

State Mortgage and Investment Bank - 2024

1. Financial Statements

1.1 Opinion

The audit of the financial statements of the State Mortgage and Investment Bank (the “Bank”) for the year ended 31 December 2024 comprising the statement of financial position as at 31 December 2024 and the statement of income, statement of comprehensive income, statement of changes in equity and statement of cash flow for the year then ended, and notes to the financial statements, including material accounting policy information, was carried out under my direction in pursuance of provisions in Article 154(1) of the Constitution of the Democratic Socialist Republic of Sri Lanka read in conjunction with provisions of the National Audit Act No. 19 of 2018 and Finance Act No. 38 of 1971. My comments and observations which I consider should be report to Parliament appear in this report.

In my opinion, the accompanying financial statements give a true and fair view of the financial position of the Bank as at 31 December 2024, and of its financial performance and its cash flows for the year then ended in accordance with Sri Lanka Accounting Standards.

1.2 Basis for Opinion

I conducted my audit in accordance with Sri Lanka Auditing Standards (SLAuSs). My responsibilities, under those standards are further described in the Auditor’s Responsibilities for the Audit of the Financial Statements section of my report. I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my opinion.

1.3 Responsibilities of Management and Those Charged with Governance for the Financial Statements

Management is responsible for the preparation of financial statements that give a true and fair view in accordance with Sri Lanka Accounting Standards and for such internal control as management determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, management is responsible for assessing the Bank’s ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless management either intend to liquidate the Bank or to cease operations, or has no realistic alternative but to do so.

Those charged with governance are responsible for overseeing the Bank’s financial reporting process.

As per Section 16(1) of the National Audit Act No. 19 of 2018, the Bank is required to maintain proper books and records of all its income, expenditure, assets and liabilities, to enable annual and periodic financial statements to be prepared of the Bank.

1.4 Auditor's Responsibilities for the Audit of the Financial Statements

My objective is to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes my opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with Sri Lanka Auditing Standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with Sri Lanka Auditing Standards, I exercise professional judgment and maintain professional skepticism throughout the audit. I also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for my opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Bank's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the management.
- Conclude on the appropriateness of the management's use of the going concern basis of accounting and based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Bank's ability to continue as a going concern. If I conclude that a material uncertainty exists, I am required to draw attention in my auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify my opinion. My conclusions are based on the audit evidence obtained up to the date of my auditor's report. However, future events or conditions may cause the Bank to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

The scope of the audit also extended to examine as far as possible, and as far as necessary the following;

- Whether the organization, systems, procedures, books, records and other documents have been properly and adequately designed from the point of view of the presentation of information to enable a continuous evaluation of the activities of the Bank, and whether such systems, procedures, books, records and other documents are in effective operation;
- Whether the Bank has complied with applicable written law, or other general or special directions issued by the governing body of the Bank;
- Whether the Bank has performed according to its powers, functions and duties; and
- Whether the resources of the Bank had been procured and utilized economically, efficiently and effectively within the time frames and in compliance with the applicable laws.

1.5 Accounts Receivable and Payable

1.5.1 Payables

Audit Issue	Management Comment	Recommendation
<p>a) Instances were observed where the installments were received for EPF loans even after the settlement of such loans. Such payments received were credited to the “Customer Refund Closed Loan Account” and the accumulated balance of that account was Rs.17,378,814 for the year ended 31 December 2024. The corresponding balance in the preceding year amounted to Rs.25,241,363 and therefore a reduction of the balance by Rs.7,862,549 was observed when compare with the preceding year.</p>	<p>The balance as of 30.09.2025 is Rs. 8,641,877</p> <p>The bank has completed refunds for 65% of the outstanding balance as of September 30, 2023. During the year 2025, Rs. 869,571.40 was paid to 91 customers, and the Clearance of this balance is in progress.</p> <p>More than 2,000 letters were sent to all customers except those with balances below Rs. 2,500/-.</p> <p>Visited several Estates and raised awareness among customers to</p>	<p>Bank should take necessary actions to settle the remaining balance.</p>

expedite about the refund.

- b) Payments made by customers for their loan installments were credited to a ledger account named “Un Appropriated Loan Balance Account” without being credited to the relevant loan account of the customer and this is due to multiple reasons such as overpayments and part payments of the installments. The accumulated balance of that account as at 31 December 2024 was Rs.18,554,426. The corresponding balance in the preceding year amounted to Rs38,935,963 and therefore a reduction of the balance by Rs.20,381,537 was observed when compare with the preceding year.
- We are in the process of transferring unappropriated balances to relevant customer savings accounts. The balance as of 14/10/2025 is Rs. 3,497,227.08. Except for 4 cases (Value Rs. 1,693,347.54), Steps made to transfer balance unappropriated balances to customer savings accounts at the end of October 2025. Payments received for deceased customers and property vested customers are included in loan accounts until the final settlement.
- Bank should take necessary actions to settle the remaining balance.

1.5.2 Advances

Audit Issue	Management Comment	Recommendation												
<p>a) The Non-Performing Loan Ratio of the Bank as at 31 December 2024 was 29.13 per cent. However, the recoverability of EPF Loans are guaranteed by the Central Bank of Sri Lanka and therefore the Non – Performing Loan Ratio of the Bank which was calculated by excluding the EPF loans shows 17.07 per cent and this ratio was also above the Licensed Specialized Bank Industry Ratio of 11.2 percent. The details are given below.</p> <table border="1"> <thead> <tr> <th>Description</th> <th>31.12.2024</th> <th>31.12.2023</th> </tr> </thead> <tbody> <tr> <td>NPL Ratio (All Loans)(Mn)</td> <td></td> <td></td> </tr> <tr> <td>Total Loans and Advances</td> <td>42,205</td> <td>39,209</td> </tr> <tr> <td>Total Non-Performing</td> <td>12,293</td> <td>9,042</td> </tr> </tbody> </table>	Description	31.12.2024	31.12.2023	NPL Ratio (All Loans)(Mn)			Total Loans and Advances	42,205	39,209	Total Non-Performing	12,293	9,042	<p>The bank has made several steps to reduce NPL as per the Board-approved recovery action plan for the year 2025. Summarize the action taken by the Bank. The Loan Collection target has been given to all branch Recovery Officers to increase the stage 01 ratio</p> <p>Awareness of EPF loan collection and monitoring</p>	<p>Management should be continue to strengthen the monitoring and evaluation mechanisms to sustain the downward trend in NPL ratios.</p>
Description	31.12.2024	31.12.2023												
NPL Ratio (All Loans)(Mn)														
Total Loans and Advances	42,205	39,209												
Total Non-Performing	12,293	9,042												

Loans			from the Head Office. A
Non-Performing Loan	29.13%	23.06%	Special letter has been
Ratio (%)			posted to all banks' new
NPL Ratio (Excluding			EPF Loan customers on a
EPF Loans)(Mn)			monthly. Customer
Total Loans and	29,467	31,192	awareness has been
Advances			increased, and a banner is
Total Non-Performing	5,030	4,220	displayed at all branches.
Loans			
Non-Performing Loan	17.07%	13.53%	New loan disbursements
Ratio (%)			are monitored monthly to
			maintain NPL below
			1.0%.

17 Special recovery and Legal drive conducted as at 30.09.2025.

Declared June months of the year 2025 as the Recovery month of the Bank in line with the Recovery plan for the year 2025.

142 loan facilities have been approved for reshedulements, and 96 have already completed the process.

25 facilities have been approved for Revival, and 20 out of them have been completed in the Revival process.

Legal Settlement plans are prepared by the Recovery Division, and 80 Settlement plans have already been entered to the court by the legal division.

NPL ration without EPF as of 30.04.2025 19.83%

and reduced 18.47% as of 30.09.2025.

b) Loan Administration (2015–2024)

The aggregated amount of loans and advances represented 75 percent of the total assets of the Bank as at 31 December 2024 and hence becomes the biggest asset of the Bank. The following observations are made regarding the loan portfolio growth, the Non Performing status and sector wise distribution of the loan portfolio of the Bank.

The bank loan portfolio represents nearly 50% for personal loan customers. This portfolio customers affected covid 19, inflation, income drop and cost pressure to increase NPL.

The management should further strengthen the established loan recovery mechanism. Steps should also be taken to ensure that the assessment of borrowers' creditworthiness is carried out properly, risk evaluation processes are adequately strengthened, and sufficient monitoring procedures are maintained after loan disbursement to minimize credit risk and enhance the overall quality of the loan portfolio.

i) The following table depicted the analysis of percentage increase of loans granted by the Bank and the percentage increase of non - performing loan portfolio of the Bank during the period of 2016 to 2024.

The bank has taken decision to curtail balancing the portfolio with other lending products in year 2022 and more focused to SME lending.

Loan recovery has been strengthened and control the NPL movement and increase loan monitoring.

Bank has steps to increase stronger credit appraisal, Central credit appraisal and Central Credit disbursement early warning and recovery system, pre and post loan disbursement and monitoring, and targeted portfolio management by sector and risk level.

Accordingly, Bank has able to manage the NPL of newly granted loans during last two years. NPL ratio of the loan granted in 2025 (Excl EPF) and 1.75%, as at the 30/09/2025.

Year	Increase in Loans Granted amount (%)	Increase in Non-Performing Loans (%)
2016	6.24	-9.0
2017	17.70	7.2
2018	4.02	-1.3
2019	5.15	2.5
2020	3.42	11.9
2021	4.23	-9.9
2022	3.86	15.3
2023	-0.27	17.7
2024	8.95	22.1

The percentage increase in loans granted amount showed an upward trend from 2016 to 2024, except in the year 2023. The percentage increase in non-performing loan portfolio (NPLs) of the Bank showed a continuous increase during the last 3 years period from 2022 to 2024 while recording the highest increase in year 2024. It was observed that, non-availability of an effective and strong loan recovery mechanism has affected on the increase of non - performing loans of the Bank.

In year 2023, the loan growth rate has declined by 0.27 percent, while the percentage of non-

performing loan (NPLs) has increased by 17.72 percent. In year 2024, while the loan growth rate increased by 8.95 percent, the NPL Ratio has also continued to increase and reached the maximum increase of 22.13 percent. This increasing trend of Non - Performing Loans indicates weaknesses in assessing borrower creditworthiness, inadequate risk evaluation, and insufficient monitoring procedures after loan disbursement.

ii) A comparison was conducted between the Licensed Specialized Bank (LSB) NPL Sector Ratio and the Non-Performing Loan (NPL) Ratio of the Bank, by both including and excluding EPF loans.

