to the table below:

No	Name and surname	Password reset date	LOGIK/SCC/REFERENCE
1	MOSTERT	20200125	RESET
2	BOOYSEN	20190502	RESET
3	PEFILE	20190711	RESET
4	LEKOKO	20191217	RESET
5	LETWABA	20191121	RESET
6	VAN NIEKERK	20191010	RESET
7	MATHEBULA	20190507	RESET
8	JANSE VAN RENSBURG	20200129	RESET
9	JOSEPH	20200121	RESET
10	MASUBELELE	20190516	RESET
11	MEELA	20190717	RESET

Risk

Without an adequately designed user account management procedure, there will be inconsistencies in processes followed for monitoring of system controller actions, user access rights and access and logon violations. This weakness could compromise the integrity of data and ultimately financial statements. Furthermore, failure to perform user reviews might result in employees being granted excessive rights that would allow them to perform inappropriate activities on the applications such as fraud being committed on the systems.

Without frequent monitoring of access and logon violation, it may be difficult to assess the effectiveness of the security controls. Attempts to breach security may remain undetected, enabling knowledge of security loopholes to be exploited for malicious purposes.

Lack of regular reviews of system controller activities might result in unauthorised system activities such as creating of unauthorised user accounts, deleting or modifying

information and unauthorised attempts to access the system may not be timely detected and resolved.

If functions granted to a specific user are not recorded and authorised, this can result in users having access rights which are in excess of what is required to perform their job responsibilities. This increases the chances of fraud being committed or unauthorised amendments being made.

Inadequate controls around the resetting of user passwords might result in unauthorised users being granted access to the system

Internal control deficiency

Financial and performance management: Control over IT Systems

Management oversight in determining the adequacy and level of detail required in the documentation of reviews performed

Management did not keep emails of password reset requests

Recommendation

Management should:

Regular review and monitoring of the automated audit trails which details activities of privileged users / administrators should be duly conducted and signed off by management as evidence of review.

Proper and accurate record keeping is done regularly

Management response

Management comment on the audit finding:

I do not agree with the finding

PERSAL Users have two IDs on the system when signing on the first ID is the Complete User ID (means the ID allocated to a User, in order to log on to the mainframe which houses PERSAL) if captured correctly the User must then access the second screen through the PERSAL User ID (means the Id allocated to a User, to log on to the PERSAL System). Each User ID requires a password to be captured before access is granted. The system requires automatically that the User change their password every month.

The procedure for the reset of the first screen requires the completing of PERSAL Reset Form and the second screen an e-mail only. The Controller will align the reset procedure to require a formal request on the PERSAL Reset Form for the second screen as well to ensure proper records.

Management comment on internal control deficiencies:

See attached communication form the DD: PERSAL and Payroll

Management comment on recommendation:

Please note that currently both the ASD Salary Controller and the ASD: Personnel Controller positions is vacant and although Ms Sibeko and Ms Manzini has been assisting

the majority of the User management in terms of resets have been dealt with by the Deputy Director: PERSAL and Payroll.

Remedial action:

What actions will be taken: Amend procedure in terms of the reset of PERSAL Users on the second screen that is reset by the PERSAL Controller	By whom: DD: PERSAL and Payroll	By when: 27 July 2020
---	---	---------------------------------

Auditor's conclusion

We wish to confirm that management did not provide the auditors with audit evidence to confirm that the reviews of logon and access violation were performed for the current period of audit, thus the finding remains.

We wish to confirm that management did not provide the auditors with audit evidence to confirm that review of system controller's activities was performed for the current period of audit, thus the finding remains.

Management responses indicating that password reset done for the 2nd screen are requested through email communication are noted; however, we wish to confirm that evidence of email communication by users requesting password resets were requested however no evidence of such was provided for audit purpose thus the finding remain.

Response:

We agree to the finding in terms of reset of passwords on the second screen and a process has been put in place in the User Account Management Protocols and Guidelines.

We do not agree with the audit conclusion; system controllers review is done by management same as with all users during the submission of annual review forms. AG did include on their sample the annual review forms of system controllers. Attach please find the reviews that were done for Ms Khumalo, Ms Manzini (who was acting ASD: Salary Controller in 2019) and Ms Sibeko who is assisting as Personnel Controller.

Auditor's conclusion

Policy

Persal User Account Management Protocol was approved after the audit review period on 31/07/2020, thus we will to confirm that the finding remains.

2.6 Inadequately designed user access management policies

Audit finding

The following design deficiencies were noted in relation to the policies governing processes in the organisation:

The User Access Management Policy states on page 9, section 9 that "This policy shall be reviewed at least once a year and amended as and when the need for changes arises". However, it was noted that the User Access Management Policy had not been signed off to indicate when it had been approved for implementation. Furthermore, it was noted that the policy did not outline the process for the review of violation/exception reports within the organisation.

The User Access Management Policy outlines the password configurations for the organisation on page 6, section 7.7. However, the following design and implementation deficiencies were not outlined in the policy:

- Password history; and
- Minimum password age.

The SAGE X3 User Administration Policy was approved on 6 June 2018 by the Director: IT Applications and it was noted that the policy does not outline a review cycle. Furthermore, it was noted that the policy does not outline the process for the review of log on violations.

The SAGE X3 User Administration Policy outlines on page 5, section 3.5 the minimum password configuration requirements for the application. However, it was noted that the policy did not outline the following password configurations:

- account lockout duration.

Risk

Failure to ensure that the User Account Management Policy has been adequately approved for implementation in the organisation may lead to the inability to enforce processes and procedures that have been outlined in the policy and may also result in the inability to hold individual accountable in the event of deviations from the policy. This may result also result in inconsistencies in the application of processes and procedures outlined in the policy, which may result in control deficiencies within the organisation.

Failure to ensure that strong passwords are configured on the application systems may result in unauthorised access being gained through brute force and other cyber security attacks, which may result in financial information being compromised, degrading its confidentiality, integrity and availability.

Failure to ensure that the SAGE X3 User Administration Policy is frequently updated may result in outdated processes and procedures being applied in the user access management of SAGE. This may compromise the security of sensitive data through unauthorised access, degrading its confidentiality, integrity and availability.

Failure to ensure that strong passwords are configured on application systems may lead to the unauthorised access of sensitive data, compromising its confidentiality, availability and integrity.

Internal control deficiency

Financial and performance management: IT systems

Lack of adherence to the User Access Management Policy in ensuring that the policy is reviewed on an annual basis and is aligned to the current IT environment.

