KPMG

CAMMA MICROFINANCE LIMITED

Management Letter
for the year ended 31 December 2022

Contents

1. Improve control over loan file administration

Observations

We noted several administrative errors from reviewing the selected loan files as follows:

(i) During our credit review, we identified there is one loan which does not input an accurate collateral value and two loans which do not update collateral value to the Morokot system according to its latest valuation. For instance:

Branch	Currency	Loan ID	Customer ID	Loan Amount (USD)	Outstanding Amount as at 31 December 2022 (USD)	Collateral Value Per Appraisal (USD)	Collateral Value Per Morokot System (USD)
HO	USD	LC22123000005	CU053716	500,000	500,000	716,336	1,137,136
HO	USD	LC22021800006	CU005404	40,000	36,666.67	53,768	53,566
KPS	USD	LC22040600004	CU026677	35,000	3,3926.76	51,200	28,000

(ii) From samples of loan files selected for review, we noted that the principal amount of certain loan ID were inaccurately input in the loan agreements. For instance:

Branch	Currency	Loan ID	Customer ID	Loan Amount (USD)	Outstanding Amount as at 31 December 2022 (USD)	Principal Per loan agreement (USD)
KPS	USD	LC21051100009	CU025905	25,901.05	22,063.81	26,262.05
KPS	USD	LC21052000014	CU023160	18,000.84	17,685.81	18,690.96

Implications

(i) The above weakness, if not rectified nor immediately addressed in the policy setting process, may put the MFI at risk in the collectability of loans. Unnecessary losses may be incurred if the entity fails to control and monitor its loan portfolio properly.

(ii) The mismatch between documents in loan agreement and the information in system can lead to invalidity of agreement signed by both parties.

Recommendation

Operation and credit department shall be more careful when filling information of customer into loan file and in system. The management shall review the loan file and cross check between each report in loan file before submitting to the committee for the approval. A periodic spot check on these loan files and recorded in system should be conducted to avoid error or missing of information.

1. Improve control over loan file administration (continued)

Management's response 31 December 2022

Action : Related to the issues finding as raised above, our Credit Department and branches have worked out and closed during the field work of Audit such as:

(i) We have already fixed the collateral value that our users recorded inconsistent between the system and loan assessment. We will also issue an internal instruction regarding the registration of collateral value from the assessment form onto the system which will be effective for implementation on March 2023 onward.

(ii) We have also completed updating the loan agreement that recorded the mismatching of loan amount compared to the system with client.

Responsible person : Credit Department and Branch Managers

Timing : March 2023 and continuity activities

2. Improve control over disaster recovery plan and drill test exercise

Observation

During the audit period, we noted that there was no disaster recovery plan (DRP) developed and test performed.

This issue was also raised in the previous year's audit.

Implication

Without a disaster recovery plan and drilling test exercise, it would increase the risk of the business disruption when it encounters a disaster or a significant incident. In the event of a disaster or business interruption, the Company would be unable to resume normal operations promptly, resulting in potential financial losses.

Recommendation

Disaster Recovery Plan should be developed and regularly tested to take account of any business interruptions within a time frame (Recovery Point Objective RPO and Recovery Time Objective RTO) acceptable to the management. Also, drill test exercises shall be performed at least once a year to ensure that there is no business interruption after the incident occurs.

Management's response 31 December 2022

Action	:	Implementation
Responsible person	:	Sim Chansea
Timing	:	Third week of December 2023

3. Improve control over user access management

Observations

During the audit period, we noted the followings:

(i) Super user accounts were granted to all IT staff in the Company.

(ii) There was no formal procedure to perform the review user access rights and status and the activities of super users.

The issues were also raised in the previous year's audit.

Implications

(i) Super user accounts are accounts with high level privileges and are able to perform actions critical to the functionality of a system. Having super user accounts granted to all IT staffs might lead the risk that the super user account can be used to perform any unauthorized activities beyond the business operation without being detected in a timely manner.