Year	LSB NPL	Bank NPL(without EPF) (%)	Bank NPL(with EPF) (%)
2015	6.4	-	29.4
2016	4.5	-	25.17
2017	4.3	-	22.93
2018	4.8	-	21.76
2019	5.5	7.7	21.21
2020	6.9	10.7	22.94
2021	6.5	9.2	19.84
2022	9.0	10.3	22.04
2023	10.6	12.3	25.99
2024	11.2	17.1	29.13

Bank Higher NPL due to,
 1. Nature of Loan portfolio
 High exposure to long-term housing and EPF-backed loans, which have longer recovery cycles and delayed cash inflows.
 Unlike some LSBs that focus more on short-term or secured commercial lending, SMIB's loan portfolio has limited immediate liquidity and slower turnover.
 Housing loans are more vulnerable to borrower income fluctuations and economic downturns.

The recommendation mentioned in above

- Bank's NPL ratio consistently exceeds that of the Licensed Specialized Banks (LSB) sector ratio in the past 10 years, which highlights significant concerns regarding its loan portfolio performance.
- In 2024, Bank's non-performing loan (NPL) ratio, excluding EPF loans, stands at 17.1 percent, which is significantly higher than the LSB sector ratio of 11.2 percent. Furthermore, when EPF loans are included, the NPL ratio remains alarmingly high at 29.13 percent. This trend indicates that bank is facing higher credit risk. To address this issue, the Bank should implement more stringent loan monitoring processes, and need to strengthen it's

2. Customer Segment and Socioeconomic Profile
 SMIB primarily serves middle- and lower-income groups, government employees, and retirees — segments with limited financial resilience.
 These borrowers are more sensitive to inflation, cost of living increases, and salary delays.

recovery efforts in order to reduce non-performing loans (NPLs) and align its performance with sector benchmarks.

Other LSBs may cater to institutional or SME borrowers with stronger repayment capacity or collateral.

3. Slow Recovery and Legal Processes.

EPF-based loan recovery depends heavily on the Labour Department's refund timelines, often causing long delays.

Legal proceedings for housing loans (e.g., mortgage bonds) are lengthy and resource-intensive.

4. Economic and External Pressures

Rising inflation, increased cost of construction, and higher interest rates after 2022 have reduced repayment capacity of housing loan borrowers.

iii) The distribution of the loan portfolio between the sectors such as SME, Agriculture, and other loan categories over the past ten years are depicted in the following table.

To grow the SME and Agriculture portfolio, Bank has recently collaborated with the Department of Development Finance-MOF and Coconut cultivation department by enabling many of re-finance loan schemes such as SMILLE III, Re-energizer, NCRCS, Kapruka Ayojana. Further more, the Bank has linked with the World Bank project on Climate Smart

It is recommended that the Bank expand its loan distribution across other product categories to promote a more balanced credit portfolio and Bank should also increase the granting of loans to the agricultural and industrial sectors in accordance with the provisions of its Act of Incorporation.

Year	Total Loans Granted (Mn)	Loans Granted under SME, Agriculture and Other loans categories (Mn)	SME, Agriculture and Other loans granted as a percentage of Total Loans (%)	Irrigated Agriculture program and two loan promotion session has already conducted.
2015	26,855	1,190	4.43%	
2016	28,530	799	2.80%	
2017	33,579	981	2.92%	
2018	34,930	1,077	3.08%	
2019	36,729	1,096	2.98%	
2020	37,984	1,137	2.99%	
2021	39,590	1,168	2.95%	
2022	41,117	1,974	4.80%	
2023	41,007	1,864	4.55%	
2024	44,678	2,404	5.38%	

(Sources: Annual Reports SMIB)

It was observed that, over the past ten years, the loans granted for SME, agriculture, and other loans categories remained below 6 percent of the total loan portfolio of the Bank. This loan percentage is significantly insufficient when compared to the bank's established purpose of supporting the development of agriculture, industry, and housing through financial and other forms of assistance.

1.6 Non-compliance with Laws, Rules, Regulations and Management Decisions etc.

Reference to Laws, Rules Regulations etc.	Non-compliance	Management Comment	Recommendation
a) State Mortgage and Investment Bank (Amendment) Act, No.29 of 1984	The Board of Directors is consisted with only six directors, though nine fit and proper persons should be appointed.	As of today, the Board of Directors consists of Eight members, including representatives from the Treasury and the Department of Livestock. Under the proposed reforms of State-	Stipulated number of directors by SMIB Act, should be appointed to the Board on time.

Owned Banks, SMIB has received 7 new nominations for the Board. With the completion of these appointments, there will be 13 directors in the Board, comprised of 11 Independent Directors and 2 non- executive directors.

- | | | | |
|--|--|---|---|
| b) Central Bank Directions No. 04 of 2022 – Section 7 | The bank has not fulfilled the minimum regulatory capital requirement of Rs.7.5Bn before 31 December 2024. | Proposal is being in progress at Ministerial level to absorb SMIB under fully own subsidiary of People’s Bank | The bank needs to take actions to fulfill the minimum regulatory capital requirement. |
| c) Central Bank’s Directive issued under Letter No. 02/19/306/0001/007 dated 16.04.2024. | The Central Bank has instructed institutions to refrain from incurring non-essential and/or non-urgent expenditures including advertising, business promotions, gift schemes, entertainment, sponsorships, travelling, and contesting for awards/trophies. The Bank has incurred a total cost of Rs. 30.43 million in year 2024 on marketing, gift, and promotional items. As per the approved procurement plan, estimated cost for marketing, gift, and promotional items is Rs. 8.03 million. It was | Future expenses related to these categories were restricted by the Bank. However, prior to the implementation of the CBSL decision, the Bank had already launched campaigns and made commitments with external parties. These campaigns were carried out accordingly. | The bank should comply with the directives issued by the Central Bank of Sri Lanka. |

observed that, an amount of Rs. 22.4 million had been spent in excess of the estimated cost, which represents an over-expenditure of 270 percent.

Additionally, special approvals for sponsorships were obtained in accordance with government circulars issued by the Department of Public Enterprises, following the

prescribed procedures. The Bank also informs the CBSL of all such expenses on a fortnightly basis, and all future expenses will continue to be incurred with prior intimation to the CBSL.

1.7. IT Controls

The Bank has upgraded its old system (AS 400) to Core Banking System (T24) with effect from 04 November 2024, and a private auditor has been appointed to perform the Data Migration Review, IT General Controls Review and Critical IT Application Control Review of the New Core Banking System. The following deficiencies were revealed during the cause of review.

1.7.1 IT General Controls

No.	Audit Issue	Management Comment	Recommendation
(a)	The facility to create system-generated User Access Matrix Report (user-wise option and option title report) is not available of new T24 banking system.	There is no out of the box report available in T24 system. Custom report development is in the development activity	It is recommended that the Bank develop enhancements to the new T24 system to enable the generation of user

		pipeline. Planel to resolve this issue before Q1 of 2026	Access matrix Reports.
(b)	Authorization limits were not assigned in accordance with the transaction value during the opening and closing of accounts through the new T24 banking system."	This is the current business practice. Branch Manager or Second officer are authorized to close FDs. Both positions are in the executive levels.	It is recommended that the Bank should implement a sound internal control framework through the new T24 banking system.
(c)	Monitoring and Logging		
(i)	The current monitoring and tracking of privileged access on servers is inadequate. Access to vendor-managed servers is facilitated through root passwords, yet there are no established controls to monitor or track these accounts effectively. Users with root access can implement changes to the system without generating logs or leaving traces of their actions. Furthermore, if root credentials are compromised, the lack of configured alerts means that such breaches may not be detected in a timely manner. This situation is further complicated by the involvement of external vendors in server management, which limits direct oversight and control.	We are in the process of implementing Privilege Access Monitoring (PAM) solution to control this vulnerability.(Q1 2026)	To enhance security, the organization should integrate a PAM tool with the SIEM system for comprehensive monitoring, ensure all root activities are logged and traceable, configure alerts for unauthorized access, conduct regular privileged access audits, and require vendors to follow the same server access security standards.
(d)	Network Security		
(i)	There is only one admin account with MFA enabled (Forti token) on a single device. Creating a single point of failure.	Acknowledges the audit observation. In collaboration with the vendor, at least two separate administrative accounts will be configured on the FortiGate firewall, each	To improve operational resilience, maintain at least two MFA-enabled admin accounts and securely store recovery keys or backup codes to ensure quick account recovery in

		with multi-factor authentication (MFA) enabled. Recovery keys and backup codes will be securely stored to ensure resilience in case of device failure or token loss. This remediation will be implemented by 30 November 2025.	emergencies.
(ii)	The firewall is not running a current firmware version and the firmware has some known vulnerabilities including: CVE-2022-35843, CVE-2022-41335, CVE-2024-46669, CVE-2024-52963, CVE-2022-42472, CVE-2023-46715 out of which one of these were rated as critical.	Acknowledges the audit observation. In coordination with the vendor, FortiToken MFA will be enforced for all VPN connections to strengthen protection against credential-based attacks. This remediation will be completed by 30th November 2025.	Upgrade the FortiGate firewall to the latest stable version promptly to address known vulnerabilities. If upgrading is delayed, document the reasons and inform the SMIB risk management team of any vulnerabilities to assess risks and apply compensating controls. Maintain a regular patch management process with continuous monitoring and timely security updates.
(e)	Active Directory		
(i)	No GPO-defined Deny logon locally, Deny logon through Remote Desktop Services, or Deny access from network settings exist for Schema Admins, Enterprise Admins, or Domain Admins on member servers and computers.	Acknowledges the audit observation. In collaboration with the vendor, the	In the Default Domain Policy, restrict Schema, Enterprise, and Domain Admins

Default Domain Policy will be updated under User Rights Assignment to restrict Schema Admins, Enterprise Admins, and Domain Admins from logging on locally, through Remote Desktop Services, or from the network, while maintaining a separate emergency “break-glass” group for controlled exceptions. This remediation will be completed by 30th November 2025.

- (ii) RC4_HMAC_MD5 is still enabled for Kerberos encryption. The domain controllers permit the weak RC4_HMAC_MD5 cipher suite alongside stronger AES options.

Acknowledges the audit observation. In collaboration with the vendor, Kerberos encryption policies will be updated to remove RC4_HMAC_MD5 and enforce stronger algorithms (AES128_HMAC_SHA1 and AES256_HMAC_SHA1) across all Domain Controllers. SMIB should align Kerberos encryption settings with best practices by disabling RC4_HMAC_MD5 and allowing only AES128_HMAC_SHA1 and AES256_HMAC_SHA1. After applying the changes, restart the Kerberos Key Distribution Center service on each Domain Controller and verify successful AES-based authentication.