Recommendation

ICT management should ensure that:

The User Access Management has been adequately approved and that it includes the process for the review of log on violations.

Strong passwords are configured on the application systems, and are driven by the prescripts of the User Access Management and SAGE X3 User Administration Policies. Furthermore, the User Access Management Policy should be updated to cater for the deficiencies reported.

The SAGE X3 User Administration Policy is updated to include a review cycle as well as the process for the review of log on violations.

Management response

Management comment on audit findings: The SAGE X3 User Management Policy is a supplement of the main ICT policy. All other items not specifically stated on this policy will be inherited from the main policy. On page 6 of the SAGE X3 policy, it is stated that users are not allowed to use any previous password therefore minimum password age is zero (0) and the password expires every 30 days.		
Management comment on internal control deficiencies:		
Management comment on recommendations:		
Remedial actions:		
What actions will be taken:	By whom:	By when:

Auditor's conclusions

Management responses are noted; however, the corrective actions agreed upon by management will be followed-up in the next audit cycle.

2.7 Inadequate implementation of user access controls on GIS

User access controls ensures that only valid and authorised users are allowed access to initiate and approve transactions on the system and that user access is adequately segregated when transactions are captured and approved.

Audit finding

The following deficiencies were noted with regards to the administration of user access controls on the GIS system:

The User Access Management Policy outlines the process to be followed for the amendment of user access on the application systems on page 6, section 7.2. However, it was noted that the user access amendment forms for amendments performed on GIS could not be obtained. Furthermore, the user profiles for the amended users could not be obtained.

The User Access Management Policy outlines the process for password resets on page 6, section 7.3. However, a system generated list of password resets could not be obtained.

The User Account Management Policy states on page 7, section 7.4 that "As soon as an employee leaves the department, all his/her system logons must be revoked." However, it was noted user SM Maluleke (Resigned 31 December 2019) was still active on GIS.

The User Access Management Policy states on page 8, section 7.6 that "The ISO will institute a review of all user access rights at least twice a year, which is designed to positively confirm all users." However, it was noted that the review of user access was not performed on GIS.

The User Access Management Policy states on page 8, section 7.7 that "The best practice for access management will institute a review of system administrator/controller activities at least four times a year, for any seriously suspicious behaviour or critical events must be assessed and acted on." Although it was noted that the review of user access for system administrators had been performed, the review of system administrator activities had not been performed.

The password configurations on GIS could not be obtained to determine whether the following configurations have been adequately set:

- Minimum password length;
- Maximum password age;
- Password complexity;
- Lockout threshold;
- Password history;
- Minimum password age; and
- Account lockout duration.

Risk

Failure to ensure that function amendments, user access terminations and password resets are approved prior to their creation on application systems may result in

unauthorised users being granted access to the application systems and the sensitive data stored on these systems, compromising its confidentiality, integrity and availability.

Failure to ensure that user access rights are regularly reviewed may lead to the inability to detect users that have inappropriate access rights, which may lead to the performance of functions that are not commensurate with those user's job functions, which may lead to unauthorised transactions compromising the integrity and availability of financial information.

Failure to ensure that system administrator activities are regularly reviewed may lead to the inability to detect fraudulent activities performed by system administrators, which may compromise the integrity of financial information.

Failure to ensure that strong passwords are configured on the application systems may result in unauthorised access being gained through brute force and other cyber security attacks, which may result in financial information being compromised, degrading its confidentiality, integrity and availability.

Internal control deficiency

Financial and performance management: IT systems

GIS and its related controls was initially implemented by business prior to being handed over to IT, which has resulted in the inability to tighten controls on the system.

Recommendation

ICT management should ensure that:

Application systems log amendments to user access, and that all user access amendments are approved and adequately documented prior to implementation.

IT management, in collaboration with HR, should ensure that terminated user's access is timeously revoked from application systems once those terminated users have left the employment of the organisation.

Application system logs password resets, password reset requests, system administrator activities and user access rights on the application systems are reviewed and adequately documented.

IT management should ensure that strong passwords are configured on the application systems, and are driven by the prescripts of the User Access Management Policy. Furthermore, the User Access Management Policy should be updated to cater for the deficiencies reported.

Management response

Management comment on audit findings: Management agrees
Management comment on internal control deficiencies:

<p>GIS is a system that was initiated and implemented by business and was only handed over to ICT once the implementation was completed hence ICT user management procedures were not implemented as part of the solution. Currently amendments requests are received from RIERS through emails or phone. Going forward ICT will standardize the process whereby users will submit a user amendment form.</p> <p>The GIS system does not log the password reset requests. This will be corrected as part of enhancement or development of a new system.</p> <p>ICT relies on line function to inform us when users leave the department so the user's account can be revoked on the system. In this case no information was received by ICT regarding Mr. Maluleke. Going forward ICT will issue reminders to line function of their responsibility to constantly review and inform ICT when officials leave the department or leave the unit</p> <p>The GIS system does not currently have the ability to log administrator activities. This will be corrected as part of enhancement or development of a new system.</p> <p>The password configuration is not line with the departmental policy. This will be corrected as part of enhancement or development of a new system.</p>		
Management comment on recommendations: Management agrees		
Remedial actions:		
What actions will be taken:	By whom:	By when:
Application systems log amendments to user access, and that all user access amendments are approved and adequately documented prior to implementation.	Khathu Nekhumbe	01 August 2020
Management to issue periodic communications to line managers on the following: User Access Review and Official resignations.	Khathu Nekhumbe	01 September 2020
Application system logs password resets, password reset requests, system administrator activities and user access rights on the application systems are reviewed and adequately documented.	Khathu Nekhumbe	01 April 2021
IT management to ensure that strong passwords are configured on the application systems, and are driven by the prescripts of the User Access Management Policy. Furthermore, the User Access Management Policy should be updated to cater for the deficiencies reported.	Khathu Nekhumbe	01 April 2021

Auditor's conclusions

Management responses are noted; however, the corrective actions agreed upon by management will be followed-up in the next audit cycle.

DRAFT

2.8 Inadequate implementation of user access management controls on SAGE

Audit finding

The following deficiencies were noted with regards to the administration of user access controls on the SAGE system:

The user access amendment form for Pheletso Sedibe had not been signed off by the system administrator. Furthermore, the profile of the user, indicating the user access amendments could not be obtained.

