BRIEFING NOTE TO SCOPA | **PFMA 2021-22**

SA POSTBANK SOC LIMITED

02 November 2022

AUDITOR-GENERAL SOUTH AFRICA

1. Introduction

1.1. Reputation promise of the Auditor-General of South Africa

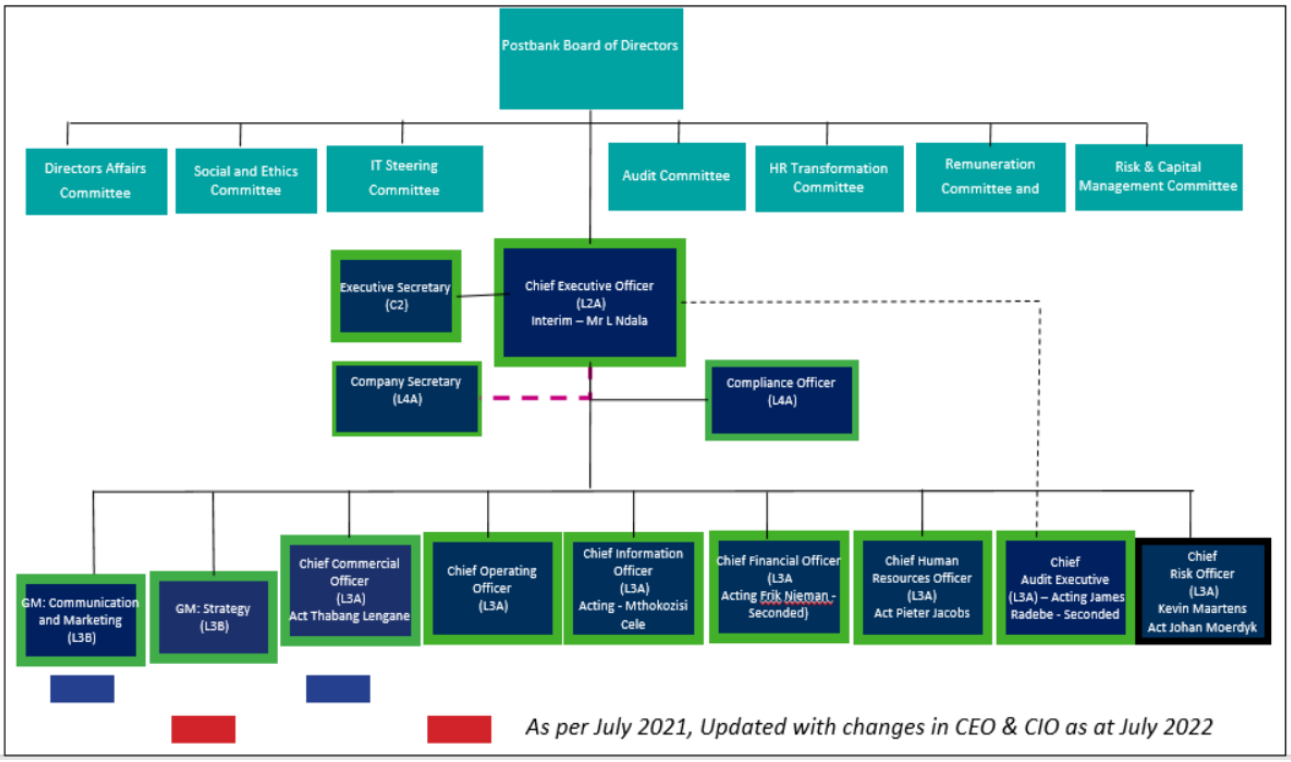
The Auditor-General of South Africa has a constitutional mandate and, as the Supreme Audit Institution (SAI) of South Africa, it exists to strengthen our country's democracy by enabling oversight, accountability and governance in the public sector through auditing, thereby building public confidence.

1.2. Purpose of document

The purpose of this briefing document is for the Auditor-General of South Africa (AGSA) to brief SCOPA on the audit outcomes and other findings in respect of the annual financial statements, compliance with legislation and performance against predetermined objectives of the South African Postbank (Postbank) for the 2021-22 financial year end.