- | | | |
|---|---|--|
| <p>(iii) The review of privileged Active Directory groups identified excessive and unnecessary membership across the following:
 Domain Admins: Includes both user and service accounts that do not require domain-wide administrative rights (e.g., Administrator, togadmin, , iwf Workflow Management System, NAS Storage, Sayani Jayawardena, Vcenter HO, MIS Co- Banking, among others).Enterprise Admins: Contains users and service accounts that may not require forest- wide administrative control (e.g., Sasindu Sudasinghe, SMIB AML, DR NAS, Internal Web, Iromi Waduge, NAS Storage, Workflow Management System).
 Schema Admins: Includes non- administrative and service accounts (e.g., Workflow Management System,)These groups grant the highest levels of privilege within the Active Directory environment and should normally contain very few, tightly controlled accounts.
 Have been provided domain admins where it might not be needed.</p> | <p>Controllers. This remediation will be completed by 31st December 2025.</p> | <p>for all clients.</p> |
| <p>(iv) The Microsoft 365 environment is configured so that the default sharing option for files and folders is set to “Anyone with the link – Edit.” This means when users share content, links are created that allow unauthenticated, external access with editing privileges unless the user manually changes the settings.</p> | <p>Acknowledges the audit observation. In collaboration with the vendor, Domain Admin over-provisioning will be remediated by removing unnecessary accounts, applying least-privilege delegations, and introducing stronger privileged access controls. This remediation will be completed by 31st December 2025.</p> | <p>Prioritize remediation of Domain Admin over-provisioning by removing unnecessary accounts, applying least-privilege access, and using Just-In-Time or time-bound privilege elevation. Implement approval workflows for privileged access, perform quarterly access reviews, limit service account permissions to their needs, and use Group Managed Service Accounts (gMSA) where possible.</p> |
| <p>(iv) The Microsoft 365 environment is configured so that the default sharing option for files and folders is set to “Anyone with the link – Edit.” This means when users share content, links are created that allow unauthenticated, external access with editing privileges unless the user manually changes the settings.</p> | <p>Management acknowledges the audit observation. In collaboration with the vendor, file sharing settings will be reconfigured to restrict default sharing links to “Only people in your organization” with view permissions,</p> | <p>To enhance security and align with best practices, it is recommended to restrict default sharing to internal users with view-only access, apply expiration policies for shared links, and monitor or disable “Anyone” links to minimize unauthorized access risks.</p> |

- apply expiration policies, and monitor or disable the use of anonymous “Anyone” links. This remediation will be completed by 31st December 2025.
- (v) The Microsoft 365 tenant is configured with external sharing set to “Anyone” for both SharePoint Online and OneDrive. This setting allows users to share content publicly via anonymous links, without requiring authentication. Acknowledges the audit observation. In collaboration with the vendor, tenant-wide anonymous sharing will be restricted by enforcing more secure external sharing configurations, link expiration policies, and periodic reviews of external sharing activity. This remediation will be completed by 31st December 2025. To improve security, limit external sharing to authenticated or pre-approved guests, apply broader access only at the site level when needed, enforce view-only link expirations, and regularly review sharing reports for compliance.
- (vi) Legacy (non-modern) authentication protocols such as IMAP, POP3, and SMTP AUTH are currently enabled within the Microsoft 365 environment. These protocols rely on basic authentication, which transmits credentials in a less secure manner and does not support enforcement of modern security controls like conditional access or multi-factor authentication (MFA). Acknowledges the audit observation. In collaboration with the vendor, legacy authentication will be blocked at the tenant level, with documented exceptions managed through Conditional Access policies that enforce MFA and compliant devices. This remediation will be completed by To enhance security, block legacy authentication tenant-wide, allow only documented exceptions with MFA-enforced Conditional Access policies, and continuously monitor and phase out remaining legacy clients or apps.

31st December 2025.

- (vii) Endpoint security monitoring reveals 46 critical and 41 warning alerts across the enterprise infrastructure, indicating substantial gaps in endpoint protection coverage. This represents a concerning deviation from established security baselines and regulatory compliance requirements. Acknowledges the audit observation. All critical and warning alerts will be investigated and remediate, and all endpoints will be brought into compliance with the latest security policies. Automated health alerts will be configured for coverage gaps. This remediation will be completed by 31st December 2025. Promptly address all critical and warning alerts, ensure all endpoints are protected by Microsoft Defender with current policies, set automated alerts for incomplete coverage, and integrate endpoint status with SIEM for continuous monitoring.
- (viii) SMIB's Microsoft 365 mail flow configuration currently permits connections using deprecated Transport Layer Security (TLS) protocols, specifically TLS versions 1.0 and 1.1. This configuration creates unnecessary exposure to sophisticated attack vectors that specifically target weaknesses in older cryptographic implementations. acknowledges the audit observation. All Exchange Online mail flow connectors will be configured to enforce TLS 1.2 as the minimum acceptable version, and connections attempting to use TLS 1.0/1.1 will be rejected. Logging will be enabled to monitor and identify any systems still attempting deprecated TLS connections. This remediation will be completed by 30th November. The bank should enforce TLS 1.2 or higher for all Exchange Online mail flow connectors, reject TLS 1.0/1.1 connections, and enable logging to detect systems still using deprecated TLS versions.

2025.

(ix) Dormant privileged accounts were identified within SMIB Active Directory environment, including accounts such as “drnas” and “hostlip1,” which exhibit no recent authentication activity. These accounts retain elevated administrative permissions despite their inactive status.

Name	Last Login Date
-----	-----
NAS DR Center	29/10/2024 10:19
Vcenter HO	23/02/2025 15:24
Internal Web	23/12/2024 10:17
HO Slip	29/11/2024 09:28
DR NAS	13/03/2025 14:16

Acknowledges the audit observation. A comprehensive audit of Enterprise Admin and Domain Admin accounts will be conducted, with inactive accounts disabled or removed.

It is recommended to conduct a comprehensive audit of all Enterprise Admin and Domain Admin accounts.

Monthly privileged-account reviews, PIM enforcement for break-glass and high-privilege roles, and automated alerts for stale admin accounts will be implemented. This remediation will be completed by 31st December 2025.

Management should consider Disable or remove any administrative accounts that have remained unused for 90 days or longer, or have never been accessed.

Additionally implement monthly privileged-account reviews, enforce PIM for all break-glass and high-privilege roles, and automate alerts for stale admin accounts

(x) Overly broad membership in high-risk groups (e.g., Global Admins, SharePoint Admins) per exported CSV.

Acknowledges the audit observation. Administrative group memberships will be audited and restricted strictly to business-critical personnel. Collateral users will be moved to role-appropriate groups, and

Audit each administrative group and limit membership strictly to business-critical personnel. Move collateral users to role-appropriate groups. Leverage dynamic group rules to auto-exclude accounts not in designated departments or

dynamic group license tiers. rules will be leveraged to auto-exclude accounts not in designated departments or license tiers. This remediation will be completed by 31st December 2025.

(f) Physical Security

(i) Network switches are left unlocked and exposed. In 6th floor in SMIB premises it could be observed that the network switch in the hallway and the training room have unlocked switches.

acknowledges the audit observation. Network equipment will be secure by disabling unused ports, locking cabinets containing switches, and keeping access keys in a secure location. This remediation will be completed by 31st December 2025.

Secure the network equipment and disable ports that are not used. Lock the cabinets that contain network equipment and keep the keys in a secure location

(ii) There are gaps in reception security procedure where an identify of a person is not verified before granting access to the premises.

Acknowledges the audit observation. A reception procedure will be established to verify visitor identities, check IDs, and issue visitor passes before granting access. This remediation will be completed by 31st

Establish a reception procedure and follow it. Make sure the IDs are checked for visitors and visitors' passes are provided.

December 2025.

(g) Endpoint Security

- | | | |
|--|---|---|
| (i) The current Endpoint Security measures does not impose any restrictions on connections to external storage devices or other external devices. This oversight allows users to connect unmonitored and potentially insecure devices to the organization's network. | Acknowledges the audit observation. This risk will be addressed through the implementation of a Data Leakage Prevention (DLP) tool, for which procurement has already commenced. In addition, cybersecurity training for staff has already been initiated to strengthen user awareness and compliance. The issue will be fully addressed by 31.12.2025. | Management should deploy device control solutions to manage and whitelist approved external devices, implement monitoring and regular audits to detect unauthorized connections, and conduct employee training to raise awareness of risks and ensure compliance with external device policies. |
|--|---|---|

(h) Information Security

- | | | |
|---|--|--|
| (i) Internal applications including T24 use unencrypted protocols. Http is being used instead of HTTPS. | Acknowledges the audit observation. HTTPS will be implemented for all internal and external application communications by deploying valid SSL/TLS certificates and updating configurations to enforce secure connections. This remediation will be completed by 28th | Use HTTPS for all internal and external application communications, deploying valid SSL/TLS certificates and configuring applications to enforce secure connections. |
|---|--|--|

February 2026.

- | | | |
|--|--|--|
| <p>(ii) Vcenter backups are not encrypted.</p> | <p>Acknowledges the audit observation. Encryption will be enabled for all vCenter backups using strong encryption algorithms to ensure confidentiality of sensitive configuration and virtual machine data. This remediation will be completed by 31st December 2025.</p> | <p>Enable encryption for all vCenter backups using strong algorithms to protect sensitive configuration and VM data from unauthorized access or media loss.</p> |
| <p>(iii) At the DR site data center, it was observed SMIB has installed a standalone PC to act as a terminal to DR side infrastructure. However, this PC was found to;</p> <ol style="list-style-type: none">1. Run outdated OS with applications that are not required.2. Use an outdated version of anti-virus. | <p>Acknowledges the audit observation. The terminal's operating system will be upgraded to a supported version with regular security updates, and unnecessary applications will be removed to reduce the attack surface. This remediation will be completed by 31st December 2025.</p> | <p>Upgrade terminals to supported OS versions with regular security updates and remove unnecessary applications to reduce attack surface and enhance security and stability.</p> |
| <p>(iv) Use of obsolete and out of date antivirus (Symantec) on the terminal attached to the DR server.</p> | <p>Acknowledges the audit observation. The obsolete antivirus software will be replaced with a modern, actively supported solution to ensure</p> | <p>Use a modern, supported antivirus with current definitions, replacing obsolete software to ensure effective malware protection and policy compliance.</p> |