The SAGE X3 User Administration Policy states on page 5, section 3.5 that "In the case of resetting password requests, the users must submit the SAGE X3 form to the system controller." However, it was noted that the password reset forms for the following users could not be obtained:

Reset by	Admin user code	Date reset	Time reset	User code	Request
Thato Magolo	HO163	2020/01/17 11:22:28 AM	11:22	H106	New password
Thato Magolo	HO163	2019/10/07 03:05:44 PM	15:05	MMB22	New password
Thato Magolo	HO163	2019/11/27 12:32:34 PM	12:32	KMB20	New password
Asok Gudibandi	SYS9	2019/09/20 10:39:02 AM	10:39	HO185	New password
Asok Gudibandi	SYS9	2019/04/30 07:58:09 AM	07:58	PLK25	New password
Thathane Prudence	SYS19	2020/02/13 02:29:09 PM	14:29	UMT59	New password
Thathane Prudence	SYS19	2020/02/03 11:33:50 AM	11:33	HO189	New password
Mamabolo Kgaogelo Oarabile	Sys18	2020/01/24 09:54:46 AM	09:54	CPT34	New password
Makgate Dineo	SYS17	2020/02/05 11:25:57 AM	11:25	UMT52	New password
Josbeth Mogomotsi	SYS 3	2019/05/07 03:02:49 PM	15:02	UMT36	New password
Byrch Miemie	BM	2019/06/10 11:32:09 AM	11:32	H086	New password

The SAGE X3 User Administration Policy states on page 5, section 5.5 that "If a user resigns or is transferred to another section, the user should submit the SAGE X3 form to the System Controller to de-activate the User ID on SAGE X3 with immediate effect." However, it was noted that there were 5 terminated users that were still active on SAGE X3, moreover, it was further noted that 2 of the 5 terminated users had accessed the system after their termination date.

Name & Surname	User Code	Login / Persal Number	Last Login Date	RESIGNATION DATE
Van Jaarsveld Wynand	H088	27568938	2019/06 /28	20191122
Mpyana Mahlodi	JHB52	28818733	2019/10 /23	00000000
Mpungose Lindani Samakhuba	JHB53	28851773	2020/03 /13	20190731

Name & Surname	User Code	Login / Persal Number	Last Login Date	RESIGNATION DATE
Thokozani Mduduzi Zulu	JHB55	28860268	2019/08/29	20190731
Mpho Maladzhi	JHB54	28860292	2019/09/26	20190731

Furthermore, the password configuration received did not outline the following:

- Maximum password age;
- Lockout threshold;
- Password history;
- Minimum password age; and
- Account lockout duration

It was noted that there were 16 users that had more than one user account on SAGE X3, namely:

Name & Surname	User Code	Login / Persal Number
Galane Mmoroti Julius	PLK29	27958166
Galane Mmoroti Julius	PLK39	27819566
Jozela Babalwa Happiness	UMT12	27569837X
Jozela Babalwa Happiness	HO176	27569837
Khuzwayo Lucky	DBN46	27789977X
Khuzwayo Lucky	HO156	27789977
Legodi Katlego	PTA53	28294457
Legodi Katlego	H135	28294467
Mahlangu Sizakele	HO181	9506190263084XXX
Mahlangu Sizakele	PTA67	9506190263084X
Mdludlu Ayanda	PE32	28175816X
Mdludlu Ayanda	UMT53	...
Ndyolashe Nomzamo	H127	52038271
Ndyolashe Nomzamo	H143	52038170
Shibambu Tiyyiselani Marvin	PLK27	27819574X
Shibambu Tiyyiselani Marvin	HO155	27819574

Risk

Failure to ensure that user access amendments and password resets are adequately implemented, user access is timeously terminated and that strong passwords are configured on application systems may lead to the unauthorised access of sensitive data, compromising its confidentiality, availability and integrity.

Failure to ensure that each user is uniquely identifiable on the application systems may result in the inability to hold a user accountable for fraudulent transactions that may be performed, compromising financial information, and degrading its integrity.

Internal control deficiency

Financial and performance management: IT systems

Lack of adherence to the SAGE X3 User Management Policy in ensuring that user access management controls are adequately implemented.

Recommendation

IT management should ensure that:

User access amendments are approved prior to implementation on the application, password resets are approved and adequately documented, user access is timeously revoked for terminated users and that strong passwords are configured on application systems.

Each user has their own unique user ID and that users are not assigned more than one user account on the application.

Management response

<p>Management comment on audit findings: Management does not agree.</p>
<p>Management comment on internal control deficiencies:</p> <p>The SAGE X3 User Management Policy is a supplement of the main ICT policy. All other items not specifically stated on this policy will be inherited from the main policy. The system generated list of users whose password was reset was submitted to AGSA as part of RFI 84, however this was part of the system administrator activity review list. ICT will be extracted the same and resubmit to the AGSA team.</p> <p>In our assessment Mr. Wynand van Jaarsveld should have been removed as part of the February 2020 user access review as received from business also in February 2019. However due to an error the system transaction instruction was not committed on the system during the deactivation process, this has since been resolved. As SAGE uses a two factor authentication process for users to gain access to the system, the first being that a user through terminal services logins to the server using Active Directory credentials and then followed by the SAGE specific credentials which were the ones still to be deactivated. We are happy to report that there were no transactions record by the account belong to Mr. van Jaarsveld. However, it must be noted that in terms of the Johannesburg regional office officials, ICT after having sent out a report of all active users on the SAGE system to line management at the JHB region, no response was received which would have then served as an instruction to ICT to deactivate the four (4) SAGE system accounts from the JHB region.</p> <p>On page 6 of the SAGE X3 policy, it is stated that users are not allowed to use any previous password therefore minimum password age is zero (0) and the password expires every 30 days.</p> <p>There are no duplicated users on the system. Some of the records that seem to be duplicated as shown on the list by AGSA are actually archived/deactivated records as the list provided by ICT included inactive accounts. ICT has separated active and inactive users and provided a report with two sheets showing the two categories of users.</p>
<p>Management comment on recommendations:</p> <p>User password reset logs are captured as part of the logged activities performed by System administrators. Users are terminated whenever a termination form is received from users. User access review is performed periodically through the user review process and this is mainly dependent on the responses received from line</p>

managers. SAGE X3 password is very strong, it forces for comply to uppercase, lower case, numerals and special characters and minimum 8 characters as per the policy on item 3.5 of the policy. Users are only assigned one user id on SAGE X3		
Remedial actions:		
What actions will be taken: Merge SAGE X3 user management policy with the ICT User Management Policy to ensure one policy for user management	What actions will be taken: Merge SAGE X3 user management policy with the ICT User Management Policy to ensure one policy for user management	What actions will be taken: Merge SAGE X3 user management policy with the ICT User Management Policy to ensure one policy for user management

Auditor's conclusions

Management responses are noted; however, the corrective actions agreed upon by management will be followed-up in the next audit cycle.