(ii) The absence of user access rights and status review procedure increases the risks of unauthorized and undetected activities over the Company sensitive information in term of creation, modification, deletion and manipulation. Then, management cannot identify and investigate the incident in a timely manner.

In the absence of a periodical monitoring procedure over the activities performed by superusers increases the risk that superusers could perform other activities than allowed and not being detected.

Recommendations

(i) As super user accounts are accounts with high level privileges, they should not be granted to all IT staffs in the Company. Super user accounts should be granted only to authorised personnel with appropriate position and approval by management.

(ii) The Company should establish a formal procedure to review users access rights, status and the activities of superusers. The procedure should be reviewed and approved by designated management.

Management's response 31 December 2022

Action : Plan

Responsible person : Sim Chansea

Timing : Third week of September 2023

4. Improve control over physical access

Observation

During the audit period, we noticed that the server room was not equipped with sufficient standard security equipment, and there was no authorized personnel list who can access to the server room approved by management.

The issue was also raised in the previous year's audit.

Implication

Insufficient implementation of server room security equipment may pose the risk that network devices or critical servers in the server room may be physically damaged or lose. Without approval for authorised personnel granted to server room in place, it may pose the risk that unauthorised access is not being detected and investigated on timely manner.

Recommendation

The Company should equip sufficient standard security equipment in the data centre. This applicable for both primary data centre and disaster recovery site. In addition to the current equipment, the following equipment should be equipped:

- Heat/water detector and humidifier
- Smoke detector
- Fire suppression system/fire distinguisher/fire alarm system
- Raised floor
- Visitor logbook

Furthermore, accessing to the data centre should only be limited to authorized personnel.

Management's response 31 December 2022

Action : Plan

Responsible person : Sim Chansea

Timing : Fourth week of September 2023

5. Establish formal organisation chart

Observation

During the audit period, we noticed that there is unofficial organisation chart established, yet there was no appropriate approval made management.

Implication

Without maintaining formal IT Organisation Chart will pose the risk that the Company cannot segregate sensitive duties among people in IT department.

Recommendation

The Company should develop and maintain formal Organisational Chart with personnel name and position for IT Department. That document must be reviewed and approved by the management level.

Management's response 31 December 2022

Action	:	Plan
Responsible person	:	Tith Vannarith
Timing	:	Fourth week of March 2023

6. Enhance password configuration

Observations

During the audit period, we noticed the following:

(i) The IT policy for password protection guideline did not include the requirement of certain password parameters as below:

- Password history remember: N/A
- Failed login attempts: 3 times
- Session time out: 15 mins

(ii) The password configuration for Morakot VB Core Banking System does not follow the password security standard.

Implications

(i) Weak password requirements in the policy may lead to insufficient password settings for the system. A weak password is easily detected and compromised to gain unauthorized access to the system.

(ii) Weak password systems may be exposed to malicious attacks that lead to unauthorized access to the systems. A weak password is easy to detect, and other people may detect the password if they know the username. In addition, without frequent password changing configuration, the password an get exposed to an outsider and undetected, which could lead to unauthorized access to the system.

Recommendations

(i) The password security requirement in the policy should be reviewed, established, and configured to follow industry best practice. At a minimum, the policy and password configuration in the system should contain the following settings:

- Minimum password length is at least 8 characters.
- Minimum password age or password change frequency is 90 days.
- Minimum password age should be more than 0 day.
- Password complexity should be enforced such as alphanumeric, special character, lower-case, upper-case character.
- Allow users to change password limit to 1 or 2 times per day only.
- Password history in enable to detect and prohibit password re-use at least 5 times; and
- Session time out 15 minutes.

6. Enhance password configuration (continued)

Recommendations (continued)

(ii) The Company should enhance the configuration of the password parameters to follow the requirements under the policy. If it is not feasible due to system constraint or technical requirements, the rationale and risk acceptance or deviation policy should be documented and approved by appropriate management.