- effective malware protection. This remediation will be completed by 30th November 2025.
- (v) SSL is turned off on the EDB server, (SSL is set to off in the pg_settings) so all traffic (including passwords) goes unencrypted. Acknowledges the audit observation. SSL/TLS encryption will be enabled on the EDB server, with valid certificates installed and TLS 1.2 or higher enforced to secure all client-server communications. This remediation will be completed by 30th March 2026. To enhance EDB server security by enabling SSL/TLS (minimum TLS 1.2), installing valid certificates, and enforcing SSL for all connections. Review and revoke unnecessary super user privileges, applying the principle of least privilege and creating roles with only the permissions required for application functionality.
- (vi) Reviewing output from 'SELECT * FROM pg_user' revealed that 'T24prod' and 'swuser' have superuser privileges, which allows full control over the database. acknowledges the audit observation. Super user privileges will be reviewed and revoked from any role or user that does not strictly require them. Roles will be aligned to the principle of least privilege by creating specific accounts with only the minimum permissions necessary for functionality. This remediation will be It is critical to immediately review the assignment of super user privileges and to revoke it from any role or user which doesn't strictly need it; instead, SMIB should implement the principle of least privilege by reviewing actual operational requirements for accounts, and create specific roles with minimum permissions

- | | | | |
|--------|---|---|--|
| | | completed by 30th January 2026 | necessary for application functionality. |
| (vii) | It was observed in addition to the T24 database, the server also hosts other production and non-production databases (test, iswitch_pre_prod_db ect.). This mixed environment can lead to security vulnerabilities as non-production databases may not have the same level of security measures in place as production databases. | Acknowledges the audit observation. All non-production databases will be isolated onto separate servers, and environment classification policies with defined security baselines will be established to prevent future co-location. This remediation will be completed by 30th January 2026. | Isolate non-production databases on a separate server and establish environment classification policies and security baselines to prevent co-location with production systems. |
| (viii) | SMIB's current password policy mandates a minimum length of 8 characters with complexity rules enabled, enforces a 60-day maximum password age, a 2-day minimum age, remembers only the last 4 passwords, and locks accounts after 6 failed attempts (30-minute reset). While these settings meet the baseline requirements of PCI DSS (minimum of 7–8 characters, complexity, 90-day rotation, 6-attempt lockout) and NIST SP 800-53 (IA-5), they fall short of the more stringent CIS Benchmarks—particularly the recommendation for a 14-character minimum, password history of 24, and more conservative lockout parameters (3 attempts). Moreover, NIST SP 800-63B's latest guidance discourages arbitrary expiration periods in favour of risk-based resets and calls for screening passwords against known compromised lists, none of which are currently addressed. | Acknowledges the audit observation. Password policies will be updated to align with CIS, NIST, and PCI DSS best practices by increasing minimum length, expanding password history, adopting risk-based resets, implementing breached-password screening, and tightening lockout settings. This remediation will be completed by 30th April 2026. | SMIB should follow CIS, NIST, and PCI best practices by using 14+ character passwords or passphrases, remembering 24 previous passwords, adopting risk-based resets, implementing breached-password screening, and enforcing strict lockout settings while maintaining PCI requirements. |
| (ix) | Number of users configured to Kaspersky is 369, the number of active devices in the AD is 485 (excluding servers). | Acknowledges the audit observation. All | Ensure that all devices within SMIB have the |

- devices within SMIB will be validated against the IT asset inventory to ensure they are covered by the EDR/AV solution. This remediation will be completed by 28th February 2026.
- (x) Currently SMIB does not have comprehensive IT Asset inventory which captures all IT assets, including endpoint devices. The inventory that is maintained by the supplies division is maintained in a physical file, and includes all types of assets. Acknowledges the audit observation. A comprehensive IT asset inventory will be established and maintained through a centralized management system to ensure effective tracking, security oversight, and lifecycle management. Implementation has commenced and will be completed by 31st December 2025. SMIB should maintain a comprehensive, electronic IT asset inventory—especially for endpoints—using a centralized system like OCS Inventory or ManageEngine to improve tracking, security, and lifecycle management.
- (xi) In T24, when configuring user access, configurations can be done in EB.USER.ROLES and USER.SMS.GROUP to restrict functionality and access to users. However there are cases where restrictions on Menus (HELPTTEXT.MENU) where these users have all access in the ROLES and GROUP but their access are restricted solely from the menu. This approach is not actual access control enforcement. Acknowledges the audit observation. Functional access controls will be enforced at the IROLES and GROUP level to comprehensively manage user privilege and access. It is recommended to enforce functional access controls at the IROLES, GROUP level to comprehensively manage user privilege and access.

Notwithstanding the different menu made available all system users falls in to 8 EB.USER.ROLES?

'@AUTH'	47
'@AUTH.CR'	2
'@AUTH.HR'	2
'@COBUSER'	1
'@FULL'	80
'@INPUT'	154
'@VIEW'	23
ALL.PG	3

This will just prevent the user from seeing the options from the UI. The endpoints in the backend would remain active and commands can be sent to these endpoints and as there is no enforcement in the ROLES or GROUP these endpoints would respond to the request without a restriction.

- (xii) It was observed several T24 users doesn't have menu level restrictions imposed, and have access to all applications. With only functional restriction ('input', 'authorization') restrictions enforced. E.g. NIDHANA.867 was observed to have been granted '@INPUT' role; which has 'ALL.PG' access with, giving her access to extensive list application/function in both user and admin menus, including product builder.

privileges and control for specific applications, functions, and fields. This remediation will be completed by 30th January 2026.

Acknowledges the audit observation. Strict menu-level access controls will be implemented based on the principle of least privilege, ensuring users only have access to applications and functions required for their roles. Periodic reviews of user access rights will be conducted, and excessive permissions will be promptly rectified with enhanced monitoring of high-privilege activities. This remediation will be completed by 30th March 2026.

- (xiii) In a disaster scenario switching to the DR site needs to be done manually, and relies on a single outsource specialist. This creates a single point of

Acknowledges the audit observation. Disaster recovery Reduce reliance on manual disaster recovery by

failure, compromising SMIB's ability to guarantee the defined RPO and TRO. The reliance on human intervention introduces unpredictability that can undermine the reliability of disaster recovery.

processes will be enhanced by documenting procedures, cross-training additional personnel, and assessing automation options to reduce reliance on a single individual. This remediation will be completed by 30th March 2026.

assessing automated failovers, documenting DR procedures, and cross-training personnel to mitigate knowledge concentration risks.

- (xiv) Following a server shutdown event, the recovery process of vCenter and VMs infrastructure requires manual intervention. Additionally, recovering application services require manual startup by application vendor team and internal IT. Critical operational procedures and their sequence remain undocumented. Furthermore, review of the vendor agreements indicated that the external vendors essential to the disaster recovery process operate without RTO obligations in their service level agreements, creating unenforceable recovery timeframes.

Acknowledges the audit observation. Comprehensive documentation for recovery processes will be developed, including roles, responsibilities, and escalation procedures. Vendor agreements will be reviewed to incorporate enforceable RTO and RPO targets, and recovery task automation will be explored to reduce reliance on manual intervention. This remediation will be completed by 30th March 2026

SMIB should maintain detailed recovery documentation for vCenter, VMs, and applications, review vendor agreements to enforce RTO/RPO targets, and automate recovery tasks where possible to reduce reliance on manual intervention.

- (xv) In the event of a disaster where the DR site is used until the primary site is restored, there is no documented and/or tested procedure for executing the switch back.

Acknowledges the audit observation. A comprehensive step-by-step plan for transitioning operations from

Develop a detailed switchback plan for returning operations from the DR site to the primary site, ensuring all teams understand their

the DR site back to the primary site will be developed, documented, and drilled to ensure data consistency and coordinated execution.

roles and have access to the documentation for a coordinated recovery.

Policies and Governance

- (i) The current Cloud Security Policy contains multiple gaps that may impact SMIB’s cloud governance and security posture. Key issues include:
 - ✓ Incomplete service approvals: Section 5.3 lists placeholder text for approved cloud services, without specifying vendor names or service details.
 - ✓ Undefined risk assessment methodology: While the Risk Assessment and Treatment section mentions quarterly assessments, it lacks detail on methodology, tools, or criteria to evaluate and prioritize risks.
 - ✓ Omission of encryption and key management standards: The Technical Security Controls Requirements enumerate access-control mechanisms but do not reference formal encryption standards (e.g., AES-256) or key-management policies for data at rest and in transit.
 - ✓ Ambiguous incident reporting and escalation: The Security Incident Recovery section outlines daily/weekly reporting but provides no defined timelines or escalation paths for high-priority incidents.
 - ✓ Incomplete training program: Cloud user awareness training is prescribed quarterly, yet content, assessment methods, pass/fail

Since CISO is now available, this can be more streamlined

SMIB should revise the Cloud Security Policy by defining approved services, strengthening operational procedures with risk assessments and clear escalation paths, formalizing encryption and key management standards, implementing role-based cloud training, and developing a detailed exit strategy for secure service termination.

While CISO is currently available there was a period (from late 2024 to mid 2025) during this period, if an incident occurs the roles and responsibilities defined in the policies could not be filled. As such make sure there is proper succession planning

criteria, and training delivery have not been defined or implemented.

- ✓ Partial exit strategy: The Exit Strategy section references acquisition requirements but does not define specific steps, responsibilities, or criteria for safely migrating or decommissioning cloud services.

and in the policies define what actions to take in the case where critical personal like CISO are absent.

(ii) The current Vulnerability Assessment & Management Procedure document at SMIB exhibits several gaps that may impact the effectiveness and consistency of the vulnerability management program:

Since CISO is now available, this can be more streamlined

To strengthen SMIB's vulnerability management, tailor assessment frequency by asset criticality, standardize scanning tools and methodologies with CVSS scoring, set remediation timelines by severity, define reporting requirements, reference hardening frameworks, implement KPIs for monitoring, and clarify key vulnerability management concepts.

- ✓ Assessment scheduling is generic, with evaluations conducted "at least bi-annually" without differentiation between internet-facing, critical, or high-risk systems, and trigger events for ad hoc assessments are undefined.
- ✓ The procedure does not specify approved scanning tools, methodologies (e.g., authenticated vs. unauthenticated scans), or reference standards such as CVSS for vulnerability scoring.
- ✓ Remediation deadlines are ambiguous: the schedule table lists duration values without mapping them to severity levels, and severity ratings are not aligned with standardized frameworks.
- ✓ Report delivery timelines and formats are undefined, potentially delaying stakeholder awareness and remediation actions.
- ✓ System hardening guidelines reference baseline security standards but do not mandate specific benchmarks (e.g., CIS or vendor hardening guides).