1.3. Organisational structure

The key positions (board, chief executive officer, chief financial officer, chief information systems officer) together with other key positions should be filled to provide some stability in the entity. See below structure, majority of the key positions are filled by acting candidates:



1.4. Overview (executive summary)

1.4.1 Throughout the audit, management have demonstrated a positive attitude towards ensuring that financial statements are prepared in accordance with the requirements of financial reporting standards and that they are supported by complete and accurate accounting records. This was evidenced by an improved turnaround time for providing requested information and responses to communication of audit findings and in certain instance issues were resolved before they were escalated resulting in much improved audit steering committee meetings.

1.4.2 Management continuously made themselves available for meetings and demonstrated their commitment to improving the audit outcome. The CEO was also very prompt in proving necessary approvals for access to information and this has enabled us to meet deadlines.

1.4.3 The overall audit outcome of Postbank has remained stagnant with a disclaimer opinion on and compliance with legislation findings reported in the audit report.

1.4.4 The financial statements submitted for audit on 31 May 2022 were not accompanied by the annual performance report (APR), the APR was prepared after we made follow ups on the submission, and this contributed to the late submission of the APR. The entity did not achieve its plans to corporatise the bank and acquire a banking license. Although the entity reported profit in the current year this was mainly due to the decrease in expected credit loss. Thus, Postbank did not increase its revenue and decrease its expenses.

1.4.5 Responses to address prior year audit findings and key internal control deficiencies identified have been slow. Action plans were not adequately designed and / implemented by management to resolve prior qualification areas. This resulted in repeat material findings in the submitted financial statements submitted for audit.

1.4.6 The following is a summary of key root causes and/ recommendations that should be addressed or implemented to improve the audit outcomes. It is important to note that most of the key root causes and/ recommendations were raised in the previous audits thus we are concerned that recommendations are not being implemented. We have also noted that these control deficiencies have fuelled fraud at Postbank which is resulting in material losses:

- The entity should fill key positions and capacitate its internal audit function, that will assist with internal controls and risk-based audits on key internal control deficiencies that resulted in negative audit outcomes.
- The overreliance of Postbank on systems and officials of the South African Post Office SOC Limited (SAPO) and the significant number of vacancies on the IT department structure also need to be addressed, as the weaknesses in internal controls of the SAPO will have an impact on Postbank.
- The internal control deficiencies on IGPS and Oracle ERP system require immediate attention, as they relate to the core of Postbank business, and affect the material transactions and account balances in the financial statements.
- The reliance on service providers for information, specifically for South African Social Security Agency (SASSA) related components of financial statements, resulted in significant delays during the audit. As a result, we were unable to conclude on the balances “other deposits (grants)” disclosed in the financial statements.
- Non-compliance within the procurement legislation and processes identified, resulted in irregular expenditure. Leadership also did not implement appropriate processes to investigate and conclude on irregular expenditure. In addition, leadership should implement consequence management for all non-compliance relating to policy and procedures and job descriptions.
- To improve the audit outcomes, the key role-players should ensure that the root causes are addressed, and more attention is given to the key IT controls.

1.4.7 We encourage the accounting authority to strengthen and improve controls that will prevent non-compliance with SCM legislation as this will reduce the incurrence of irregular expenditure. Key risk management processes must also be prioritised and implemented to ensure that key business and strategic risks are properly mitigated.

2. Audit opinion

2.1. Postbank audit opinion history

SOUTH AFRICAN POSTBANK SOC (LIMITED)					
DESCRIPTION	**2021-22**	**2020-21**	**2019-20**	**2018-19***	**2017-18***
A: Report on the audit of the financial statements					
Audit opinions					
Areas of qualification:					
• *Other deposit (grants)*	√	√	√		
• *Other reserves*	√	√			
• *Transaction & fee income*	√	√			
• *Material losses*	√				
• *Intercompany receivable*	√	√			
• *Deposit from customers*		√			
Emphasis of matter:					
• *Material uncertainty relating to going concern*	√				
• *Restatement of corresponding figures*	√				
• *Cyber security incidents*	√				
• *Material impairment financial assets*			√		
• *Fruitless & wasteful expenditure*			√		
• *Material losses*		√	√		
B: Report on predetermined objectives					
• *Report on predetermined objectives*	No material findings reported.				
C: Report on compliance with legislation					
• *Financial statements, performance report and annual report*	√	√	√		
• *Procurement and contract management*	√	√	√		
• *Expenditure management*	√	√			
• *Strategic Planning*			√		
• *Consequence management*	√	√			
• *SOE & governance*			√		
• *Revenue management*	√	√			

AUDIT OPINION INDEX

	CLEAN AUDIT OPINION: No findings on PDO and compliance
	UNQUALIFIED with findings on PDO and compliance
	QUALIFIED AUDIT OPINION (with/without findings)
	ADVERSE AUDIT OPINION
	DISCLAIMER AUDIT OPINION

***** Dormant

2.2. Report on the audit of the Annual Financial Statements

The issues form a basis of the ***disclaimer of opinion*** included in the audit report of the Postbank on their annual financial statements for the 2021-22 financial year-end.