Management's response 31 December 2022

Action	:	Plan
Responsible person	:	Sim Chansea
Timing	:	Third week of December 2023

7. Improve control over periodic data restoration test

Observation

During the audit period, we noticed that the Company has formal backup and data restoration procedure in IT policy; however, there was no data restoration testing performed and reported with management sign off.

Implication

Without performing backup data restoration, the management cannot ensure the availability of critical financial data when need for any investigation in the future.

Recommendation

As doing a manual backup, the Company should perform backup to support the task of backing up critical business data and have proper acknowledge sign off from respective staff from IT department should be obtained in the checklist. The Company should establish the data restoration testing to ensure that the data can be restored in the future for any reporting or investigation purpose. The restoration report should contain the following important minimum information:

- Backup data
- Status of restoration
- Server Reference
- Prepared by
- Reviewed and approved by
- Backup/ restoration date

Management's response 31 December 2022

Action : Plan

Responsible person : Sim Chansea

Timing : Fourth week of December 2023

8. Improve control over end-of day processing

Observation

During the audit period, we noticed that there was no formal end-of day procedure with proper sign off by management.

Implication

Without formal end of day procedure, the Company could not ensure that the daily end-of day was successfully run, and exceptions were identified and resolved appropriately.

Recommendation

The Company should establish formal procedure of end of day processing with proper approval by management to monitor the result.

Management's response 31 December 2022

Action	:	Plan
Responsible person	:	Sok Vibol
Timing	:	Third week of September 2023

Status of previous auditor's observations and recommendations

No.	Observations	Recommendations	Status
1.	**Develop formal policies/processes for managing changes to IT systems** During our review of IT policies, we noted that the Company in practice has procedures for managing changes to core-banking system, Morakot VB. However, these procedures have not been formalized and documented into IT policies and processes.	Management should revisit the current practice and formally document the Change Management policies and procedures for IT system. This should include, at a minimum, the procedures for the following: - requisition and authorisation of change requests - classification of change request - development of the change - testing of change prior to migration to production - approval of change for migration to production - migration of change to production environment - monitoring of changes implemented in the production environment	Implemented.

Status of previous auditor's observations and recommendations (continued)

No.	Observations	Recommendations	Status
2.	**Enhance control over monitoring activities of administrator accounts** Based on our review of monitoring access to Morakot VB, we noted that the Company has not established control over monitoring access to Morakot VB which includes: - Reviewing access violation to Morakot VB and supporting infrastructure; and - Reviewing activities of administrator in Morakot VB and supporting infrastructure.	We recommend the management to turn on and regularly review the access violation log of Morakot VB System. Based on this log, IT Department should periodically investigate the users with frequent account lockouts. The results should also be documented as evidence that such investigation was performed. Regularly review the administrator's activities in Morakot VB in order to check that all the activities performed by the administrators are authorized and valid.	Implemented
3.	**Develop business continuity plan and disaster recovery plan** We noted that the Company has established a recovery site but not yet developed a business continuity plan ("BCP") and disaster recovery plan ("DRP") to recover the system when incidents / disaster occurs. Currently, the Company only has process to test backup recovery quarterly.	We recommend the management to develop a formal BCP and DRP and the following items should be included in the BCP/DRP documentation: - Risk Assessment (RA) – documentation detailing the orderly process of identifying risks that may cause an interruption to the normal functions and operations of the Company and describing potential preventive and mitigation processes that could minimize them.	Partially implemented. Refer to management letter item #2.

Status of previous auditor's observations and recommendations (continued)

No.	Observations	Recommendations	Status
3.	**Develop business continuity plan and disaster recovery plan (continued)**	- Business Impact Analysis (BIA) – documentation identifying the time-sensitive, mission-critical areas in the organisation, the possible impact of a disruption to the organisation, and to determine the requirements for recovering disrupted mission-critical processes of the Company in the event of a disaster. - Business Continuity Strategy (per critical process identified) – documentation discussing the recovery options per critical processes that will be utilized as alternatives should the existing critical resources become unavailable as a result of a disaster. Associated costs and other information that are necessary to evaluate the alternatives should also be included. - BCP Testing and Maintenance – documentation discussing the test preparation, execution and result evaluation. - Critical IT and Non-IT Resources Information – list of all facilities, IT and non-IT equipment, furniture and fixtures that are essential to the critical processes. - Call Tree – is a hierarchical structure that represents team members and their notification sequence. This will provide a structure to ensure that all personnel are contacted in the event of a disaster.	

