PRASAC MICROFINANCE INSTITUTION LTD

INTERNAL CONTROL REPORT
FOR THE YEAR ENDED 31 DECEMBER 2007

PRICEWATERHOUSECOOPERS

PricewaterhouseCoopers (Cambodia) Ltd
124 Norodom Boulevard, Chamkarmon
Phnom Penh
Kingdom of Cambodia.
Tel : (855) 23 218 086
Fax : (855) 23 211 594

6 June 2008

Mr. Michael Temple
Chairman
PRASAC MICROFINANCE INSTITUTION LTD
#25, St 294 & 57, Chamkarmon
Phnom Penh, Kingdom of Cambodia

Dear Mr. Michael,

INTERNAL CONTROL REPORT
FOR THE PERIOD FROM 1 JANUARY TO 31 DECEMBER 2007

We have pleasure in enclosing our Internal Control Report following the completion of the audit of the Prasac Microfinance Institution Ltd ("PRASAC") for the period from 1 January to 31 December 2007, during which we examined certain aspects of PRASAC's system of internal control.

Prior to describing the control weaknesses, it should be noted that our role as external auditors is to express an opinion on the financial statements prepared by the management of PRASAC. This task was entrusted to us after the operation and activities were implemented. Therefore we are not in a position to ascertain and confirm the actual occurrence of events and project activities for which the internal control is being implemented. This is mainly because we were checking and verifying historical facts and data. It must be appreciated that the matters raised in this report came to our attention during the conduct of our normal audit procedures, which are designed primarily with a view to the expression of our opinion on the year end accounts. Our comments cannot, therefore, be expected to include all possible improvements in internal controls, which a more extensive special examination might reveal.

We have identified a number of areas where we believe it is appropriate for management to consider improvements to the accounting and control systems. Our recommendations have been set out in the attached report. The facts and our recommendations have been discussed with various responsible officials from PRASAC and their comments have been incorporated into the text.

We would like to take this opportunity to express our appreciation for the co-operation we received from all of PRASAC's staff during the course of our audit. We hope for the same support and assistance in our future audits.

Yours sincerely,

PricewaterhouseCoopers (Cambodia) Ltd.

Senaka Fernando
Director

PRASAC MICROFINANCE INSTITUTION LTD

INTERNAL CONTROL REPORT
FOR THE YEAR ENDED 31 DECEMBER 2007

TABLE OF CONTENTS

PAGES

PRASAC MICROFINANCE INSTITUTION LTD

INTERNAL CONTROL REPORT
FOR THE YEAR ENDED 31 DECEMBER 2007

1. CASH AND BANK

1.1 There is no CCTV in the office to safeguard vulnerable or high risk areas

Condition

We observed that there is no CCTV in the office to safeguard vulnerable or high risk areas such as the server room, accounting room, cashier room.

Implication

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

Recommendation

We recommend that CCTV should be placed in all high risk areas. There should also be someone always watching the CCTV footage to alert people when there are things which go wrong in those areas.

Management comments

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

Implementation date

October 2008

Individual responsible for the implementation

- Internal Audit Department Manager
- Finance Department Manager

1.2 No segregation of duties in safeguarding the petty cash vault

Condition

We noted that cashier can open the petty cash safe in her room alone. She holds both accesses to the entrance door and to the vault.

Implication

There should be the chance to commit fraud, and the money could be used for other purposes than PRASAC's purposes.

Recommendation

There should be segregation of duties over all safes that PRASAC hold.

Management comments

The petty cash is responsible by the cashier “HO” for daily cash payment transactions. Cashier takes cash float for the bank or cash reserve with the limited balance of 20,000USD and it is verified and checked at end of day transaction on daily basis by Treasury Unit Manager. Therefore, we do not see a need to have two staff hold this amount of cash for the moments. However, we accepted the recommendations.

Implementation date

July 2008

Individual responsible for the implementation

- Finance Department Manager
- Treasury Unit Manager

2. FIXED ASSETS

2.1 There are no remarks on disposal items kept in the office

Condition

During our physical count, we noted that disposal items were kept aside in the relevant department without a disposal register listing as a control. Only the person who controls each department knows which items were disposed of.

Implication

It is difficult to follow up which items have been written off, and which have not been. Disposal items are not under control because they are placed in an unidentified place.

Recommendation

We recommend that a disposal register list should be prepared. The disposal list should consist of critical information such as preparation date, disposal date, description of asset, tag number. More importantly, the fixed asset disposal register needs to be updated on a timely basis, and disposal items should be marked as disposal on the tag.

Management comments

We accept that the fixed assets disposed are not tagged with register number. However, the list of disposal of fixed asset is prepared when there are fixed asset disposal and these fixed assets were already tagged with registered number.