Finding	Root cause	Recommendation
Other reserves I could not obtain sufficient appropriate audit evidence that other reserves had been properly transferred and accounted for on 1 April 2019, due to the poor status of accounting records. The other reserves were determined and included after deducting the liability of the other deposits (grants) liability transferred to the public entity.	• Lack of proper record keeping that will ensure complete, relevant and accurate information is accessible and available to support credible financial and performance reporting. • Inadequate risk management process • Slow response by management in implementing recommendations resulting in repeat findings • A lack of adequate review processes to ensure that amounts recorded in the financial statements are accurate, agree to the supporting schedules, that errors identified, are corrected timeously and that presentation and disclosure is in line with the relevant financial reporting framework • Regular reconciliations were not always adequately prepared during the year, • The use of manual reconciliations coupled with a lack of assurance processes not implemented in time to ensure that information was accurate and complete, resulted in a number of limitations and errors being experienced and identified. • Overreliance on South African Post Office (SAPO) for critical information technology services meanwhile SAPO's infrastructure is old, SAPO faces instability in key vacant positions and has weak internal controls thereby spreading to Postbank as well. • Poor controls on Integrated Grant Payment System (IGPS) leading to issues such as duplicated user accounts, inadequate user profile roles, disabled general ledger tests, negative balance transactions and no transactions logs to name but a few	• Management must develop and implement an effective audit action plan to address the root causes and ensure proper record keeping. This will enable complete, relevant and accurate information being accessible and available to support financial and *performance reporting.* • Management should further fill key vacant positions to ensure stability and prioritise key information technology concerns identified to enable an environment that is conducive for effective internal controls
Other deposits (grants) I could not obtain sufficient and appropriate audit evidence for other deposits (grants) due to the limitations imposed by the information system to manage the related transactions. The required supporting documents such as Bankserv to IGPS recon for IGPS transactions was not provided, we started following up with management early April 2022 and management was not ready. To date, the required support has still not been provided and we had discussed with management that the limitation will be reported in the audit report.		
Fee and transactional income I could not obtain sufficient appropriate audit evidence for fee and transactional income, due to the inadequate status of accounting records and a lack of required reconciliations between the supporting information systems not conducted in a timely manner. Postbank generates material revenue on the transactions from IGPS and since we could not verify the number and amount of transactions on IGPS due to the absence of a Bankserv reconciliation, there is therefore a consequential limitation on the transaction and service		

fee income as reported in the statement of financial performance.		
Material losses We could not obtain sufficient appropriate audit evidence that material losses are complete due to the significance of internal control deficiencies identified on key systems and cyber security incidents. We have also issued a number of findings on IT related internal controls as reported in the management report, majority of these findings were also reported in the previous financial year. The weaknesses identified in these findings contributed to the continuous cyber incidents on IGPS.		
Intercompany receivable We could not obtain sufficient appropriate audit evidence for the intercompany receivable and its related accounts due to the inadequate status of accounting records and a lack of sufficient and appropriate supporting information. We stared following up with management on the progress made on the journals issues raised in the prior year and management was not ready and indicated that the support will be provided with the AFS submission however management still did not provide adequate support to the prior year journals. The journals without support were processed to balance the trial balance and was reported in the audit report as there are still no support for them.		

2.3. Emphasis of matter paragraphs

The ***following emphasis of matter paragraphs*** were included in the audit report of the Postbank on their annual financial statements for the 2021-22 financial year-end.

