PRASAC MICROFINANCE
INSTITUTION LTD

Management Letter

Year ended 31 December 2009

KPMG Cambodia Ltd
No. 2, Street 208
Sangkat Beoung Prolit
Khan 7 Makara, Phnom Penh
Kingdom of Cambodia

Telephone +855 (23) 216 899
Fax +855 (23) 217 279
Internet www.kpmg.com

Mr. Sim Senacheert
General Manager
PRASAC MICROFINANCE INSTITUTION LIMITED
#25, Street 57&294,
Sangkat Boeung Kengkang 1
Khan Chamkarmon,
Phnom Penh,
Cambodia

Our ref CMD/KSN/KLN/vy

Contact Kun Samnang

26 April 2010

Dear Sir,

Management Letter – Year ended 31 December 2009

We have audited in accordance with International Standards on Auditing the financial statements of PRASAC Microfinance Institution Limited ("PRASAC" or "the Company") for the year ended 31 December 2009, and have issued our report thereon dated 17 March 2010. An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on our judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, we considered internal control relevant to the Company's preparation and fair presentation of the financial statements 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 Company's internal control. Accordingly, we do not express an opinion on the effectiveness of the Company's internal control.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarised in the enclosed report.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of the Company gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The Company's written response to our comments and recommendations has not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

This communication is intended solely for the information and use of the audit committee, management, and others within the Company and is not intended to be and should not be used by anyone other than these specified parties.

Yours faithfully
KPMG Cambodia Ltd

Craig McDonald
Audit Partner

Contents

1 Following internal credit policies and procedures

Observations

From our review of samples of credit files and home visits, we noted the following:

(i) Some customers used loans from the Company for purposes other than those stated in loan contracts. Examples are as follows:

Customer's name	Branch	Purposes in the loan application	Actual uses
Say Sophak	Kampong Chhnang	Selling rice	Selling clothes
Chea Sophal	Kampong Chhnang	Farming	Refinancing to others
Ly Phyny	Kampong Chrey	Farming	Purchase of rice field for farming
Uy En	Ang Ta Saom	Purchasing taxi	Funding son to go to Korea
Sam Phieng	Ang Ta Saom	Purchasing a motorbike	Purchasing fertilizer
Sao Sarak	Kampot	Purchasing taxi	Selling clothes
Kan Vanthoeun	Kampot	Expand wedding service	Selling wood
Chhun Boeun	Kampot	Purchasing cows	Repaired kitchen
Ouch Sunly	Kampot	Purchasing pigs	Refinancing to other villagers
Noun Din	Kampot	Buy fishing boat	Borrowed on behalf of her aunt

(ii) Some borrowers have outstanding loans with other micro-finance institutions.

Customer's name	Loan account	Loan amount	Balance with other MFI
Kampong Chhnang			
Say Sophak	79-04045-2	KHR 1,000,000	Amret
Sun Vath	8G-00478-7	KHR 2,000,000	HKL & ACLEDA
Keo Sophy	8D-00136-2	KHR 2,000,000	Credit
Khiev Sarith	9W-00053-1	US$2,000	AMK
Takeo			
Suon Chanthy	8D-00502-3	KHR 4,000,000	Amret
Nai Buthun	9X-00002-5	US$12,000	ACLEDA
Kampot			
Nuon Din	8H-00008-7	KHR 5,000,000	ACLEDA Bank
York Kan	8D-00195-9	KHR 4,000,000	ACLEDA Bank, CHC, TPC and Sathaphana

1 Following internal credit policies and procedures (continued)

Observations (continued)

(iii) The credit manual states that the follow up of the loan status should be performed after 15 days or no later than 1 month after the disbursement and be followed up on a monthly basis by the credit officer. We were informed that the credit officers regularly follow up the loans outstanding, however the loan follow up reports were not always updated in the respective files. For instance:

Customer's name	***Loan account***	***Location***	***Name of credit officer***
Kampong Chhnang			
Chea Sophal	8G-00015-2	Kampong Chhnang	Tep Sothun
Kong Yoeun	87-02633-6	Kampong Leang	Sras Virak
Takeo			
Un Noem	70-00260-8	Kampong Chrey	Khat Nel
Nhep Run	8I-00217-7	Kampong Chrey	Nuon Savuth
Ruos Sophat	79-00965-6	Ang Ta Saom	Has Da
Un on	79-00966-0	Ang Ta Saom	Nguon Pao
Kampot			
Nget Dorn	9V-00128-8	Banteay Meas	Bun Hou
Seng Sokha	79-01715-8	Banteay Meas	Son Chandara

(iv) From our home visit, we noted the following sharing loans:

- Loan provided to Kong Sokheun, account # 9W-00047-7, CO: Pov Vanna in Kampong Chhnang, shared with her sister.
- Kul Rorn who is a member of the group loan amounting to KHR 4,100,000, loan account # 79-00965-6, which Ruos Sophat is the group leader in Ang Ta Saom Branch has borrowed KHR 1,000,000 and shared half of the loan amount with her neighbour.
- Mr. Sao Sarak, A/C No.9W-00085-5, Mr.Chhun Boeun, A/C No.79-00159-5 and Tim Sin, A/C No.8G-00173-1 in Kampot Branch, have shared the loan proceeds amounting to US$500, KHR 500,000 and KHR 1,000,000 respectively, with their relatives.