- ✓ The procedure lacks metrics or KPIs to measure remediation timeliness or overall program effectiveness. Definitions of key vulnerability management concepts, including CVSS, CVE, and penetration testing, are missing.

1.7.2 IT Application controls review of T24 Core Banking System

No.	Audit Issue	Management Comment	Recommendation
(a)	Customer Modules		
(i)	<p>When a customer presents his new NIC (EIC), as a practice the BA verifies whether the customer is an existing customer by searching for his CIF with both the new and the old NIC numbers.</p> <p>However, it was noted that when it comes to the Customer creations screen, the system allows a new CIF to be created for a customer, who already has a CIF linked to their old NIC number, by using the new NIC. The same can occur vice versa when a CIF already exists with the new NIC.</p>	<p>We are search both (NIC & EIC) numbers before creating a CIF in the system for prevent this issue. How ever we have change Mnemonic to rectify this error.</p>	<p>The system should validate NICs and other identifiers to prevent duplicate records, prompting updates to existing customer information to maintain data integrity and improve efficiency.</p>
(ii)	<p>When a posting restriction is applied to an account this action requires authorization from an authorizer. However, if the user wishes to remove a posting restriction, they can do so independently, without needing approval from an authorizer.</p> <p>Furthermore, the system doesn't require a remark to be added when applying or lifting a posting restrictions.</p>	<p>Until removal authorization by an authorized officer, the restriction type is nor change in the system. All changes are under the dual control mechanism.</p>	<p>The system should enforce maker-checker controls, restrict access by roles, and maintain an audit trail to ensure authorized approval and monitoring of changes to blacklisted customer records.</p>
(b)	Fixed Deposit Module		
(i)	<p>The Treasury Department oversees the granting of special rates for fixed deposits, determining additional rates based on the deposit amount in consultation with an ALCO committee member. Once established, the rate is assigned to the customer, and instructions are sent to process the fixed deposit.</p>	<p>Agreed. In order to expedite the process the Branch Managers have delegated the authority to</p>	<p>It is recommended to modify the system to include an approval workflow that mandates a second-level approval. This process should involve the approval</p>

Communication between the Treasury and branches occurs via telephone. At month-end, a report detailing the special rates granted is presented to the ALCO committee, compiled from separate system reports generated by each branch. However, the current system lacks a process for additional approvals for special rates, with only standard entry and approval in place.

Notably, there are no limits on additional rates, allowing for excessive rates, such as a 100% increase, and leading to a total interest rate of 107%.

authorized the special rates offered by the treasury and the treasury department has the records of granting special interest rates.

Further, the approval of ALCO is given at the following ALCO meeting based on the information given by the treasury with in the prior approval of interest margin delegated to DGM and GM/CEO. Action will be taken to obtain a system generate report directly from the system for the special rates granted.

of either the Treasury Department or a member of the ALCO committee before special rates are assigned to customers

- (ii) It was observed that the system provides the option to change the customer who is the beneficial owner for a fixed deposit. Furthermore, an individual customer's CIF can be updated for a corporate customer's FD. However, this option requires approval. Current approver is a JEO. Previous customer and the new customer is displayed in the audit tab upon authorization. However the information is not displayed in the activity log.

Agreed. Actions will be implemented to prevent modifying beneficial owners without a authorization of Branch Manager/ 2nd officer of the Branch.

However, It will be identified

It is suggested to prevent modifying beneficial owners for fixed deposits in the system.

when closing FD as the NIC and other required documents are attached with the FD mandates which are lodged in the dual control cupboard. Therefore, he can not closed and withdraw money from FD

- | | | | |
|-------|---|--|--|
| (iii) | It was observed that the system allows the creation of a fixed deposit (FD) loan for a customer who does not possess a fixed deposit. The system permitted the entry of the customer's savings account instead of the fixed deposit account. | Agreed. Actions will be taken to restrict the FD / Savings number field as mandatory. However, FD loans are granted after obtaining the original of FD certificates and it is underlien when granting an FD loans. It will be released after settling the FD loan. | It is suggested to restrict the FD /Savings number field only for fixed deposit arrangements. |
| (iv) | It was observed that the system does not require mandatory entry of Collateral Details and Collateral Rights after a loan is granted, allowing loans to be issued without verifying the fixed deposit (FD) percentage or locking the required amount. Consequently, loans can be approved for amounts exceeding the FD balance, as the loan amount is not validated against the FD. Funds are often disbursed immediately upon loan approval, even before collateral details are processed. This oversight permits the withdrawal of the FD while the loan remains active. According to company policy, if the FD is less than one year or interest is due monthly, the loan should be eligible for | Agreed. In order to provide an effective & efficient service to the customers, FD loan is processed & released without create the Collateral. Collateral is created after | It is suggested to eliminate the requirement for collateral details and collateral rights, and to implement strict validation controls to ensure that the loan amount is checked against the fixed deposit (FD) amount and the necessary amount is locked at the time of |

80% of the FD. For FDs over one year with interest due at maturity, the eligibility increases to 90%, with the necessary FD amount locked using the collateral rights screen.

releasing the loan and before processing the End of the Day on the same day.

granting the loan.

However, Matters will be discussed and actions will be taken as per the recommendation accordingly.

- (v) It was observed that the system allows a lesser loan amount to be entered in the executional amount field in the collateral detail screen.

Agreed. Actions will be taken to modify the system to automatically populate the FD amount, integrate rate and Term to display when creating the FD loan accordingly.

It is suggested to modify the system to automatically populate the loan amount in an uneditable field in order to keep control in the loan amount

(c) Savings Module

- (i) During the savings account opening process, the system does not validate whether the required minimum balance has been deposited. For instance, for a savings account type where the minimum balance is set at LKR 1,000, the system still allows the account to be opened with as little as LKR 100, without generating any error or warning.

Since there are few promotion introduced in time to time specially for the Minor savings, the accounts are able to opened with the amount less than the minimum required amount and it is required a authorization manager or authorize officer.

Enforce minimum deposit requirements at account creation, allowing a monitored grace period with alerts and follow-ups if needed.

However, the

Bank charges will be deducted if there is no minimum balance maintained.

(d) Treasury Module

- (i) The system has fields to enter the deposit value and the rate, this manual calculation is still being performed. So that it was observed that the rates for treasury bills are calculated manually using an Excel formula to determine the rate based on the maturity value and the deposit value.
- Development of system for Treasury function was not covered in the RFP on core banking system. However, implementing agency has developed current system on free of charge to record transaction relating to treasury activities base on volume of transactions. Since this has been developed under the loan module, it is required to input the calculated rates based on the requirement.
- Modify the system to include automated calculations for treasury bill rates based on the entry of deposit value and maturity value.
- (ii) It was observed that the rate is not a mandatory field when entering treasury bills in the system. If an entry is added without assigning a rate, the treasury bill is still processed as scheduled without accruing any interest. However, the entry of treasury bills requires authorization.
- Data entered in to the system is verified under a dual control system, and the core banking team has confirmed that the rate field can be set as a mandatory field based on the requirement.
- It is suggested to modify the system to make the Rate field mandatory.

(e) Lending Module

- | | | | |
|-------|---|--|--|
| (i) | During our review, it was observed that additional charges that need to be recovered from customers are populating in the system, but sometimes the amounts can be incorrect, leading the Banking Assistant to enter the correct amount manually. Although SMIB has standard amounts defined for these charges, they are not configured in the system. Once the customer pays the charges, the payment is not reflected in the system but is instead maintained manually in a physical file as a payment slip. Customers typically pay a total amount, and the system does not track which charges have been recovered and which have not | Reply relating (i),(ii),(iii). Needs detail discussion with relevant business units before giving a feedback as these are current operational practices/system functionalities | Ensure that the standard amounts for additional charges defined by SMIB are properly configured in the system. This will help automate charge calculations and reduce the likelihood of errors in manual calculation. |
| (ii) | During the review, it was observed that after the Pre-Disbursement Officer's approval, a voucher should be created for the loan disbursement. During the loan arrangement creation process, the disbursement amount can be entered manually. The system allows entry of an amount higher than the approved loan amount. | | Integrate the loan arrangement creation process with the loan approval screen to automatically retrieve and display the approved loan amount. This will help minimize the risk of manual entry errors. For EPF loans, the disbursement amount can be automatically calculated based on the approved disbursement percentage. |
| (iii) | During the review, it was observed that SMIB sends reminder letters to customers who default on rental payments. If a customer does not pay for 1 month, they send a 'White Notice.' If the customer does not pay for 2 or 3 months, they send a 'Green Notice,' and if the customer does not pay for more than 3 months, they send a 'Red | | Develop a feature within the system that automatically generates reminder letters based on the customer's payment status. This should |

Notice.’ The reminder letters are in pre- printed format. Recovery Department users receive the details of defaulted customers on a USB drive and take it to the IT Department, where they have a printer to print the customer details on the pre-printed letters.

include predefined templates for 'White Notice,' 'Green Notice,' and 'Red Notice' that can be printed directly from the system.

1.7.3 Data Migration Review

No.	Audit Issue	Management Comment	Recommendation
(a)	Planning Strategy and Documentation Issues		
(i)	<p>The BTE report noted significant gaps in the Data Migration Work Plan, particularly in go live readiness. Documentation of the migration process, conversion scripts, and mapping artifacts was incomplete, and the plan did not provide a detailed activity breakdown, task dependencies, or clearly defined data sign off responsibilities. These factors increased risks to project preparedness and timeline control, with potential for delays and unclear accountability. The limited documentation also reduced the ability to evidence the effectiveness of the migration strategy and governance, thereby elevating operational risk.</p> <p>SMIB’s Management Response of BTE observations: ‘The Steering Committee has acknowledged that while formal documentation and planning processes were limited, the adaptive approaches used by the project teams such as iterative corrections, repeated mock runs, and oversight—were deemed sufficient for enabling a successful migration. They confirmed that the risks highlighted in these observations were understood and consciously accepted as part of the migration process.’</p>	<p>Detailed documentations were not done due to the limited time factor and more focus towards critical project activities. But all critical areas were adequately documented and all the risk areas are well discussed at the steering committee meetings with necessary precautions in place which leads to a successful implementation of the project</p>	<p>Prioritize comprehensive strategies, thorough documentation, and contingency plans during data migration to reduce risks, enhance transparency, ensure accountability, and improve operational resilience and compliance, leading to a more successful migration.</p>
(b)	Trial Balance Discrepancies		
(i)	<p>Initial reconciliation of the trial balance with the product portfolio from the source system showed a difference of 843,327,451.10. This difference was later reconciled and brought down to an un reconciled deference of Rs. 1,554,099. This</p>	<p>A long-standing unreconciled difference existed between the General Ledger</p>	<p>Conduct an internal review to identify the cause of the discrepancy, document the</p>

discrepancy cannot currently be traced to specific transactions or balances and will be treated as an accounting adjustment at year-end. The lack of alignment in financial data raises concerns about the accuracy and reliability of the migrated data, which is crucial for operational integrity and compliance.

and schedules due to unidentified contract discrepancies in the AS400 system. Despite this, the Steering Committee approved the system migration, permitting a variance tolerance of up to Rs. 2 million.

findings thoroughly, and retain them for future reference and compliance, providing clarity and a resource for similar issues.