Implementation date

June 2008

Individual responsible for the implementation

- Finance Department Manager
- Management Account Unit Manager
- Administration Officer

2.2 A few fixed assets are not tagged and a few are tagged with the wrong code

Condition

We acknowledge that PRASAC has a procedure with respect to labeling fixed assets. However, during the performance of our physical verification of fixed assets at PRASAC Head Quarters, we noted that some fixed asset items are not tagged and some are tagged with a different tag code. They include:

No	Branch Code	New Code	Fixed Assets Description	Purchased/ Received Date	Purchased Amount	Comment
1	909	FA909510063	PRINTER DeskJet Color 1080	26-Nov-03	799,200	Wrong description 1180
2	909	FA909510104	Printer HP LaserJet2420	24-Aug-06	2,262,700	Wrong tag
3	909	FA909510095	Laptop IBM T43	28-Feb-06	7,767,200	No tag
4	909	FA909530081	Fire Alarm System	05-Jun-07	10,054,447	No tag
5	909	FA909530069	Receptionist Desk	27-Mar-06	3,059,250	No tag

Implication

Lack of tagging may cause difficulties in identifying the assets and, consequently, lack of physical control over the assets. Moreover, accounting for exact fixed assets might prove difficult in the absence of correct identification codes/tags.

Recommendation

Tagging PRASAC's assets is a key control to avoid misplacement or unauthorised use of these assets. For proper monitoring and to minimise the loss of fixed assets, we recommend that PRASAC should ensure that the procedures for labeling fixed assets are observed by PRASAC.

Management comments

The above fixed assets are not tagged with label, but they were now tagged label of all the above items since the verifications with auditors.

Implementation date

Quarterly verification on fixed asset is implemented from 2008.

Individual responsible for the implementation

- Finance Department Manager
- Management Account Unit Manager
- Administration Officer

2.3 PRASAC uses the fixed asset cycle to calculate depreciation

Condition

We understand that PRASAC estimates depreciation using declining balance method. Depreciation is calculated based on approved depreciation rates to match the cost with the benefit revealed. However, we noted that assets are depreciated based on the calendar year from purchase date and depreciation charges are spreading evenly throughout the relevant periods.

Implication

The current practice provides the inappropriate amount of depreciation for monthly information, interim and annual financial information due to cut off error while PRSAC uses declining balance method.

Recommendation

A standard depreciation calculating method using either the double declining balance or straight line methods should be used to calculate depreciation to get the appropriate reasonable result and proportionate result.

Management comments

PRASAC implement depreciation method based on FA cycle for calculating depreciation amount which is different from depreciation method based on physical year. As per discussed with audit team, the different amount is not significant, only around 3 million riel.

In order to eliminate the error and to calculate reasonable depreciation amount, PRASAC will change this depreciation calculation.

Implementation date

July 2008

Individual responsible for the implementation

- Finance Department Manager
- Management Account Unit Manager

3. PAYROLL

3.1 Non-compliance with government regulations on Tax on Salary ("ToS")

Condition

ToS was under accounted for and paid by PRASAC. As payroll tax is paid to the tax department on behalf of employees rather than withheld, it must be grossed up before tax calculation.

Implication

Failure to comply with the Tax Rules and Regulations with regard to ToS leads to the following penalties:

a. 40% of the total amount owed;
b. 2% interest per month; and
c. 5 million to 10 million Riels or imprisonment for a period of between one month and one year.

Recommendation

PRASAC should gross up the payroll amount before calculating ToS to avoid possible tax penalties which may be excessive. This would also indicate good practice of being in compliance with local law.

Management Comments

This procedure has been implementing since PRASAC transforming from the project into PRASAC MFI (i.e. 2005). The past two-year internal control reports produced by PwC did not provide us any comments on this non-compliance. However, the recommendation is accepted and PRASAC will change the method to be inline recommendation and tax rules.

Implementation date

June 2008

Individual responsible for the implementation

Human Resource Manager

3.2 Necessary information should be kept track of and retained for the purpose of estimating retirement benefit obligation

Condition

PRASAC's retirement and severance benefit is as follows:

- The age of retirement for male employees is 60 years old and 55 years for female employees.
- An employee who reaches the age of retirement or resigns before the retirement date is entitled to the following:

Year of Service rendered	Entitlement (Percentage to one month of current salary for each year of service rendered)
Less than 3 years	50%
More than 3 years and less than 6 years	80%
More than 6 years and less than 10 years	100%
More than 10 years	120%

- The differences between provision for retirement and severance benefits and realised amount will be charged to income statement when incurred.

We noted that PRASAC estimated the liability based on 100% of the employee's last salary of the year reported.

Implication

According to Cambodian Accounting Standard 37 – Provisions, Contingent Liabilities and Contingent Assets, PRASAC should come up with the reliable estimate of the provision for retirement and severance benefit obligation.

In order to produce a reliable estimate, provision should be estimated based on the some assumptions (based on the policy) such as staff turnovers, salary incremental rates, estimate of employment period of each staff, discount rate based on high-quality corporate bond, etc.