Management comments for the following findings have been received, but do not align to the findings that were raised:

The user access form for Pheletso Sedibe had not been signed off. Furthermore, the user profile for Pheletso Sedibe could not be obtained.

Password reset forms for the sampled users could not be obtained.

Inadequate password configurations on SAGE.

Duplicate users (Following assessment of the supplementary evidence provided, it was noted that there were still duplicate users on the system)

2.9 Inadequate implementation of user access management controls on PMIS

Audit finding

The following deficiencies were noted with regards to the administration of user access controls on the PMIS system:

The User Access Management Policy outlines the process to be followed for the amendment of user access on the application systems on page 6, section 7.2. However, a system generated list of user amendments could not be obtained.

The User Access Management Policy outlines the process for password resets on page 6, section 7.3. However, password reset forms for the following users could not be obtained:

Name	Surname	Password reset date
Martha	Ramafalo	15/08/2019
Dimakatso	Shai	4/2/2020
Refilwe	Masemola	10/10/2019
Bathmanathen	Moodley	9/12/2019
Tebogo	Phiri	10/7/2019
Refilwe	Masemola	14/10/2019
Sonto	Sambo	22/08/2019
Cebo	Ndlovu	25/07/2019
Gordon	Thakanyane	22/01/2020
Nompumelelo	Manzezulu	6/3/2020
Nishi	Sharma	11/3/2020

The User Account Management Policy outlines on page 7, section 7.4 the process for revoking user access on applications. However, a comparison between the active user list and the HR terminations could not be performed as the active user list did not have a standard naming convention for users on the system.

The User Access Management Policy outlines on page 8, section 7.6 the process for the review of user access rights. However, it was noted that the review of user access was not performed on PMIS.

The User Access Management Policy outlines on page 8, section 7.7 the process for the review of system administrator activities. However, the review of system administrator activities had not been performed.

The following password configurations could not be obtained to ascertain whether the PMIS system was adequately configured:

- Minimum password length;
- Maximum password age;
- Password complexity;
- Lockout threshold;
- Password history;
- Minimum password age; and
- Account lockout duration.

Risks

Failure to ensure that function amendments, password resets and user terminations are approved prior to their creation on application systems may result in unauthorised users being granted access to the application systems and the sensitive data stored on these systems, compromising its confidentiality, integrity and availability.

Failure to ensure that system administrator activities are regularly reviewed may lead to the inability to detect fraudulent activities performed by system administrators, which may compromise the integrity of financial information.

Failure to ensure that strong passwords are configured on the application systems may result in unauthorised access being gained through brute force and other cyber security attacks, which may result in financial information being compromised, degrading its confidentiality, integrity and availability.

Internal control deficiency

Financial and performance management: IT systems

Lack of adherence to the User Access Management Policy in ensuring that user access management controls are adequately implemented.

Recommendation

IT management should ensure that:

Function amendments, password resets and user terminations are adequately approved and documented.

System administrator activities are regularly reviewed and adequately documented.

Strong passwords are configured on the application systems, and are driven by the prescripts of the User Access Management Policy.

Management response

Management comment on audit findings: Management disagrees with all the findings except for the finding on PMIS administrator activities review and user access reviews

Management comment on internal control deficiencies:

The user list from the PMIS system was provided to AGSA with the user profile included as well as part of the report.

ICT provided the forms as ICT understood the request as to provide the forms provided by the users. The list could not be immediately provided after receiving clarification from AGSA team for ICT to provide a report extracted from PMIS.

This is a repetition from the SAGE request above on item 1.2.

The forms are received with the information as captured and approved by line managers where officials captured their names in the manner as captured on the system.

<p>The lack of the access review for PMIS users can be contributed to the task not correctly assigned to the new official due to the hand over process where one of the activities assigned should have been to also perform a user access review for PMIS system as well.</p> <p>PMIS Password configurations are solely managed by SITA as part of all the mainframe systems password configuration and/or policy. This includes systems such as WCS, PERSAL, etc.</p>		
<p>Management comment on recommendations:</p> <p>Function amendments, password resets, user access and user access are only performed through an approved user profile amendment form. User terminations must be communicated by line function to ICT for immediate execution.</p> <p>System administrator activities to be regularly reviewed and adequately documented on the ICT User management policy.</p> <p>For PMIS and all mainframe systems this process can only be managed by SITA. The DPWI ICT User Management Policy must be adequately documented to specify the same</p>		
<p>Remedial actions:</p>		
<p>What actions will be taken:</p>	<p>What actions will be taken:</p>	<p>What actions will be taken:</p>

Auditor's conclusions

Management responses are noted; however, the corrective actions agreed upon by management will be followed-up in the next audit cycle.

2.10 Inadequate implementation of user access management controls on WCS

Audit finding

The following deficiencies were noted with regards to the administration of user access controls on the WCS system:

The User Access Management Policy outlines the process for the creation of new users on applications systems on page 5, section 7.1. It was noted that there were 38 new users that had been created on WCS, however, the new user access form for William Lebudi could not be obtained. Furthermore, it was noted that the new user access forms for Patrick Nesangani and Mvelisi Mnyaka did not outline the access to be granted to the users.

The User Access Management Policy outlines the process to be followed for the amendment of user access on the application systems on page 6, section 7.2. However, the user amendment form for Valencia van Deventer had been approved to grant the user access to the Key Account Administration function, however, the user was granted access to the Project Budget Administration function.

The User Access Management Policy outlines the process for password resets on page 6, section 7.3 however, password reset forms for users that had reset their passwords could not be obtained.

The User Account Management Policy states on page 7, section 7.4 that "As soon as an employee leaves the department, all his/her system logons must be revoked." The following terminated users still had access to WCS, furthermore, 1 of the 5 terminated users had accessed the system after their termination date.