2. Financial Review

2.1 Financial Result

The operating result of the year under review amounted to a profit of Rs. 157,798,019 and the corresponding loss in the preceding year amounted to Rs. 1,164,780,667. Therefore improvement amounting to Rs. 1,322,578,686 of the financial result was observed. The reasons for the improvement are significant increase of the net interest margin and the increase in fees and commission income.

2.2 Trend Analysis of major Income and Expenditure items

Analysis of major income and expenditure items of the year under review as compared with the preceding year with the percentage of increase or decrease are given below.

Description	Variance Increase/(Decrease) (Rs'000)	Variance (%)	Reason for the variance
Interest income	(1,733,481,992)	19	Decrease of interest rates of existing and newly granted loans and investments.
Interest expense	(3,340,372,415)	38	Decrease of interest rate on savings and fixed deposits.
Net fair value gain/(loss)	220,463,317	140	Value appreciation on unit trust investments.
Impairment charges	(20,502,296)	4	Significant increase in EPF

			loans that are not included in impairment calculation and decrease in the granted personal loans.
Income tax expenses/ (gain)	287,405,970	178	Profit incurred during the year comparing with loss of the preceding year.
VAT on financial services	239,861,414	4679	Taxable profit increased during the year comparing with preceding year.

2.3 Ratio Analysis

According to the information made available, certain important ratios of the Bank for the year under review and the preceding year with comparison to the Sector Ratios are given below.

Description	Sector Ratio (2024) (%)	Bank Ratio (%)			
		2024	2023	2022	2021
Profitability Ratio					
Return on Average Equity (ROE)	7.72	0.59	-16.82	3.17	4.11
Return on Average Assets (ROA)	0.45	0.28	-2.01	-0.16	0.76
Net Interest Margin (Percentage)	2.94	3.83	1.02	3.52	4.34
Capital Adequacy					
Basel 111 – Tier I (Minimum 7%)		19.28	18.81	18.81	21.91
Basel III –Tier I & II(Minimum 8.5%)		19.28	18.89	19.76	23.87
Asset Quality					
Non-Performing Loans and Advance (Including EPF)		29.13	25.99	22.02	19.84
Non-Performing Loans and Advance (Excluding EPF)	10.6	17.07	12.32	10.31	9.2
Liquidity Ratios					
Liquidity Coverage Ratio (Percentage) (100%)		104.79	175	148.1	115

3. Operational Review

3.1 Management Inefficiencies

Audit Issue	Management Comment	Recommendation
<p>a) Even though, the bank has been established for more than 50 years, the management has not yet been able to introduce at least ATM facilities for their customers, indicating a notable gap in service delivery.</p>	<p>An Arrangement has already made to implement ATM under secondary participant with Commercial Bank, Approval of Central Bank is awaited.</p>	<p>The Bank should prioritize implementing ATMs to improve customer service, accessibility, and align with modern banking standards.</p>
<p>b) Since the establishment of the Panadura branch in year 2016, the Bank has not established any new branches up to 2024. The branch network has seen no physical expansion over the past eight years, indicating stagnation in growth.</p>	<p>Even though bank has requested approval of Central bank for branch extension since 2017, CBSL has refused grant further branch extension due to shortfalls in minimum regulatory capital.</p>	<p>The Bank should create and execute a branch expansion strategy to strengthen market presence and drive business growth.</p>
<p>c) Bonus payment As per Board Meeting Minute No. 23.SP.05.14.01, the Board of Directors approved a one-time advance payment of Rs.100,000 for permanent employees and Rs.25,000 for trainee banking assistants, recoverable within six months from the provisions for the 2024 annual bonus. Subsequently, as per Board Meeting Minute No. 24.12.160.02, the Board had approved Rs.15 million in year 2024 to settle the outstanding advance payments granted in December 2023. Accordingly, it was noted that the Bank had indirectly paid a bonus to employees below Chief Manager grade for the year 2023, although the bank was in a critical situation with a loss of Rs 1,164,780,667.</p>	<p>The bank had the capacity to set off loan amounts against the financial status at that time. However, it did not have the ability to pay bonuses based on the financial situation of that period. Recognizing the importance of maintaining the morale and motivation of the operational staff, the bank decided to set off the loans for employees below the senior manager category. It has been demonstrated that the bank's current financial status is significantly better compared to the previous period. As a</p>	<p>It is recommended that any form of employee benefit, to be granted only after a thorough assessment of the Bank's financial position and in alignment with regulatory and governance requirements. Further clear policies and approval mechanisms should be established to ensure transparency and consistency in</p>

result, this decision has positively impacted the bank's business goals. decision-making.

- | | | |
|--|--|--|
| <p>d) The budget for the year 2024 was revised and approved by the Board of Directors on 23 December 2024 with the objective of minimizing variances. Hence, it was observed that the intended objectives of budget had not been achieved.</p> | <p>Budget for the year 2024 was amended on request of the Board of Director</p> | <p>It is recommended that the Bank strengthen its budgetary control and monitoring mechanisms to ensure that the intended objectives of the budget are effectively achieved.</p> |
| <p>e) The Bank has implemented the new T24 banking system with effect from 01 November 2024. However, the Bank continues to follow the outdated Operational Manual, as the revised Operational Manual has not yet been approved.</p> | <p>The Operational Manual has been thoroughly reviewed by the Heads of Divisions and was forwarded to the EIRMC meeting held on 17 October 2025. It is scheduled for submission to the upcoming BIRMC meeting and will be circulated thereafter.</p> | <p>It is recommended that the Bank expedite the review and approval of the revised Operational Manual to align with the new T24 banking system.</p> |

3.2 Operational Inefficiencies

Audit Issue	Management Comment	Recommendation
<p>a) Audit of fraudulent transaction on FD.A fraud was identified involving the closure and re-opening of fixed deposit (FD) accounts on May 9 and May 13, 2022. Specifically, three fixed deposit accounts, 001/25/0045363 (Rs. 1,145,884.78), 001/25/14242 (Rs. 1,835,069.53), and 001/25/13560 (Rs. 970,486.06) were closed, amounting to a total of Rs. 3,951,440. Subsequently, three new FDs were opened under account numbers 1/46/3207 (Rs. 1,142,000), 1/18/4540 (Rs. 310,000), and 1/18/4536 (Rs. 2,500,000), totaling Rs. 3,952,000. Both the data entry and authorization of these transactions were performed using the same user ID "FEDGA",</p>	<p>Currently, the Bank has taken steps to rectify and prevent such malpractices. Initially, most of those involved in fraudulent activities were interdicted, and inquiries have been launched against four employees. It is planned to complete these inquiries</p>	<p>It is recommended that the Bank strengthen internal control procedures related to document management and work allocation to ensure clear accountability and proper segregation of duties.</p>

assigned to employee number 443, in clear violation of internal control protocols which require segregation of duties.

Furthermore, all supporting documents related to the closure and opening of these fixed deposits were found to be missing, raising significant concerns regarding document handling and recordkeeping practices.

In addition, on the same dates, unauthorized fund transfers were carried out through slip transfer using the user ID assigned to employee number 703. A total of Rs. 1,141,950 was transferred to an account at Bank of Ceylon (Account No. 72026029) and Rs. 2,810,000 was transferred to an account at Hatton National Bank (Account No. 022020279305), both belonging to individuals outside the bank.

i) The occurrence of this fraudulent transaction can be attributed to deficiencies in both the establishment and implementation of the bank's internal control system.

- As per the letter dated 12 December 2024, from Staff Officer, it was revealed that when fraudulent activity occurred during May 2022, employees from other divisions were assigned to the banking unit due to high customer volumes. Fixed deposit applications, signed certificates, and related documents were removed from official files and transferred without proper record-keeping and some were sent outside the unit. These irregular practices raise concerns regarding the adequacy of data confidentiality measures and have led to the misplacement of important fixed deposit documents.

ii) Inadequate Human Resource Management

- The officer suspected to be involved in the fraudulent transaction, , has stated that she performed duties within the Banking Unit in

by November 2025.

In addition, as a further measure, the Bank has lodged police complaints regarding the criminal offences. The financial loss arising from these incidents has now been fully recovered. To prevent recurrence, the Bank has already implemented a core banking system along with special control mechanisms to mitigate such issues. These controls include increased password restrictions and other access limitations. The Bank is also working to strengthen internal controls through enhanced IT systems and operational procedures to ensure better oversight and risk management.

The Bank has taken steps to protect documents and now issues them only with written consent from a superior. Additionally, dual control procedures are currently implemented through the system to enhance security and oversight

Currently, it is not possible to repeat this process due to the new system restrictions, as the appropriate employment

February 2022 based on a verbal request from the Manager of the banking unit, without any formal written authorization. It indicates that the lack of adequate oversight by senior management. At this situation the bank has failed to implement an effective HR control mechanisms which shows impaired responsibility and prudence. The suspected officer, was assigned not only the opening and closing of fixed deposit accounts but also the reconciliation of fixed deposit general ledger accounts. It was evident that proper work allocation had not been carried out with proper delegation..

levels have already been deployed at the branches.

3.3 Procurement Management

Audit Issue

The total procurement expenditure of the Bank during the year 2024 was aggregated to Rs. 377.64Mn. From total procurements , a sample valued at Rs.306.28Mn was selected for audit review, and the following observations were revealed.

- a) In accordance with Section 4.2.1 of the Procurement Guidelines 2006, procurement activities anticipated for a minimum period of three years must be included in the Master Procurement Plan (MPP). However, the Bank has not prepared the MPP as stipulated in Section 4.2.1.

Management Comment

During that period, the bank was proposed for amalgamation and merging. Due to this uncertainty, long-term business planning was not practical, and the bank operated based on an annual action plan. Accordingly, the bank prepared a procurement plan for the year and took steps to obtain approval from the board, after which procurements were executed. Currently, the bank is in the process of revising its corporate plan and preparing a

Recommendation

It is recommended that the Bank finalize and implement the Master Procurement Plan in alignment with the revised corporate plan, ensuring compliance with the Procurement Guidelines.

master procurement plan for the upcoming year, considering the long-term existence and stability of the bank.