Finding	Root causes	Recommendation
Material uncertainty related to going concern I draw attention to note 33 to the financial statements, which indicates that the annual financial statements have been prepared on the basis of accounting policies applicable to a going concern, describes the events or conditions, along with other matters as set forth in note 33 that may cast significant doubt on the public's ability to continue as a going concern and how the public entity is responding to them. My opinion is not modified in respect of this matter	• Slow response by management in implementing recommendations • Failure to implement risk mitigation measures as directed by the SARB as well as non-compliance with the Designation Notice conditions	Management must ensure that recommendation made are implemented timely by enforcing consequence management
Restatement of corresponding figures As disclosed in note 32 to the financial statements, the corresponding figures for 31 March 2021 were restated as a result of errors in the financial statements of the public entity at, and for the year ended, 31 March 2022	• A lack of adequate review and processes that should be there to ensure that amounts recorded in the financial statements are accurate, agree to the supporting schedules, that errors identified, are corrected timeously and that presentation and disclosure is in line with the relevant financial reporting framework	Leadership must stabilise the finance unit by filling key vacant positions to enable the development of adequate processes and procedures for daily processing and monitoring.

3. Report on the audit of compliance with legislation

Finding	Root cause	Recommendation
Annual financial statements and annual report • The financial statements submitted for auditing were not prepared in accordance with the prescribed financial reporting framework and supported by full and proper records, as required by section 55(1)(a) and (b) of the PFMA. • Material misstatements of current assets identified by the auditors in the submitted financial statements were corrected, but the supporting records that could not be provided resulted in the financial statements receiving a disclaimer of opinion.	• The instability and capacity issues including the board members resulted in the slow response by management in implementing recommendations as all the non-compliance subject matters are repeat • Policies and standard operating procedures were not designed and implemented to facilitate an effective process of consequence management. • Disciplinary steps were not taken against officials who had incurred irregular and fruitless expenditure as investigations were not performed. • Postbank leadership did not exercise adequate oversight responsibility regarding compliance and related internal controls to ensure that compliance requirements are met • Inadequate compliance monitoring procedures to ensure compliance with relevant laws and regulations. • Overreliance on South African Post Office	Management must develop and implement an effective audit action plan to address the root causes and ensure that recommendations are implemented timely by enforcing consequence management
Expenditure management • Effective and appropriate steps were not taken to prevent irregular expenditure amounting to R117 946 000 as disclosed in note 35 to the annual financial statements, as required by section 51(1)(b)(ii) of the PFMA. The majority of the irregular expenditure was caused by the entity approving an agreement without following proper SCM processes. • Effective steps were not taken to prevent fruitless and wasteful expenditure amounting to R5 979 000, as disclosed in note 34 to the annual financial statements, as required by section 51(1)(b)(ii) of the PFMA. The majority of the fruitless and wasteful expenditure was caused by assets procedure in vain and interest incurred due to late payment to creditors.		

Finding	Root cause	Recommendation
Procurement and contract management • Some of the contracts were not awarded in an economical manner and/or the prices of the goods or services were not reasonable as required by PFMA 57(b).		
Consequence management Disciplinary steps were taken against officials who had incurred irregular and fruitless and wasteful expenditure as required by section 51(1)(e)(iii) of the PFMA. This was because the investigations into irregular and fruitless and wasteful expenditure were not performed		
Revenue management • Effective and appropriate steps were not taken to collect all revenue due, as required by section 51(1)(b)(i) of the PFMA. This was mainly due to SASSA-related revenue not collected from another entity within the portfolio.		

4. Financial health risk

The South African Reserve Bank (SARB) has issued a variation notice to Postbank. The variation order contained a number of recommendations required to be implemented by the bank in order to deal with the significant deficiencies in the internal control environment.

Failure to implement the variation conditions may result in the revocation of Postbank's designation as a designated clearing system participant (DCSP) in terms of section 6(3)(b) of the NPS (National Payment System) Act. The variation notice was gazetted on 17 December 2021 with an implementation period of 12 months with a due date of 16 December 2022.

Management regularly meets with the SARB where the provide regular feedback on the status of implementation of these recommendations.