First Name	Surname	Persal-No	Last Transaction	RESIGNATION DATE	Comment
SIPHESIHLE	DIDISHE	25577603	20161206	20191231	Did not process transaction after termination
KIDWELL	MOKADI	27158659	20180510	20191231	Did not process transaction after termination
BOIPELO VERONICA	MOABI	27785866	20160513	20191231	Did not process transaction after termination
MAILE GEOFFREY	KGATLA	28126653	20161025	20191231	Did not process transaction after termination
MPHO	MALADZHI	28860292	20190808	20190731	Processed transaction after termination

The User Access Management Policy states on page 8, section 7.7 that "The best practice for access management will institute a review of system administrator/controller activities at least four times a year, for any seriously suspicious behaviour or critical events must be assessed and acted on." Although it was noted that the review of user access for system administrators had been performed, the review of system administrator activities had not been performed.

Furthermore, the password configuration received from the WCS system did not outline the following:

- Maximum password age;
- Lockout threshold;
- Minimum password age; and
- Account lockout duration.

It was further noted that the minimum password length (6 characters) had not been configured in line with the ICT Business Systems User Access Management Policy (8 characters).

The User Access Management Policy states on page 5, section 7.1 that "Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.". However, it was noted that there were 4 users that had duplicate user ID's on WCS, namely:

User-Id	First Name	Surname	Initials
OPW000	CHARLOTTE	DU TOIT	C
OPW000	DIMITRI	GEORGEADES	D.
OPW001	MALEFETSA E	MOSIA	MP
OPW001	NAMHLA	MAYEKISO	N.N.M.

Furthermore, there were 10 users that had duplicate ID numbers on WCS, namely:

User-Id	First Name	Surname	ID_NO
OPW001	MALEFETSA NE	MOSIA	101010000000
OPW002	THABO	MOSIA	101010000000
OPWAOF	KATHLEEN	SWANEPOEL	5903100169085
OPWBAZ	KATHLEEN	SWANEPOEL	5903100169085
OPW790	JINNY	FROST	6408105084080
OPWACH	JIMMY	FROST	6408105084080
OPW743	ANELEEZ	SWANEPOEL	7008030012088
OPW970	ANELEEZ	SWANEPOEL	7008030012088
OPW017	PM	PROJECT MANAGER	7409110027089
OPW060	RENAY	THERON	7409110027089

Risk

Failure to ensure that new users, user access amendments, password resets and user access terminations are approved prior to their creation on application systems, may

result in unauthorised users being granted access to the application systems and the sensitive data stored on these systems, compromising its confidentiality, integrity and availability.

Failure to ensure that system administrator activities are regularly reviewed may lead to the inability to detect fraudulent activities performed by system administrators, which may compromise the integrity of financial information.

Failure to ensure that strong passwords are configured on the application systems may result in unauthorised access being gained through brute force and other cyber security attacks, which may result in financial information being compromised, degrading its confidentiality, integrity and availability.

Failure to ensure that each user is uniquely identifiable on the application systems may result in the inability to hold a user accountable for fraudulent transactions that may be performed, compromising financial information, and degrading its integrity.

Internal control deficiency

Financial and performance management: IT systems

Lack of adherence to the User Access Management Policy in ensuring that user access management controls are adequately implemented.

Recommendation

IT management should ensure that:

ICT management should ensure that the process for the approval of access for new users, user access amendments, password resets and user access terminations are performed adequately.

IT management should ensure that system administrator activities are regularly reviewed and adequately documented.

IT management should ensure that strong passwords are configured on the application systems, and are driven by the prescripts of the User Access Management Policy.

IT management should ensure that each user has their own unique user ID and that users are not assigned more than one user account on the application.

Management response

Management comment on audit findings: Management disagrees with all the findings except for the finding on WCS admin access review

Management comment on internal control deficiencies:

Provided list of 11 sampled users with profiles
 Provided list of 11 sampled users with amended profiles
 No user password reset forms were requested under WCS, hence none were provided.
 This is a repetition from the SAGE request above on item 1.2.

Please see attached user access review Report does not currently exist on the system. PMIS Password configurations are solely managed by SITA as part of all the mainframe systems password configuration and/or policy. This includes systems such as WCS, PERSAL, etc. As this is a main frame system, user accounts are created and deactivated at SITA.		
Management comment on recommendations:		
Remedial actions:		
What actions will be taken:	By whom:	By when:
Perform regular review of system administrator activities	Khathu Nekhumbe	01 October 2020
Ensure user account end dates are updated on WCS	Khathu Nekhumbe	01 October 2020

Auditor's conclusions

Management responses are noted; however, the corrective actions agreed upon by management will be followed-up in the next audit cycle.

Management comments for the following findings have been received, but do not align to the findings that were raised:

The new user access form for William Lebudi could not be obtained. Furthermore, it was noted that the new user access forms for Patrick Nesangani and Mvelisi Mnyaka did not outline the access to be granted to the users.

The user amendment form for Valencia van Deventer had been approved to grant the user access to the Key Account Administration function, however, the user was granted access to the Project Budget Administration function.

Password reset forms for users that had reset their passwords could not be obtained.

Password configurations were not outlined

There were 4 users that had duplicate user ID's on WCS. Furthermore, there were 10 users that had duplicate ID numbers.

2.11 Inadequate implementation of user access management controls on Archibus

Finding:

The following deficiencies were noted with regards to the administration of user access controls on the Archibus system:

The User Access Management Policy outlines the process for the creation of new users on applications systems on page 5, section 7.1. However, it was noted that the user account for Odwa Nqwili had been created on 14 April 2019, whereas the user access form had been completed and approved on 12 December 2019.

The user account profiles on Archibus could not be obtained for the below new users. Furthermore, it was noted that there were 374 users that were created before 2015, when the reported implementation of Archibus was in August 2015.

Name and Surname	Date Created
MBALENTLE MANINGI	2019/08/02
KOKETSO MANOK	2019/04/17
ODWA NQWILI	2019/04/17
OBERT NKONWANA	2020/02/03
NTOKOZO KHOMO	2019/06/04
NONKCUBEKO SONGELWA	2019/04/17
NQABAKAZI MALAMLELA	2019/07/02
VHUTALI TSHIVHASE	2019/05/03
SIYABONGA KHUMALO	2019/04/03
HULISANI DZIALWA	2019/07/03
NTSIKELELO SMAYE	2019/11/07

The User Access Management Policy outlines the process to be followed for the amendment of user access on the application systems on page 6, section 7.2. However, the user amendment list received did not outline the changes that had been performed. Furthermore, user amendment forms for changes that had been made could not be obtained.