(v) Improve control over loan files

- In the client assessment form, the collateral information i.e. size of land/house is not properly documented by the credit officer (CO: In Somaly, Borrower: Soem Siyat, account # 9W-00009-8, in Kampong Chhnang Branch).
- The loan to Kong Sokheun, account # 9W-00047-7, CO: Pov Sovanna at Kampong Chhnang Branch, the ID number stated the collateral receipt issued by the PRASAC is not consistent with the ID number in the certificate of ownership.
- No certification from the chief of village on the ownership of the collateral pledged for the loan to Uon Phally, loan account # 79-00565-0, CO: Chan Chamnan, at Kampong Chrey sub-branch.

1 Following internal credit policies and procedures (continued)

Observations (continued)

(v) Improve control over loan files (continued)

- There is an amendment on the loan assessment form, for instance the collateral evaluation of the loan to Suon Channy, loan account # 8D-00502-3, CO: Poeng Chheng Leang at Ang Ta Saom sub-branch. However, there was no initial of the superior to certify the validity of the amendment.
- The loan to Chea Phai, account # 8D-00479-7 at Ang Ta Saom, the estimated value of collateral was not documented by the credit office, Poeng Chheng Leang.

Similar issues were also raised in the previous year's audits.

Implications

(i) to (iv) These examples indicate that the control over the loan disbursement to the customer is inappropriate and the credit policy is not being complied with, which may expose the Company to significant business risks.

(v) The inconsistency of information may result in less internal control over loan disbursement recording; this may cause difficulty for the management's review.

Recommendations

(i) to (iv) The management should ensure that credit policies and procedures as set out in the manual are strictly adhered to at all branch levels.

(v) The management should ensure that all elements of the Loan Agreement are recorded accurately. In addition, all data recorded in the system needs to be properly updated and reviewed by a superior.

Management's response 2008

(i) After loan disbursement, CO will conduct loan monitoring on the loan utilisation. In some cases clients were forced to pay back loans and some cases new business was accessed by the CO to evaluate the repayment capacity of the new business. But it was difficult to control the use of loan, particularly for small loans. However, the loan utilisation will be strengthening through loan assessment and monitoring after loan disbursement. The disciplinary action will be taken for non-compliance staff.

(ii) It is hard to protect clients from borrowing multiple loans since there is no credit bureau or other mechanism in place. However, multiple is not the problem if the clients are not over-indebtedness. To minimise the over-indebtedness, the Credit Officers are required to check at least two references for each client (it was enforced since February 2009).

1 Following internal credit policies and procedures (continued)

Management's response 2009

(i) It is hard to make borrowers using loan with the term and condition stated in loan application and agreement. To mitigate the credit risk from borrowers using loan with other purposes than those stated in the contract, staff capacity building is main thing to be assure that the borrowers are experiencing in loan purpose, the loan amount is match with the size of the business. In some cases when it was found that the borrowers used loan with wrong purpose stated in loan contract and if the risk related to the borrowers is high, the borrowers will be forced to pay back the loan.

(ii) It's hard to protect client not to more loan from different lenders. PRASAC's credit policy is not allowed to provide loan to borrowers if they are on debt with another lender more than KHR 500,000 in group or more than 30% of disbursed amount in individual loan. To reduce credit risk of borrowers getting more loan from many lenders, regular loan follow up will be done. To avoid of providing on debtors of other lenders, discipline action policy will be implemented against non compliance with set credit policy and procedure.

(iii) Loan follow up must be done in 15 days or not later than 30 days after loan had been disbursed. Every time of follow up the loan, credit officer must fill the follow up form and submit to sub branch manager to review and file it in the loan file. To assure that credit officer follow the loan, daily activities achievement will be recorded by credit officer himself and sub branch manager will ask for supporting document. To strengthen the compliance of this, disciplinary policy will be implemented in 2010.

(iv) It's hard to protect client from sharing loan to other even though credit officer, sub branch manager try to assess client and tell the disadvantage of sharing loan but some clients still committed. To avoid this, correct assessment of the size of the borrowers business is the primary action and regular loan follow up after finding is what to be done by credit officer. If the borrowers are high risk, the borrowers may be forced to pay back the loan.