5. Irregular expenditure analysis

During the year under review, the public incurred irregular expenditure amounting to R117 million, which was disclosed in the financial statements. The analysis of irregular expenditure shows that irregular expenditure increased by 57% compared to the prior year. The expenditure can be broken down as follows:

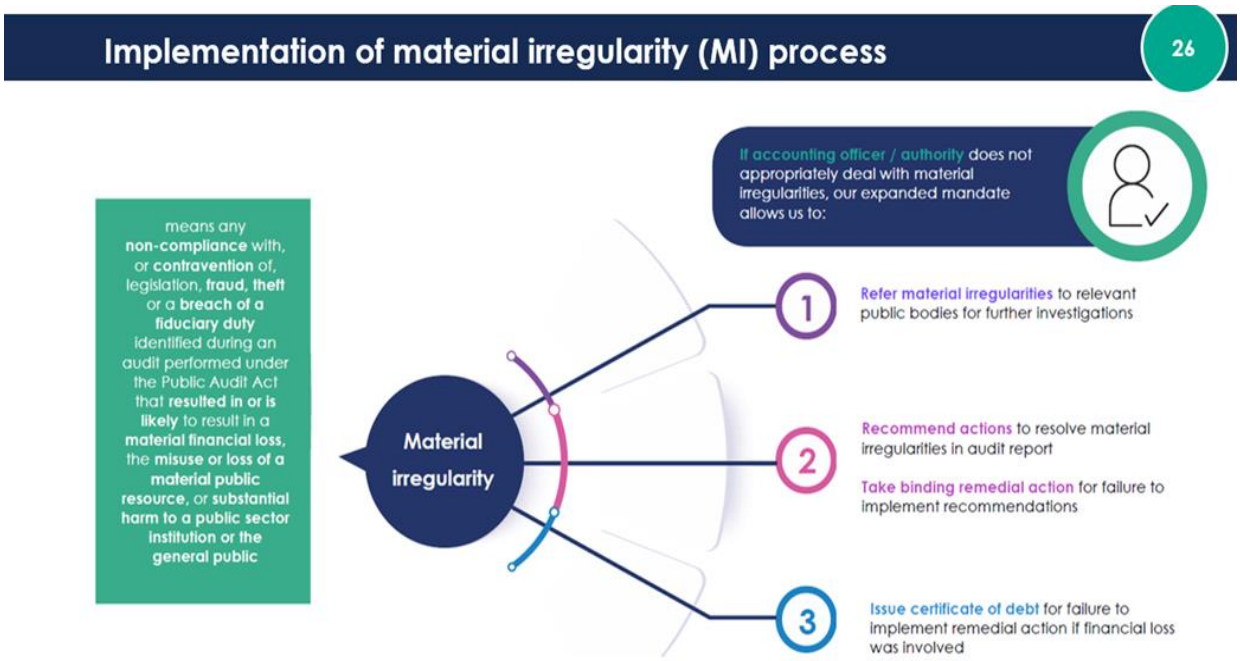
Description	Amount (R)	Root cause	Impact
Incurred in current year	117 946 000	Services procured without contracts in place and non-adherence to procurement processes	Non-compliance resulting in irregular expenditure
Total IE disclosed	**117 946 000**		

6. Fruitless and wasteful expenditure analysis

During the year under review, the public entity incurred fruitless and wasteful expenditure amounting to R5, 9 million, which was disclosed in the financial statements. The analysis of fruitless and wasteful expenditure shows a slight increase when compared to the prior year. The expenditure can be broken down as follows:

Description	Amount (R)	Root cause	Impact
South African Revenue Services (SARS)	1 888	SARS payment was late and therefore incurred penalty interest	Non-compliance resulting in fruitless and wasteful expenditure
Oracle Corporation (Pty) Ltd	4 059 201	Software licences procured but not in use (Oracle)	
Telkom Soc Ltd	1 917 980	Interest charged by Telkom for late payment or delay in paying the supplier	
Total FWE disclosed	**5 979 000**		

7. Material irregularities



The following are material irregularities were transferred from SAPO

Description	Actual / likely Loss	Actions taken	Status of MI
Failure to maintain an effective system of internal control over safeguarding of customer bank cards issued – financial loss incurred due to inventory of cards that were unaccounted for that were written down.	R68 760 420	Failure to implement effective controls on the card management and SASSA beneficiary payment system. The entity has recently suffered a series of cyber breaches that indicates the absence of key controls that the entity has been failing to implement The MI is in the process of being referred to MIC. Further actions might be taken based on submission made by the AA	Referral in progress
Failure to implement effective controls on the card management and SASSA beneficiary payment process: Cards written off due to compromised Issuer Master Keys (IMKs)	R13 579 174	Stolen SASSA cards used to commit fraud The MI is in the process of being referred to MIC. Further actions might be taken based on submission made by the AA	Referral in progress