The User Account Management Policy states on page 7, section 7.4 that "As soon as an employee leaves the department, all his/her system logons must be revoked." It was noted that the below terminated users were active on Archibus: Moreover 4 of the 5 terminated users accessed the system after their termination date.

Name	Surname	Last Login Date	RESIGNATION_DATE	Comment
RAJA	GANGAVARAPU	2020/04/04	20191231	Accessed system after termination date
JACOB	MALELE	2020/04/03	20191231	Accessed system after termination date
NTOMBIFUTHI	MBELE	2020/03/26	20191115	Accessed system after

Name	Surname	Last Login Date	RESIGNATION_DATE	Comment
				termination date
AYANDA	SEGONE	2020/04/04	20191231	Accessed system after termination date
WYNAND	VAN JAARSVELD	2019/11/22	20191122	Did not access system after termination date

The User Access Management Policy states on page 8, section 7.6 that "The ISO will institute a review of all user access rights at least twice a year, which is designed to positively confirm all users." However, it was noted that the review of user access was not performed on Archibus.

The User Access Management Policy states on page 8, section 7.7 that "The best practice for access management will institute a review of system administrator/controller activities at least four times a year, for any seriously suspicious behaviour or critical events must be assessed and acted on." Although it was noted that the review of user access for system administrators had been performed, it had been noted that the review had not been performed on a quarterly basis as required by the User Access Management Policy.

Risk

Failure to ensure that new users, user access amendments, password resets and user terminations are approved prior to their creation on application systems may result in unauthorised users being granted access to the application systems and the sensitive data stored on these systems, compromising its confidentiality, integrity and availability.

Failure to ensure that user access rights are regularly reviewed may lead to the inability to detect users that have inappropriate access rights, which may lead to the performance of functions that are not commensurate with those user's job functions, which may lead to unauthorised transactions compromising the integrity and availability of financial information.

Failure to ensure that system administrator activities are regularly reviewed may lead to the inability to detect fraudulent activities performed by system administrators, which may compromise the integrity of financial information.

Failure to ensure that strong passwords are configured on the application systems may result in unauthorised access being gained through brute force and other cyber security attacks, which may result in financial information being compromised, degrading its confidentiality, integrity and availability.

Internal control deficiency

Financial and performance management: IT systems

Lack of adherence to the User Access Management Policy in ensuring that user access management controls are adequately implemented.

Recommendation

IT management should ensure that:

ICT management should ensure that the process for the approval of access for new users, user access amendments, password resets and user terminations are approved and implemented appropriately.

IT management should ensure that user access rights on the application systems are reviewed and adequately documented.

IT management should ensure that system administrator activities are regularly reviewed and adequately documented as required by the User Access Management Policy.

IT management should ensure that strong passwords are configured on the application systems, and are driven by the prescripts of the User Access Management Policy.

Management response

Management comment on audit findings: Management does not agree		
Management comment on internal control deficiencies: The following deficiencies were noted with regards to the administration of user access controls on the Archibus system: The Account for Odwa Nqwili was approved on 12 September 2019 and registered on ARCHIBUS on 17 September 2019 as per our records on audit trail. The user roles of sampled users as per the AGSA has been provided. A list of sampled users was not provided to DPWI ICT where in return the list of amended users and roles could be listed. This request is not applicable on for ARCHIBUS or any system that authenticates through Active Directory (AD). Password reset forms cannot be provided as ARCHIBUS authenticates through the departments Active Directory as a result user password reset are not done directly on ARCHIBUS. Four (4) out of the five (5) users on the list are still active members of the department. Furthermore, whether a user is active or not is determined at AD level where the authentication happens as ARCHIBUS will only manage the profile of the user. Since ARCHIBUS authenticates through AD, it would be duplication of effort if user access review is also implemented on ARCHIBUS as well. Furthermore, user access review remains the responsibility of line function and/or user to ensure a communication is sent to ICT through call centre to inform of changes in user's system access to effect the same on the system. Since ARCHIBUS has only been live since August 2019, the review of access and activities could only be done once, the review report is submitted		
Management comment on recommendations:		
Remedial actions:		
What actions will be taken:	What actions will be taken:	What actions will be taken:

Auditor's conclusions

Management responses are noted; however, the corrective actions agreed upon by management will be followed-up in the next audit cycle.

2.12 Inadequate implementation of user access management controls on WORX4U

Finding

The following deficiencies were noted with regards to the administration of user access controls on the WORX4U system:

The User Access Management Policy outlines the process for the creation of new users on applications systems on page 5, section 7.1. It was noted that a system generated list of active users with creation dates could not be obtained.

The User Access Management Policy outlines the process to be followed for the amendment of user access on the application systems on page 6, section 7.2 System generated list of user amendments obtained did not indicate the date that the amendments had been implemented.

The User Access Management Policy outlines the process for password resets on page 6, section 7.3 However, a system generated list of password resets could not be obtained from WORX4U.

The User Account Management Policy states on page 7, section 7.4 that "As soon as an employee leaves the department, all his/her system logons must be revoked." It was noted that there were 38 terminated users that did not have their access revoked, namely:

Name	Surname	Comment
Bongeka	Dlamini	Termination
Lynn	Erasmus	Termination
raja	gangavarapu	Termination
Sithembile	Gcwensa	Termination
zamo	gumede	Termination
maile	kgatla	Termination
Phindile	Khoza	Termination
Nondumiso	Khuzwayo	Termination
Meisie	Letsoaka	Termination
sandile	mabaso	Termination
Musa	Mabuza	Termination
Johannah	Mahlangu	Termination
Sasabona	Makama	Termination
prudence	makhubela	Termination
Mpho	Maladzhi	Termination
lister	mashaba	Termination
Zamambo	Mkhize	Termination
Zinhle	Mkhize	Termination
Boipelo	Moabi	Termination
kagiso	molala	Termination
hyworth	molefe	Termination

Mahlodi	Mpyana	Termination
Merriam	Mtsweni	Termination
Merriam MtsMerriam	Mtsweni	Termination
Tshinondiwa	Mulaudzi	Termination
samkelo	ngcobo	Termination
nsovo	nkanyani	Termination
calvin	nkgadime	Termination
Jupiter	Nkuna	Termination
Angelina	Phahlamohlak a	Termination
Cleopatra	Ramaru	Termination
Murendeni	Rasiluma	Termination
Onalenna	Segone	Termination
buyisile	shabalala	Termination
nokuthula	shabalala	Termination
Xitshembiso	Shirinda	Termination
Molebogeng	Sono	Termination
Khalipha	Xhanti	Termination

The User Access Management Policy states on page 8, section 7.6 that "The ISO will institute a review of all user access rights at least twice a year, which is designed to positively confirm all users." However, it was noted that the review of user access was not performed on WORX4U.