(v) It is obligations of credit officer, sub branch manager, branch manager, and also credit department to review the information in loan document and supporting document. Before submitting loan document to sub branch manager credit officer must review all information whether they are right with supporting document. Before approving each loan sub branch manager, branch manager, credit department must review data and information in loan document with supporting document and evaluate whether the data and information content in loan document is correct and comply with instruction. If not the loan cannot be approved. To strengthen the compliance with credit policy, procedure and instruction disciplinary policy on non compliance will be implemented in 2010

2 Monitoring access to Programmes and Data

Observations

We noted the following:

- The information system ("IS") policy had not yet been approved by Management of Prasac.
- There is no formal procedure to add/modify/remove users in the Micro Banking system.
- The password complexity of Micro Banking system was not configured to follow standard practices due to limitation of the programme.

Similar issues were also raised in the previous years' audit.

Implications

- There is an increased risk of unauthorised access and modification of financial data due to errors and mistakes by end-users, the exploitation of system weaknesses by intruders and there is a lack of controls to detect weaknesses.
- Without setting complex passwords, there is a risk of unauthorised access and of passwords being stolen or hacked. It may also result in the system being tampered with and exploited for malicious actions.

Recommendations

- The IS policy and procedure should be approved by the management. The Company should conduct induction training regarding information security policy where all new employees are required to be aware of and adhere to IT Security requirements as part of day-to-day operations of the Company. Additionally, each new employee should be required to sign a form to confirm their understanding of the company's security policy before commencing work.
- The Company should establish formal user management procedures with the involvement of both MIS and other departments. Central to these procedures is the User Request Form which captures at a minimum, the following information:

    (i). Effective date

    (ii). Full name

    (iii). Username

    (iv). User level and department

    (v). Action: new/change/delete/other

    (vi). Action description

    (vii). List of systems and respective access rights

    (viii). System administration sign-off

    (ix). User department management sign-off

2 Monitoring access to Programmes and Data (continued)

Recommendations (continued)

MIS department should be responsible for management of these forms. A periodical review procedure should be conducted to ensure appropriate operating compliance.

- We recommend that Prasac periodically changes all passwords which are used to access the system. Best practice in password administration is as follows:
  a) Passwords should be changed at least every 3 months;
  b) Password length should be at least 6 characters;
  c) Passwords should be a combination of these characters: alphabet, numeric, and special characters; and
  d) Password changes would be better implemented by way of an automatic mechanism built-in to the software.

Management's response 2008

- The policy will be issued and started training to all the users along with new system from August 2009.
- The request form will be designed and implement from June 2009.
- The request form for new users in the Head Office was prepared, but the request for removal of the user from the system was not prepared for the resigned staff. The form will be designed and implement in May 2009.
- It was difficult to do so in the current system because it is stand-alone system, but it will be done frequently in the new system.

The access rights were automatically controlled by the server, however, the manual check will be implementation from May 2009.

Management's response 2009

In MB DOS System password length is fixed of only four characters and it cannot be increased. In Server domain password expiry (every six months) and minimum length (at least six characters) were set and controlled by domain controller in server.

3 Improving computer operation

Observations

We noted the following issues:

- Backup for critical information systems is performed once a month which does not follow industry best practice. The backup database of MB Dos was not periodically tested by MIS department in order to ascertain that the databases were available for restoring in case of urgent requirement.
- The issues or problems encountered on computer systems are reported by users to IT/MIS officers verbally and not logged and tracked to be able to identify critical or recurring errors for resolution process. This includes how and when the problem has been solved and who has implemented the correction on the system.

Similar issues were also raised in the previous years' audits.

Implications

- There is higher risk of unavailability or failure of backup media when recovery is required.
- It is difficult to ensure that all IT incidents are resolved in a timely manner.

Recommendations

- Regular back up of computer system information should be carried out daily, weekly, monthly and yearly. Backup media should be periodically tested and the test results should be logged for further review and follow up.
- IT incidents should be logged every time they are reported/requested by end-users and the status of IT incidents should be updated/reported to the management to ensure that all IT incidents are followed up and resolved in a timely manner. In addition, the IT/MIS department should utilise a structured method to receive user requests. Initially it is best to be implemented with a common mailbox containing all mail requests. The mail format can have predefined fields for the users to fill in.

Management's response 2008

- The monitoring of job processing will be improved with the new system implementation.
- The backup policy will be enforced from May 2009.
- The backup policy will be improved with the new system implementation.
- The back-up media was not used because it was complicated for restoring, therefore, the external hard disk was used to backup the whole data from the sever. However, there was no logbook to keep the activities. The logbook to keep track the backup and testing will be prepared and implemented in May 2009.
- The procedure will be including into the DRP.