8. Status of internal controls

	Leadership						Financial and performance					Governance		
Entity	Oversight responsibility	Effective leadership culture	HR Management	Policies & procedures	Action plans	IT governance	Proper record keeping	Processing and reconciling controls	Reporting	Compliance	IT Systems controls	Risk management	Internal audit	Audit committee
Postbank SOC Ltd														

Legend Drivers	Good	Causing Concern	Intervention required

The following internal control deficiencies relate to the significant internal control deficiencies that resulted in the basis for a disclaimer of opinion, the findings on compliance with legislation and the audit of predetermined objectives:

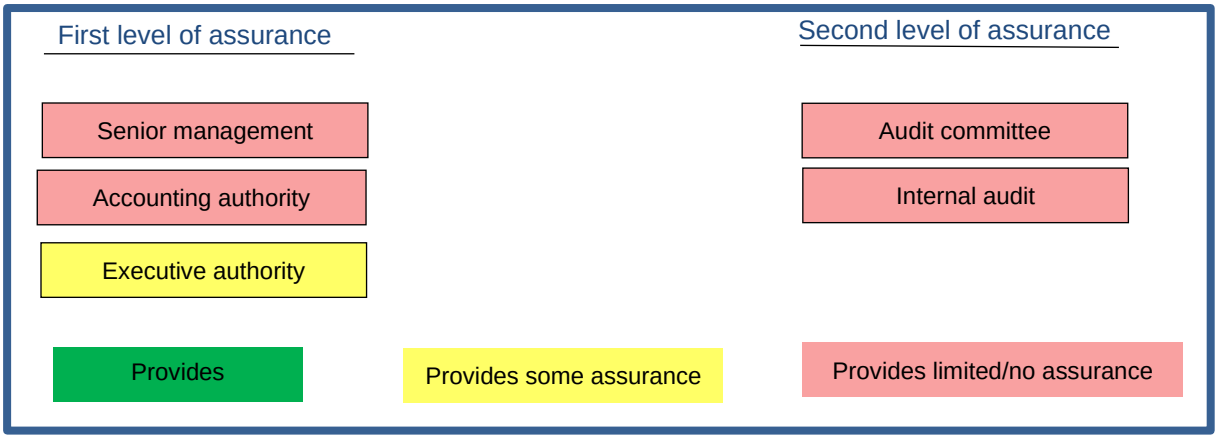
- Instability and vacancies in key leadership and management positions during the year contributed to the inadequate implementation of the approved action plan as it was not effectively monitored, and recommendations were not properly followed through.
- Leadership and management did not implement oversight responsibilities to ensure that the internal control deficiencies on Integrated Grants Payment System (IGPS), such as reconciliations of data to the systems are addressed to ensure that the system generates reliable data.
- Leadership did not ensure that the entity has effective policies and processes in place to prevent irregular and fruitless, and wasteful expenditure. Additionally, they did not ensure that instances of irregular and fruitless, and wasteful expenditure were investigated in order to implement disciplinary action where necessary.
- Leadership did not implement effective monitoring controls over services rendered by a shareholding entity on its behalf. The entity remained over-reliant on the processes and controls of the shareholding entity, which were deficient, for significant components of financial information and compliance requirements of supply chain management processes. This impacted on significant limitations and delays in the submission of information, material errors and material non-compliance, which resulted in irregular expenditure and unfavourable audit outcomes.
- Management did not timeously implement proper record keeping over information they were responsible for, to ensure that complete, relevant and accurate information was accessible and readily available to support credible financial reporting and compliance.
- The leadership did not ensure that adequate structures, processes and practices were implemented for the governance of IT. Principles and guidance of good corporate governance (King IV) and IT governance (COBIT) practices were not adequately implemented.

- Leadership did not ensure a sound IT control environment that is supported by a sound IT infrastructure, the significant internal control weaknesses identified on the bank's key applications and databases contributed to material losses.
- The weak and/or lack of IT security controls was due to outdated IT Infrastructure (Server, Operating Systems, Databases and Applications) as well as a moratorium on procurement.
- The weak disaster recovery processes were due to failure to upgrade the supporting hosting infrastructure, manage disk space and renew expired backup software license.

9. Assurance providers

9.1 Our reporting and the oversight processes reflect on past events, as it takes place after the end of the financial year. However, management, the leadership and those charged with governance contribute throughout the year to the credibility of financial and performance information and compliance with legislation by ensuring that adequate internal controls are implemented.