The User Access Management Policy states on page 8, section 7.7 that "The best practice for access management will institute a review of system administrator/controller activities at least four times a year, for any seriously suspicious behaviour or critical events must be assessed and acted on." Although it was noted that the review of user access for system administrators had been performed, the review of system administrator activities had not been performed.

Furthermore, the following password configurations could not be determined:

- Minimum password length;
- Maximum password age;
- Password complexity;
- Lockout threshold;
- Password history;
- Minimum password age; and
- Account lockout duration.

Risk

Failure to ensure that new users, user access amendments, password resets and user access terminations are approved prior to their creation on application systems may result in unauthorised users being granted access to the application systems and the sensitive data stored on these systems, compromising its confidentiality, integrity and availability.

Failure to ensure that user access rights are regularly reviewed may lead to the inability to detect users that have inappropriate access rights, which may lead to the performance of functions that are not commensurate with those user's job functions, which may lead to unauthorised transactions compromising the integrity and availability of financial information.

Failure to ensure that system administrator activities are regularly reviewed may lead to the inability to detect fraudulent activities performed by system administrators, which may compromise the integrity of financial information.

Failure to ensure that strong passwords are configured on the application systems may result in unauthorised access being gained through brute force and other cyber security attacks, which may result in financial information being compromised, degrading its confidentiality, integrity and availability.

Internal control deficiency

Financial and performance management: IT systems

Lack of adherence to the User Access Management Policy in ensuring that user access management controls are adequately implemented.

Recommendation

IT management should ensure that:

ICT management should ensure that the process for the approval of access for new users, user access amendments, password resets and user access terminations are approved and are adequately performed.

IT management should ensure that user access rights on the application systems are reviewed and adequately documented.

IT management should ensure that system administrator activities are regularly reviewed and adequately documented.

IT management should ensure that strong passwords are configured on the application systems, and are driven by the prescripts of the User Access Management Policy.

Management response

Management comment on audit findings: Management agrees.
Management comment on internal control deficiencies:

<p>WORX4U system does not have record creation or update dates thus the requested additional information on the dates could not be extracted.</p> <p>User access review is a critical process that line function must always ensure that it is performed to ensure ICT is informed of any changes to a user's accessibility to the system.</p> <p>ICT together with business is in the process of migrating from this system to another system, ARCHIBUS.</p>		
<p>Management comment on recommendations:</p> <p>As user access reviews are implemented for the WORX4u system management will ensure all other recommendations are considered noting the fact that this system may not be used by business going forward.</p>		
<p>Remedial actions:</p>		
What actions will be taken:	What actions will be taken:	What actions will be taken:

Auditor's conclusions

Management responses are noted; however, the corrective actions agreed upon by management will be followed-up in the next audit cycle.

3. SECURITY MANAGEMENT

3.1 Inadequate Security Management controls

According to best practise, the organisation should develop and enforce security policies and procedures to protect organisation information to maintain the level of information security risk acceptable to the organisation.

Audit finding

As previously reported, the following security management processes weaknesses were noted:

The ICT Security Policy was still in draft format;

There was no process in place to review the activity logs on active directory for security significant events;

Furthermore, the password security settings to the archibus, EPWP, PMIS and SAGE systems were not in line with the department's ICT security policy

These matters were reported in 2018-19 financial year.

Risk

Without an approved ICT security policy, the organisation might not be able to adequately and effectively support the overall objective of the organisation in terms of security. Furthermore, security breaches and incidents may not be timely detected, which may affect the confidentiality, integrity and availability of the systems.

Internal control deficiency

Financial and performance management: Formal controls over IT Systems

Lack of consequence management for not resolving prior audit findings.

Recommendation

Management should consider implementing the following:

Ensure that the ICT security policy is approved.

Ensuring that operating security logs are enabled and reviewed on the regular basis.

Ensure that password settings on all systems are in place and adequate as per the department's ICT security policy and best practices.

Management response

Management comment on audit finding:

Management agrees with the finding. WCS password history is managed by SITA using mainframe systems policy.

AD password history is at 10 to strengthen security. Management will update the policy to take into consideration to cater for per system security measures as long as they are in line with best practice.		
Management comment on internal control deficiencies: Management agrees		
Management comment on recommendation: Management Agrees		
Remedial action: Update policy to take into consideration to cater for per system security measures as long as they are in line with best practice.		
What actions will be taken: Update policy to take into consideration to cater for per system security measures as long as they are in line with best practice	By whom: Bheki Zwane Position: Act: CIO	By when: 30 September 2020

Auditor's conclusion

Management comments are noted and corrective actions will be evaluated in next audit cycle.

4. CHANGE MANAGEMENT CONTROL

4.1 Inadequate change management process

Program change management controls ensure that any proposed changes to an existing information systems environment would be coordinated, scheduled, authorised and tested to prevent unnecessary disruptions, erroneous changes and unauthorised and inappropriate access to programs.

Audit finding:

The ICT Policy states on page 12, section 1.4 that "This policy shall be reviewed at least once every three years and amended as and when the need for changes arises.". Furthermore, the ICT Policy states on page 64, section 7.4.3.1 that "Every change to the DPW ICT infrastructure component such as: operating systems, computing hardware, networks and applications is subject to the Change Management Policy and must follow the Change Management Procedures."

The following control deficiencies were noted:

The ICT Policy had not been approved for implementation in the organisation and did not outline the following:

- Development of changes requested;
- Testing of changes (QA and user acceptance test); and
- Implementation of changes.

A system generated list of changes could not be obtained from the following applications in scope:

- GIS;
- SAGE;
- PMIS;
- Archibus;
- WORX4U; and
- WCS.

Risk

Failure to ensure that there is an approved ICT Policy that governs change management may result in the inability to enforce procedures within the organisation and to hold them accountable for transgressions of the policy. Furthermore, failure to maintain a system generated list of changes on the application systems may lead to the inability to trace unauthorised changes that have been implemented on the applications systems, which may alter system functionality, compromising data integrity.