In addition, the IT Audit Unit was already established in January 2009 to audit the IT, but it was not fully functioned yet. The number of auditors will be increased in late 2009 in order to have full capacity to conduct IT audit.

3 Improving computer operation (continued)

Management's response 2009

MB back up head office is off-site backup of branch/sub branch office. Where at branch/sub branch they do backup every day, every weekend and every months keep in safe and flash drive. Backup database of MB were used very often for verification purpose at HO and Branch Level.

After repaired computer system, IT department has PCs repair sign-off report that signed by users and IT staff that solved the problems.

4 Consider equipping the office with CCTV to safeguard vulnerable or high risk areas

Observation

The CCTV in the office has been installed; however, vulnerable or high risk areas such as cashier rooms do not have CCTV.

This issue was also raised in the previous years' audits.

Implication

Without CCTV in high risk areas, PRASAC could be exposed to the risk of the loss of important client documents, loss of money in the safe and unauthorised entry to the server room. PRASAC would also have no means of tracing who committed the action.

Recommendation

CCTV should be placed in all high risk areas. There should always be someone monitoring the CCTV footage to alert people when things go wrong in high risk areas.

Management's response 2008

PRASAC will consider the recommendation and study the costs, benefits and effects of installation of CCTV on the high risk areas.

Management's response 2009

We do not consider Cashier Room of Head Office as high risk areas because most transactions related with staff only and management will consider installing CCTV at branch level in high risk areas and in server room.

Status of the previous year's auditors recommendations

We have reviewed the Management Letter issued for the year ended 31 December 2008 and comment on the status of the recommendations:

No.	Auditors' recommendations - in the previous report	Status
1	**Following internal credit policies and procedures** The management should ensure that credit policies and procedures as set out in the manual are strictly adhered to at all branch levels. The management should ensure that all elements of the Loan Agreement are recorded accurately. In addition, all data recorded in the system needs to be properly updated and reviewed by a superior.	Partially implemented. Refer to item #1.
2	**Maintaining cash float limits** The Company should either take appropriate action to avoid cash floats exceeding the maximum limit or conduct a risk assessment to determine whether the risks related to maintaining a higher cash float are manageable. If so, they may consider increasing the approved limit for cash floats. In addition, a weekly cash projection report should be prepared and be updated daily for actual cash collections and disbursements to assist the branch in complying with the required cash float balances.	Implemented.
3	**Improving documentation of internal auditors' work** We recommend that all audit findings and issues should be referenced to the work papers and the audit programmes. In addition, a complete audit file should be produced whereby findings in the final reports can be traced to the working papers.	Implemented.
4	**Monitoring access to Programmes and Data** The Company could consider implementing the following initiatives to address the above deficiencies: (vi) The Company should conduct induction training regarding information security policy where all new employees are required to be aware of and adhere to IT Security requirements as part of day-to-day operations of the Company. Additionally, each new employee should be	Partially implemented. Refer to item #2.

No.	Auditors' recommendations - in the previous report	Status
	required to sign a form to confirm understanding of the company's security policy before commencing work. (vii) The Company should implement a formal procedure with appropriate forms for request for access and termination of access to the company network MB system. The form should be approved by the management, confirmed by the IT department and appropriately filed as evidence for later review. (viii) The list of all system users should be reviewed and signed off periodically by both IT and the management.	
5	**Improving computer operations** The Company should consider implementing the following initiatives to address the above deficiencies: ▪ End-of-day and end-of-month processing should be executed and monitored by authorised users and processing results should be logged after completion for further review and follow up. ▪ Daily backup results at branches and head office should be logged for further review and follow up. ▪ Backup media for head office should be rotated off-site so that backup media can be available when serious disasters happen on the main site. ▪ Backup media should be periodically tested and the test results should be logged for further review and follow up. ▪ IT incidents should be logged every time they are reported/requested by end-users and the status of IT incidents should be updated/reported to the management to ensure that all IT incidents are followed up and resolved in a timely manner.	Partially implemented. Refer to item #3.
6	**Consider equipping the office with CCTV to safeguard vulnerable or high risk areas** We recommend that CCTV should be placed in all high risk areas. There should also be someone monitoring the CCTV footage to alert people when things go wrong in high risk areas.	Partially implemented. Refer to item #4

No.	Auditors' recommendations - in the previous report	Status
7	**Estimating retirement benefit obligations** Necessary information should be kept and tracked and provision should be made in light of the information available. When the Prakas on implementation of pension plan becomes effective, PRASAC should take the necessary action to ensure compliance with the regulations.	Not applicable since the Company's policy is the provision for severance pay but not the retirement benefit.
8	**Preparing a formal internal audit follow-up schedule** A formal follow up schedule should be prepared to ensure that all the previous year's findings are being followed up.	Implemented.