- b) The Bank did not prepare the procurement plan by using the prescribed format in accordance with Section 4.2.1 of the Procurement Manual 2006, and does not provide adequate information to act upon and measure the performance of planned activities.
- It was identified that there was a knowledge gap in preparing these documents and in adhering to the government procurement guidelines. Currently, the bank has conducted a comprehensive workshop to address this knowledge gap and has already taken steps to align with the new 2025 guidelines. Preparations are also underway to ensure compliance with the 2025 guidelines. Beyond procurement guidelines, management has implemented controls to oversee related activities, enabling the bank to fulfill its requirements effectively.
- Procurement plan should be prepared according to the prescribed format given by procurement guidelines 2006.

c) **Procurement of Hardware and other Internal Systems for the Core Banking implementation.(Bid reference No.SMIB/TD/2024/01/01)(Rs.85,489,440)**

- | | | |
|--|--|---|
| <p>(i) According to Section 2.8.4 of the Procurement Guidelines 2006, the Technical Evaluation Committee (TEC) for major contracts (DPC) should comprise from three to five members. However, two expertise and seven other members were included to the TEC for the aforementioned procurement, which does not comply with the stipulated requirements.</p> | <p>i)The entity has appointed additional TEC members as well as consultants to enhance the quality of service, exceeding the minimum required number of members. Such practice was not violated the cited direction</p> | <p>Management should ensure that the composition of the Technical Evaluation Committee (TEC) strictly adheres to the provisions of Section 2.8.4 of the Procurement Guidelines – 2006.</p> |
| <p>(ii)In accordance with Section 4.3 of the Procurement Guidelines 2006, even though the Bank is required to prepare cost estimation, including all associated costs, the Bank has not complied with this requirement.</p> | <p>ii) For each part of the project. The cost for the fundamental project estimation was conducted by SMIB. However, practical issues arose with the detail components, which should be taken into consideration at the earliest. Despite these challenges, the competition was maintained, and the project's financing was not affected, as separate board papers were submitted for approval and financial allocation.</p> | <p>Management should ensure that a cost estimation, including all associated costs, is prepared in accordance with Section 4.3 of the Procurement Guidelines – 2006 prior to initiating any procurement activity.</p> |
| <p>(iii)The value of the Bid security remained below the stipulated minimum threshold, and thereby indicating non-compliance with Section 5.3.13(a) of the Procurement Guidelines, 2006.</p> | <p>iii) and iv) Bid security of the procurement is determined based on estimated cost. Accordingly, the value of Rs.200,000/- due to</p> | <p>The Bank should ensure that the value of bid securities and performance securities obtained</p> |

- (iv) The value of the Performance Security remained below the stipulated minimum threshold, and thereby indicating non-compliance with Section 5.4.10(c) of the Procurement Guidelines, 2006.”
- practical difficulties of estimating cost of server with specifications required for the system and no financial impact to the bank.
- from bidders complies with the requirements specified in Section 5.3.13(a) and 5.4.10(c) respectively as per the Procurement Guidelines – 2006. Appropriate checks and controls should be implemented to verify bid security values during the bid evaluation stage.
- (v) The Bank had committed to provide an advance payment of fifty percent (50%) of the contract value, which is not in compliance with Section 5.4.5 of the Procurement Guidelines, 2006.
- v) Technical specification of the required server for T24 system need to be order from relevant manufacture by the vendor & vendor has confirm that it is required to pay 50% of advance of the total value of the server to place order. Under such situation bank has released 50% of advance by obtaining advance guarantee bond from the BOC.
- The Bank should ensure that advance payments made under procurement contracts comply with the limits specified in Section 5.4.5 of the Procurement Guidelines – 2006.
- (vi) It was observed that, the Bank has made a payment amounting to Rs. 41,445,209 on 03 June 2024, prior to signing of the contract agreement, which was formally executed on 07 July 2024. This action is not in compliance with the stipulated procedures of the procurement process.
- vi) Payment has been made to vendor based on acceptance of offer letter and advance guarantee bond agreement was signed subsequent to the payment with respect installation and setup of the server.
- The Bank should ensure that payments are only made after the contract is formally signed.

d) **Procurement of Supply , Installation ,Implementation and Customization of Core Banking Solution (Tender No.QT/185/2021) (Rs.196,798,385 exclusive of tax)**

i) According to the agreement with Dialog Broadband Networks (Pvt) Ltd, the bank had paid the 1st installment on 24 March 2023, amounting to Rs. 92,844,754 as 40 percent of the total payment. However, the bank had kicked off the core banking implementation on 18 July 2023. It was observed that, the bank had incurred a significant expenditure during the first six months of the year without receiving any corresponding services.

Bank has released 40% advance on contract value by obtaining of Bank guarantee on value equal to advance value from commercial bank. This agreement was with Dialog Broadband Pvt Ltd., a reputed company. The company entered into an agreement with SMIB to implement a core banking system at a specified price in LKR. However, due to a crisis situation, the currency value appreciated significantly, with USD 1 equaling approximately 202 LKR, which is roughly equivalent to 356 LKR for one USD. The total loss resulting from this appreciation was borne by the vendor.

It is recommended that the Bank implement a structured project readiness assessment prior to advance payments and formal project kick-off.

ii) In this procurement process, the bank had changed the payment schedule after selecting the bidder .Details are as follows.

During the course of the project, SMIB amended the payment structure beyond the initial agreement at the vendor's request, without altering the total project value. The payments were made in milestone installments, in accordance with the revised structure, with

The Bank should ensure that the payment schedule is not changed after the award of a contract, as such changes could unfairly disadvantage other competitive bidders and compromise the integrity and

Installment	As per Bidding Document	As per Agreement
1 st installment	20%	40%
2nd installment	20%	40%
3rd installment	20%	10%
4th installment	30%	5%
5th installment	10%	5%

However, the change of the conditions included in the tender document after award of the contract may compromise the fairness and integrity of the procurement process and therefore such changes should be avoided unless there is a compelling, documented justification and proper approval from relevant authorities.

approval from the Board. fairness of the procurement process.

Given the circumstances, it was not feasible to strictly adhere to the original payment terms due to the crisis. However, it is important to note that there was no financial loss to the bank, as the project was completed and handed over to the bank. Had these amendments not been made, the bank would have had to initiate a new procurement process, which would likely have resulted in a higher cost.

e) The bank has carried out five separate procurements with an aggregated value of Rs.556.18 Mn, All these procurements are aimed at achieving a common objective, of implementation of the Core Banking Solution.

i) In accordance with Section 2.4 of the Procurement Guidelines 2006, the appropriate procurement committee and appropriate TEC shall carry out the relevant aspects of the procurement process. An umbrella of procurement activities connected with common objectives shall be handled by the appropriate procurement committee. However, the Bank has not complied with this requirement.

These procurement activities are sequential, as each depends on the completion of the previous step. For example, the procurement of infrastructure cannot be accurately finalized until initial activities, such as the T24 implementation and pre-implementation setup, are completed. Additionally, a single bidder may not be

The Bank should ensure that all procurement activities aligned with common objectives are conducted in accordance with Section 2.4 of the Procurement Guidelines – 2006.

capable of supplying all required IT components, given the varied nature of the procurements. Due to these dependencies and the complexity of the project, it is not possible to estimate all procurements at the outset. However, the entity was able to proceed with separate procurements based on specific requirements, utilizing the thresholds of the DPC (Departmental Procurement Committee) for major procurements. This approach ensures procurement activities are managed effectively according to project needs.

ii) Although the procurements had been approved separately by different procurement committees, it was observed that the total value amounted to Rs. 556.18 million has considered as a single activity. When considered as a whole, this is a procurement process that should have been approved by the Cabinet Appointed Procurement Committee. However, the separated procurement activities of the core banking system have been performed through DPC major and DPC minor procurement committees.

Due to these dependencies and the complexity of the project, it is not possible to estimate all procurements at the outset. However, the entity was able to proceed with separate procurements based on specific requirements, utilizing the thresholds of the DPC (Departmental Procurement Committee) for major procurements. This approach ensures procurement activities

Management should ensure that procurement activities are aggregated and classified based on their total value to determine the appropriate approval authority, in accordance with

are managed effectively according to project needs. the Procurement Guidelines – 2006.

h) Audit of Procurements relating to Media Buying and Planning Service of the Bank for the year 2024(Rs.11,925,095)

The following observations were made during the audit conducted on the procurement process related to Tenders No. 37/2024, media buying and planning service, which was carried out for marketing and advertising purposes for the year 2024.

- | | | |
|--|--|---|
| i)The bank had processed media buying and planning service procurement activity by considering it as a service procurement by referring to the guideline on consultancy procurement, without selecting the correct procurement method. However, Audit is emphasized that the correct procurement procedure should be followed by the bank. | i)Agreed. However, it has not been adversely affected by the procurement decision. | Management should ensure that the appropriate procurement method is selected based on the nature of the goods or services being procured, in accordance with the Procurement Guidelines – 2006. |
| ii) The Bank had entered into agreements with three (03) agencies for a period of three years (from 30 December 2022 to 30 December 2025) to carry out all marketing activities. Further, the Board of Directors had authorized the Marketing Committee to select, from time to time, one of the aforesaid agencies for the execution of marketing activities, which is a non - compliance with Section 1.2.1(d) of the Procurement Guidelines, 2007.” | ii) The existing agreements are set to lapse in August and September. Afterward, the entity will implement a competitive bidding process to select suitable service providers. | The Management of Bank should be complied with Section 1.2.1(d) of the Procurement Guidelines, 2007 |
| iii) The marketing is a very dynamic field that is growing day by day, and being limiting to three marketing agencies prevent the Bank from getting the maximum benefits from the service of the industry experts. As well the decision taken by the Board of Directors may also adversely affect on fair, equal and maximum | iii) At present, no new assignments have been given to these service providers, and procurement is being conducted from the open market. | Management should ensure that procurement of marketing services is conducted in a manner that allows fair, equal, and |