9.2 We assess the level of assurance provided by these assurance providers based on the status of internal controls as reported above and the impact of the different role players on these controls. We provide our assessment for this audit cycle below.



Senior management provides limited assurance

- Senior management did not monitor compliance effectively in some instances. Despite some progress in some areas, there were 6 repeat non-compliance findings identified during the audit.
- Senior management did not monitor the controls around the organisation's processes and reconciling controls, which resulted in various number of material findings raised during the audit. Some of the findings were resolved through the audit process.
- Adequate reviews to ensure that financial statements and annual performance report submitted for auditing were free from material errors and misstatements were not performed by senior managers, even though some were subsequently resolved.
- The IT system controls were not effectively updated to ensure that effective IT system controls are in place to address the risks surrounding the IT environment. This is evidenced by the recent Cyber-Attacks on the entity that has resulted in fraudulent activities and money stolen.

- Management managed to provide the information requested for a number of requests on time especially within the Finance Division however, we had a number of non-submission findings raised during the audit mainly relating to Supply Chain Management/Procurement which are material.
- There have been a number of acting CEOs over the years, which contributed to a lack of an effective leadership culture and risk governance was not always assigned the necessary attention.

Accounting authority provides limited assurance

- The accounting authority was not properly capacitated and despite following up with executive management to address prior matters and non-compliance, these efforts were negatively affected by the constant changes within the senior management as well as the vacancy rate at senior management level.
- The audit action plans developed were not always adequate to fully address the matters from the prior years, evidenced by the repeat limitations of scope on some of the same line items as in prior years.
- A number of policies and procedures of the entity are sitting as draft or not in place or South African Post Office policies are being used, which is not a good indicator of the control environment.

Executive Authority provides Some assurance

- The executive authority implemented a moratorium due to the state of affairs at the entity to ensure that operations that are detrimental to the entity be managed better and monitored from the ministry. There were some staff deployed to act in key roles (i.e. seconded from other State-owned entities) just to ensure a bit more stability.
- The executive authority has been monitoring the cyber incidents closely and has also been pro-active in the fit and proper assessments process with the aim of filling the board positions.

Internal audit provides limited assurance

- The Internal Audit function was established during the 2021/22 financial year with only two members and therefore did not carry out any work for the year under review. Furthermore, the Internal audit did not have an audit charter, an audit action plan and therefore no reports were produced as minimal work was conducted.

Audit committee: provides limited assurance

- The audit committee had instabilities with a resignation towards the end of the year by the chairperson of the committee, thus resulting in the committee having only 2 members. This impacted on the various roles and responsibilities the committee needed to perform in terms of its oversight, including adequate annual financial statement reviews.
- Despite reviewing, evaluating and monitoring responses to risks with the view to promote accountability and achievement of strategic goals of the entity, the audit committee was not always effective in providing oversight over the internal control environment, including financial and performance reporting and compliance with legislation.

10. Cyber security incidents

10.1 On 28 October 2021, Postbank identified an unusual balance in a SASSA beneficiary account. The internal investigation by Postbank identified the creation of two privileged accounts on the IGPS database server, and unauthorised access to the Oracle database. Further beneficiary accounts had their limits inflated and a "malicious scheduled job" was found to have been implemented within Oracle, removing audit logs from the audit table.

10.2 This resulted in a loss of approximately R89 million, as also reported in the media. Similar incidents also occurred in 2019 where a series of fraudulent transactions took place through use of the SASSA cards, resulting in losses of millions. These matters, raised as material irregularities, were referred to the Directorate for Priority Crime Investigation and a probe is currently underway.

10.3 The fraud committed demonstrated many similarities based on a systematic approach which included four (4) variables namely, encryption keys, EMV software, EMV reader and a physical SASSA card.

10.4 These incidents point to an environment where the risk of fraud continues to materialise as it continues to be perpetuated and it remains susceptible (exposed) to fraud. Furthermore, these incidents have introduced additional audit risks, which must be addressed.

10.5 The majority of the matters remained unaddressed despite them being reported since the inception of the SASSA/ Post Office contract to distribute grant payments. These also formed a major basis for the disclaimer of audit opinions for the Postbank over the past two (2) audit cycles. The weaknesses also formed the basis for the variation order issued by the South African Reserve Bank (SARB) in Dec 2021, which noted failure to implement its recommendation might result in the bank's privileges being revoked, thereby posing threat to its ability to render these services.