Status of previous auditor's observations and recommendations (continued)

No.	Observations	Recommendations	Status
3.	**Develop business continuity plan and disaster recovery plan (continued)**	In addition, the BCP and DRP should be tested regularly (i.e., at least annually) to ensure that all essential aspects of critical business operations, including logistical issues, have been adequately covered and that relevant individuals are fully aware of their responsibilities in the event of having to invoke the BCP, DRP.	Partially implemented. Refer to management letter item #2.
4.	**Enhance incident management procedures** During the audit, we noted that the Company has not developed a formal procedure for incident management. Incidents are received and supported by IT via email, phone call without tools or formal procedures to record and analyse.	We recommend the Company to develop a problem and incident management and monitoring policies and procedures. The policies and procedures should include the following at a minimum: - Process for identifying and classifying problems and incidents - Process for resolving problems and incidents and escalation to vendor support - Process for reviewing on a periodic basis the problems and incidents that are resolved and not yet resolved - Process for analysing the cause of problems and incidents and how to solve these problems and incidents if they will occur again	Implemented. Implemented

Status of previous auditor's observations and recommendations (continued)

No.	Observations	Recommendations	Status
5.	**Improve control over change management procedure** There was no formal documentation of changes made to the systems, and there was no user acceptance test performed to ensure the correctness of changes.	Managements should implement a change management policy and procedures for all systems (Morakot system, SQL database and Ubuntu server) that include at least the following: - Request and approval process flow including change requesting, approving, testing, and deployment approving and roll back plan. - Change impact analysis. - Authorized production change users (for example, developer should not have access to production environment). - Change request form that at least includes formal sign off change requester, approver, tester and deployment approver. - Test results and user acceptance testing (UAT) should be recorded and signed off by responsible management and the requestor.	Partially implemented. Refer to management letter item #3.

Status of previous auditor's observations and recommendations (continued)

No.	Observations	Recommendations	Status
6.	**Improve control over user access management** We noted as follows: (i) Super user accounts were shared among the IT team and management has no procedure to review their activities in the systems. (ii) There is no procedure to review the user access rights review and status and the activities of super user accounts.	Management should establish a regular access rights and access status review for all systems. The review should at least include verifying that no terminated employees still have active user accounts after effective resignation date and verifying that users' access rights are appropriate and in line with their current job functions. High privilege or super user accounts should be restricted to a specific user with a proper approval by authorized management. Moreover, management should have procedure to review users' activities. Moreover, the management should at least have the following procedures: - Using dual control password among the IT team for each of system layer such as core application, database and operating system supporting the core banking system or documenting a clear responsibility based on the skill set while their usage of those accounts are requested. - Documenting a clear responsibility based on the skill set while their usage of those accounts are requested. - Logging their usage activities and reviewing their activities daily/weekly/monthly based on the difficulty of activities log.	Partially implemented. (i) Partially implemented. (ii) Not yet implemented. Refer to management letter item #3.

Status of previous auditor's observations and recommendations (continued)

No.	Observations	Recommendations	Status
7.	**Improve control in server room environment** There is no sufficient controlling environment such as temperature meter, fire suppression, raised floor, proper approval of authorized personnel to server room, smoke detector, fire alarm and server room environmental checklist.	Server room should be at least properly equipped with smoke/heat detector, cooling system, raised floor, automatic fire suppressor, etc. A regular maintenance and reviewed on that equipment should be in place. List of authorized staff should be documented and reviewed on a regular basis while every visitor should be escorted. Logbook should be signed by each access to keep track of every individual access in and out to the data centre.	Partially implemented. Refer to management letter item #4.