<p>opportunity for eligible interested parties to participate in procurement.</p>	<p>open participation of all eligible service providers.</p>
<p>iv) According to Section 6.5.9 of the Procurement Guideline 2007 for selection and employment of consultants, key staff's qualifications and competence for the assignment shall be used as basis for evaluation criteria. However, Bank had not used the above mentioned criteria for its evaluation process.</p>	<p>iv) The service provider has completed the assigned tasks satisfactorily. In the future, based on the 2025 guidelines, proper procedures will be followed, supported by staff training. Management should ensure that the evaluation of consultants are carried out according to Section 6.5.9 of the Procurement Guidelines – 2007</p>
<p>v) As per the Board paper No.22/14/BD/(APP)/05 dated 30 December 2022, stated that an agreement should be entered into among the three agencies, framework agreement with agency named Digibrush Production (pvt) Ltd was made effective from 9 September 2023. It was observed that the management of the bank had been taken 9 months to implement the decision of the Board of Directors. Further it was observed that the General Manager had signed the above mentioned agreement on 3 January 2025 and a delay of 16 months was observed between the effective date of the agreement and the date signed by the General Manager.</p>	<p>v) Delays occurred due to requirements. The framework agreement was signed for three years to utilize when requirements arise. Projects should be signed as and when needed. The delays are due to this process. Management should ensure that decisions of the Board of Directors are implemented promptly and that all agreements are executed in a timely manner to avoid delays that may impact operations or create administrative and legal risks.</p>
<p>vi) In the Selection and Employment of Consultants, the suggested proposal validity period for contracts valued at Rs. 5 million or more but less than Rs. 20 million is 91 days. However, the Bank had specified the validity period in the RFP documents as 60 days, which is not in compliance with Section 6.5.7 of the Procurement Guidelines, 2007.</p>	<p>vi) Agreed. Corrective actions have been taken by management at this time. However, it has not been found to have a major impact on procurement. The Bank should comply with Section 6.5.7 of the Procurement Guidelines, 2007.</p>
<p>vii) According to Section 7.2.2 of the Procurement Guideline – 2007, minimum proposal preparation period shall be 28 days. Since the</p>	

Bank has submitted the bid document to suppliers, via email and not providing documentary evidence to audit it was unable to verify whether the Bank has provided adequate period for the proposal preparation.

vii) Agreed. This was sent via email. However, the soft copy could not be found at the moment. The procurement division has taken steps to follow the proper procedures moving forward.

The Bank should implement procedures to document and retain evidence of bid document issuance, including dates and delivery methods, to enable verification and demonstrate compliance with procurement timelines.

viii) According to Section 1.4.3 of the Procurement Guideline 2007 for Selection and Employment of Consultants, officials shall declare that they shall remain without a conflict of interest throughout the process. However, former head of marketing who is the member of CPCD (Media Buying and Planning service – 2024) has conflict of interest with one of the supplier (Digibrush production (Pvt) Ltd) who presented a bid for media buying and planning service. However, former head of marketing had not declared this conflict of interest at any stage of the procurement. It was observed that the former head of marketing has participated in the evaluation process which is violation of the Procurement Guideline.

viii) An inquiry was conducted by the internal audit division, which found that the marketing manager was suspected but could not be proven guilty. The inquiry was concluded at the time with remedial actions. Additionally, the matter raised by you was questioned and reviewed by internal audit; however, it was clarified and resolved. Management has taken steps to prevent similar issues in the future.

Management should ensure that all officials involved in the procurement and evaluation process declare any actual or potential conflicts of interest, in accordance with Section 1.4.3 of the Procurement Guidelines – 2007.

ix) The Letter of Award in relating to this procurement was not complied with Section 8.7.1 of the Procurement Guideline 2006.

ix) Agreed. The award letter was prepared based on recommendations from the Technical Evaluation Committee (TEC). Instead of stating the bid amount explicitly, the letter outlines the payment terms, conditions, and

Management should ensure that Letters of Award (LoA) are issued in compliance with Section 8.7.1 of the Procurement Guidelines – 2006.

services as specified in the bid proposal. However, it is strongly advised to adhere to proper procedures in the future.

- | | | |
|--|--|---|
| x) The attendance forms for the bid opening were not duly completed, as key details such as the title of the procurement, date, time, and location were not entered. Furthermore, no information was recorded in the bid opening minutes form and the financial information form. | x) Agreed Corrective actions have been taken to address procedural lapses, and the entity is committed to maintaining these improvements in future procurement processes. | The bank should ensure that all bid opening documentation, including the attendance forms, bid opening minutes, and financial information forms, are duly and completely filled out for every procurement activity. |
| xi) Bank had not entered into a formal contract agreement, which is not in compliance with Section 8.9.3(a) of the Procurement Guidelines 2006. However despite the absence of a signed contract agreement, a contract payment of Rs. 11,925,095 has been made on 18 September 2024. | xi) Agreed. A framework agreement was signed with Digi Brush Production (Pvt) Ltd., including the RFP and other terms and conditions. Contract management was carried out accordingly. Payments were made only after project completion, ensuring no financial loss to the bank. | The Bank should ensure that no payments are made to contractors without a duly signed and valid contract agreement. |
| xii) Furthermore, it was observed that throughout the entire procurement process, the value of the contract was recorded only in the invitation for proposal submitted by the contractor and was not mentioned in any other document such as | xii) Bid values are stated in the bid proposals and invoices. Payments have been made only after project completion, comparing invoices, the | Management should ensure that the contract amount should be explicitly stated in the letter of award, |

letter of award, financial information form, evaluation report, etc.. The only source from which the exact contract value could be verified was the voucher provided by the contractor. The lack of documentation raises serious concerns regarding transparency, accuracy, and accountability in the bank's procurement process.

framework agreement, and job performance to ensure that the bank has not suffered any financial loss.

evaluation report, financial information form, and any related procurement documentation.

- i) Under Tender No. SMIB/TD/2024/03/02, the Bank has outsourced Database Administration and System Administration services to VS Information (Pvt) Ltd for a period of six months, and under Tender No. SMIB/TD/2024/08/04 the Bank has obtained the services of a Software Engineer and Application Support Engineers from Millennium I.T.E.S.P. (Pvt) Ltd for a period of six months. , The Bank has re-procured Database Administration and System Administration services from VS Information (Pvt) Ltd for a period of one year. The following observations were made regarding the aforementioned procurement.

Tender No: SMIB/TD/2024/03/02 –

- i) The following deficiencies were identified in the bid opening process.
- The format for attendance at bid opening meetings was signed by only one member of Bid opening committee.
 - The format for observations of each bid was incomplete.
 - According to Section 6.3.6 of the Procurement manual, the format for financial information was not correct and complete.
- ii) The minutes of the Procurement Committee had not been signed by any members of the Minor Procurement Committee.
- iii) The Bank had not been complied with the Section 2(a) of the agreement signed with VS

Accepted. However, the final report was signed by the committee members and was prepared based on the unsigned procurement minutes. Accordingly, they have clearly given their consent to proceed.

Management should strengthen controls over the bid opening process to ensure full compliance with the Procurement Manual and established procedures.

iii) In the first phase, attendance is mandatory and explicitly stated in the signed agreement

The Bank should ensure that all terms and conditions of the agreement are fully complied

Information (Pvt) Ltd and Millennium I.T.E.S.P. (Pvt) Ltd.

However, attendance of the service providers had not been maintained for the contract period.

for that phase. with.

Attendance was documented in a security book a copy of which is attached.

iv) The Bank had made a payment of Rs. 12,070,775 in accordance with the Second Schedule, considering the provision of 'on-site' services. However, it was observed that the authorized officers had recommended and approved the payments without verifying attendance records or any other supporting documents to confirm that the service provider had properly rendered the services on-site.

iv) This period was critical for the project. It is confirmed by the Head of IT that this critical phase could not be completed without full-time service. Additionally, the completion of these tasks is a prerequisite for making payments. Without support services, the scheduled go-live would not have been achievable. Attendance records are maintained by security personnel and are attached for your reference.

Management should ensure strict compliance with all contractual terms and conditions as stipulated in agreements signed with service providers. Authorized officers should verify attendance records, service logs, or other relevant supporting documents before recommending or approving payments, particularly for contracts that stipulate 'on-site' service delivery.

Tender No: SMIB/TD/2024/08/04 - Outsourcing Service Database Administration and System Administration for a period of one year(5.11.2024-5.11.2025)

i) According to the Section 6.2.2 of the Procurement Guideline 2006, minimum period of bidding for a procurement performed under National Competitive Bidding (NCB) should be 21 days. However, the bidding period of this procurement process was only 16 days.

i) Accepted. To meet project requirements, the process was expedited by shortening the bidding period. Corrective measures will be implemented

Management should ensure strict adherence to the bidding timelines prescribed in the Procurement Guideline 2006,

to prevent similar issues in the future. The procurement process was conducted fairly, ensuring the selection of the most suitable service provider.

- ii) According to the Section 2 of the agreement with VS information (Pvt) Ltd, the description of working hours same as the above mentioned Tender No: SMIB/TD/2024/03/02. The Bank has made a payment of Rs. 360,000 for Database Administration and System Administration on a monthly basis since 5th November 2024 to 5th November 2025 for a period of one year, considering the provision of 'on-site' services. However, attendance was observed only from month of May 2025 onwards.

Onsite support was essential during the first six months to facilitate the projects go-live. After this period, onsite presence was no longer necessary. According to the RFP, prices were separately requested for remote support, indicating that further cost reductions could only be achieved through remote intervention, not physical deployment. As a result, financial benefits were realized for the entity. However, approval for payments was obtained from the AGM.

Management should ensure that payments to service providers are made accordance with the terms and conditions of the agreement.

During the second phase, onsite presence was deemed unnecessary, as reflected in the relevant documentation and the RFP. However, the clause is mistakenly included in the agreement the cost of onsite work even in the second phase. To verify attendance, a separate

sign-in register is now maintained.

3.4 Management of Vehicle fleet

Audit Issue

(i) In accordance with Section 12 of the Motor Vehicles Act, 1951, if a vehicle sold, the bank is required to transfer ownership to the relevant party. However, the motorcycle No. 128-7922 has transferred to a third party as per the letter dated 02 April 2012, signed by the Senior Manager (HR & Supply) and a Statement of Change of Possession of a Motor Vehicle (M.T.A.6 form) is also available in the vehicle file. However, the vehicle registration has not yet been officially transferred. Furthermore, there is no evidence in the file that the motorcycle was sold to the third party.

(ii) The Motor car bearing registration number 6-8937 (registered in year 1972) and motorcycle bearing registration number TU-7328 (registered in year 2007) are not physically present at the bank and any information had not been available in the bank regarding above mention two vehicles.

Management Comment

i) & ii)
According to the final accounts and the official documents sent to the Comptroller Department of Treasury, these vehicles no longer exist. The relevant documents are not available since they are over 12 years old. Currently, there are no available documents regarding these vehicles. Based on accounting practices, it is confirmed that the vehicles are fully depreciated. Given their age and non-existence, the vehicles should be disposed of by the bank.

Recommendation

Management should take immediate action to regularize and properly document the ownership and disposal of all bank-owned vehicles.