10.6 The modus operandi included a criminal syndicate accessed the Oracle database and stole a reported R89 million. They created inflated limits on 281 x Post Bank Beneficiary cards. Without the knowledge of the beneficiaries, money was withdrawn from ATMs, primarily in Gauteng and KwaZulu Natal. There were 3 main types of account takeovers:

- Straight account takeover: credit added into the account and funds withdrawn without beneficiary's knowledge.
- Account clustering: the use of multiple beneficiaries' accounts linked to a single Post Bank user ID; and
- The use of deceased beneficiary bank accounts.

10.7 Since then, there have been a further three (3) heists of smaller magnitude but similar modus operandi. The IGPS system and the Oracle database are completely compromised, and the risk if future theft must be mitigated by fully addressing the weaknesses reported. These weaknesses noted, were mainly due to A lack of past investment in IT infrastructure as well as poor IT governance processes that do not support the advancement of IT in the entity.

10.8 The weaknesses noted pose high risk to the bank's operations. Negative impact on the bank's operations will have a severe impact on the millions of South Africans who rely on the grant payments to sustain their livelihoods. The bank should prioritise the deployment of the IT refresh (systems, storage, network, services and security management) to address all systems areas and operations to support all the Postbank beneficiaries.

11. Key recommendation to the committee

At a bare minimum, we recommended that the Postbank leadership must implemented the following through our engagements and various reports:

- Fill key IT vacant positions to ensure stability and Implement controls to prevent unauthorised access to the Postbank Oracle Databases
- Conduct effective independent security reviews / audits of key suppliers supporting critical Postbank systems
- Implement adequate controls around Joiners, Movers, and Leavers (JML) to ensure that the correct roles and appropriate access rights are assigned to individuals.
- Strengthen security controls (user access management, Change management and audit trails) within the Oracle database using enhanced database security software that could support additional controls such as data encryption, increased monitoring of key tables / columns
- Implement controls to monitor server activities (off the server activity logging). Undertaken on a remote secure server to capture all events, thereby reducing the chances of an attacker deleting or compromising logging events
- Implement effective controls that ensures robust and regular critical patching
- Implement effective controls on multi-factor authentication (MFA) for VPN accounts and reviews of who is maintaining access to the VPN management system.
- Implement effective controls on network segmentation that should restrict the ability to connect non-Postbank assets (such as laptops, desktops, and devices) to the Postbank network
- Effective Implementation of Multi-factor authentication (MFA) for access to critical systems to reduce reliance on choosing strong passwords, the chances of brute-forcing and/or credentials stuffing attacks on the network by potential threat actors.
- Ensure that adequate structures, processes and. practices were implemented for the governance of IT and ensure a sound IT control environment that is supported by a sound IT infrastructure

We therefore *request and recommend that the SCOPA should closely assess and monitor the proposed action plans by Postbank* to ensure adequate implementation so that all the cyber security risks can be addressed.

- To follow up on all action plans per entity to ensure AGSA's recommendations are tracked, and internal controls are strengthened, which will include:
  - Implementation for proper record keeping and reconciliations for all quarterly reports which will effectively feed into the financial statements; and
  - Compliance with regulations relating to procurement, contract management and performance information.

- Request a full detailed briefing by the accounting authority and the executive authority on the implementation of effective measures to decisively deal with the significant weakness reported, which have already materialised through the financial losses suffered, and how these are being addressed. The plan should not only focus on dealing with the current identified gaps, but also indicate sustainable preventative measures.

- Request the accounting authority, supported by the strategic leadership of the executive authority, to present a proper recruitment plan on how the remaining key vacancies (CEO, CFO ect) will be filled. The progress on the implementation of this plan must also be regularly reported to SCOPA to demonstrate the active and effective implementation and monitoring of the filling of these key vacancies. This will promote stability of leadership so that the appointed leadership can then focus on corporatising the operations for sustainability.

- Prioritise regular engagement with management on the consequence management processes for all these reported losses, including the IFWE. Leadership of the Postbank must also be clear on the processes they will follow to investigate and deal with these cases, including progress of cases lodged with SAPS and DPCI. These investigations must be conducted in a proper manner that will facilitate appropriate action being taken to enforce consequence management. The accounting authority should then report, through the executive on a quarterly basis to SCOPA, and therefore SCOPA should also continue to insistently request feedback on these matters, as it has done on other entities.