Internal control deficiency

Financial and performance management: IT Systems

Systems limitations on GIS, SAGE, PMIS, WORX4U and WCS resulted in the inability to extract a list of changes.

Recommendation

ICT management should ensure that the ICT Policy is approved. Furthermore, ICT management should ensure that system generated logs to track changes on application systems are maintained, and that changes that have been made on the applications have been approved and tested prior to implementation.

Management response

Management comment on audit findings: Management agrees.		
Management comment on internal control deficiencies: The department follows a change management process however for the audit period there were no changes to submit or implemented on the systems; <ul style="list-style-type: none"> ○ GIS; ○ SAGE; ○ PMIS; ○ WORX4U; and ○ WCS. On ARCHIBUS however, the system went live from August 2019 with only three modules. The only changes that were being affected were deployment and infrastructure changes during go live		
Management comment on recommendations: Management to consider and add where possible the recommendations provided		
Remedial actions:		
What actions will be taken: Review ICT policy	By whom: Pakiso Mphuthi Position: Security Manager	By when: 31 March 2021

Auditor's conclusion

Management comments are noted and corrective actions will be evaluated in next audit cycle.

4.2 Inadequate implementation of change controls around Reapatala and EPWP

Program change management controls ensure that any proposed changes to an existing information systems environment would be coordinated, scheduled, authorised and tested to prevent unnecessary disruptions, erroneous changes and unauthorised and inappropriate access to programs.

Audit finding

The policy on program change management is included in the Consolidated Information and Communication Technology Policy, it was noted that the current policy was still in draft since 28/08/2018 and does not provide adequate guidance on the process to be followed when:

- Performing change management activities;
- Migration of changes to production
- Development of changes requested;
- Testing of changes (QA and user acceptance test); and
- Implementation of changes.

Although paragraph 64 of the policy stated that the policy stated “A *Change Management Log must be maintained for all changes. The log must contain, but is not limited to; Date of submission and date of change, Owner and custodian contact information, Nature of the change and Indication of success or failure,*” system generated logs of all changes implemented on systems during the period under review could not be provided due to system limitation, thus assurance could not be provided on whether all changes implemented followed a proper change management process (i.e. changes were formally requested, approved and tested prior implementation into production)

Without adequate program change management policy, there might not be a process which provides a managed and orderly method in which changes to the information technology environment are requested, tested and approved prior to installation or implementation.

Without the change logs it would be difficult to trace if any changes were made on the system, by whom and why the changes were and whether the change were properly authorized by management.

Internal control deficiency

Financial and performance management: Control over IT Systems

Failure by IT management in ensuring that application systems in use can log and track changes that have been implemented.

Recommendation

ICT management should ensure that the ICT Policy is approved. Furthermore, ICT management should ensure that system generated logs to track changes on application systems are maintained, and that changes that have been made on the applications have been approved and tested prior to implementation. This policy should be kept up to date in order to enforce compliance.

Management response

Management comment on the audit finding: Management agrees.		
Management comment on internal control deficiencies: The policy has now been approved, we are waiting for the hard copy to implement. Deficiencies on policy will be reviewed.		
Management comment on recommendation: Recommendation will be considered when policy is reviewed.		
Remedial action: All identified deficiencies will be addressed		
What actions will be taken: All identified deficiencies will be addressed	By whom: Pakiso Mphuthi Position: Security Manager	By when: 31 March 2021

Auditor's conclusion

Management responses are noted; the corrective actions agreed upon by management will be followed-up in the next audit cycle.

5. INFORMATION TECHNOLOGY CONTINUITY MANAGEMENT

5.1 Inadequate IT service continuity controls

Section 7.3.3.7. of the DPW Annual Performance Plan (APP) states that the lack of a disaster recovery plan (DRP) has been a recurring audit finding. The department has now finalised and signed off a DRP plan and is in the process of implementing it.

Audit finding

As previously reported, the following deficiencies were noted with regard to the management and implementation of IT Service Continuity/ Disaster Recovery processes at the department:

- Although Disaster Recovery Plan (DRP) was developed and approved, it was noted that the DRP was not tested in the financial year under review.
- There was no formal backup policy and procedure.
- There was no performance of periodic restoration of backups.
- These matters were reported in 2018-19 financial year.

Without a comprehensively documented, tested and regularly updated Disaster Recovery and Business Continuity Plan, it might not be possible to recover the key business operations, critical systems, applications, their supporting infrastructure or networking capability in the correct sequence and time, to ensure that the department's business operations could be sufficiently resumed at an alternative processing site without considerable loss to its financial well-being and negative impact of service delivery should a disaster occur.

Internal control deficiency

Financial and performance management: Formal controls over IT Systems

The non-implementation of the DRP was due to delay in the DR solution tender issued last year. Also Lack of consequence management for not resolving prior audit findings.

Recommendation

The Chief Information Officer should ensure that the DRP is periodically tested to ensure that the plan is practical with regard to its execution. During the testing process, the relevant role players in the disaster recovery process should receive the necessary training to ensure the success of the recovery process. Furthermore, document and approve the backup policy to include the following:

s

- Backup strategy
- Roles and responsibilities
- Backup frequency
- Retention period
- Backup window (time available each day to complete backups)
- Back restoration process
- On and off-site requirements
- Archival requirements
- Special media considerations

Management response

Management comment on audit findings: Management disagrees with the findings Although Disaster Recovery Plan (DRP) was developed and approved, it was noted that the DRP was not tested in the financial year under review. Response: The primary site for DR is still under construction. The alternative site is available and running however in terms of replication of data there was a delay due to the procurement of software licenses. There was no formal backup policy and procedure. Response: There is a formal backup policy and the procedure will be developed by Quarter 3. There was no performance of periodic restoration of backups. Response: Periodic restorations of backups will be done after the implementation of the DR solution. At the moment restorations are done on request. These matters were reported in 2018-19 financial year.		
Management comment on internal control deficiencies:		
Management comment on recommendations:		
Remedial actions:		
What actions will be taken:	By whom:	By when:
Procurement of the software licenses		
Develop SOP for backup and recovery	Bheki Zwane (Act: CIO)	November 2020
Testing DR	Bheki Zwane (Act: CIO)	February 2021

Auditor's conclusions

Management comments are noted and acknowledged. The action plans will be followed up during the 2020/21 audit and the outcome of the assessment will be communicated at completion of the audit.