The current policy indicates that PRASAC has actuarial risk. Should Cambodian Accounting Standards adopt standard on employee benefit, the current policy might require PRASAC to involve independent actuaries to calculate the defined benefit obligation.

Recommendation

Necessary information should be kept and tracked and the provision should be made on the light of the information available.

When the Prakas on implementation of pension plan becomes effective, PRASAC should take necessary actions to ensure compliance with the regulation.

3.2 Necessary information should be kept track of and retained for the purpose of estimating retirement benefit obligation (continued)

Management comments

PRASAC will revise staff benefits that will easily keep track such as changing from defined benefits to contribution and to be inline with the "law on social security schemes for persons defined by the provision of the labor law".

Implementation date

Start from September 2008.

Individual responsible for the implementation

Human Resource Manager

4. BORROWING

4.1 All loan benchmarks should be regularly tested and reviewed by appropriate management

Condition

PRASAC has entered into, with some creditors, loan agreements which impose some loan benchmarks for some financial ratios. However, we noted that PRASAC has not monitored whether these ratios are within the benchmarking ranges as specified in the loan agreements and what actions shall be made on any unusual trends as comparing to the benchmarking factors.

Implication

Without a proper monitoring loan benchmarks, the PRASAC may not be aware of any unusual trends against benchmarks/key milestones that may cause PRASAC difficulties in obtaining new/additional financing from the creditors.

Recommendation

We recommend that the PRASAC should closely monitor and formalise the review of loan benchmarks as part of the financial management process.

Management comments

Most of the benchmarks given by the lenders were closely monitored, for instance there was one non-compliant benchmark found during the audit exercise and PRASAC communicated with the lender on that regard. The benchmarks are not covenant that requires complying with all the time. However, PRASAC accepted this recommendation and will develop a system to keep track all covenants and benchmark of lenders.

Implementation date

July 2008

Individual responsible for the implementation

- Finance Department Manager
- Treasury Unit Manager

5. INTERNAL AUDITORS' WORK

5.1 Internal audit (follow-up) working papers done by junior auditors should be reviewed promptly by senior auditors

Condition

We understand that during a client's procedures, all junior auditors' work and findings from fieldwork need reviewing by senior auditors. However, we noted that some audit working papers done by junior auditors after fieldwork took a long time (1 or 2 weeks) to be reviewed by senior auditors.

Implication

Delay in reviewing junior auditors' work may affect the quality of audit work. Audit work performed by junior auditors may not be adequate or not follow audit procedures and this may not be identified by a senior auditor in a timely manner. Furthermore, delay in reviewing junior auditors' work may cause the delay of audit reports, making the audit reports less useful by not providing information on time and the findings in the audit reports not being communicated to the management in a timely manner.

Recommendation

We recommend that junior auditors' work and audit working papers be reviewed promptly by senior auditors in order to gather all necessary information and findings to produce an audit report for management's review and action on time.

Management comment

Although, the review of junior auditors' works and working papers were not promptly reviewed, but the findings were recorded into the system in which the senior auditors can review the findings and issue the report within the timeframe. However, the recommendation is accepted and will be improved.

Implementation date

July 2008

Individual responsible for the implementation

Internal Audit Manager

5.2 Audit Reports should be reviewed promptly and action taken on them by Management

Condition

It is a formal procedure that the Internal Audit Report has to be sent to the Internal Audit Director for review prior to being submitted to the General Manager for approval. However, we noted from our audit that during this year audit reports took a long time to be approved by the General Manager.

Implication

The current treatment of the reports indicates poor monitoring control within PRASAC's control environment. Delay in the approval of audit reports causes delay in disseminating audit reports to relevant departments which may need information in the reports to plan or make decisions about day to day operation or to remedy weaknesses found by the internal auditor.

Recommendation

We recommend that audit reports be reviewed and approved promptly by Management and disseminated to relevant departments promptly so that each department manager concerned has the necessary information in order to plan or make decisions on operational matters properly.

Management comments

Although, the report was not promptly approved by the GM but the report was sent to the audited branches for comments before the issuance of the report. In addition, there was a exit meeting with the audited branches conducted by internal auditors, therefore, the findings were discussed and informed to the branch managers or sub-branch managers. In case there is fraud founded the case was immediate reported to the GM and the immediate action was took place. However, the recommendation is accepted and the report will be reviewed promptly by audit committee.

Implementation date

July 2008

Individual responsible for the implementation

Audit Committee

5.3 Internal audit should be recruited by and report to the Audit Committee/Board of Director, not General Manager

Condition

We understand that internal auditor recruitment is the decision of the General Manager and internal auditors are required to report to the General Manager.

Implication

Current practice may impair the independence of internal audit function. Furthermore, it would not be effectively sounded internal controls as the role of internal auditor is report to General Manager who is not independent from the day to day operation.

Recommendation

Considering best practice of good corporate governance, we recommend that the internal auditor function be recruited by and report to the Audit Committee or Board of Directors to ensure the independence, transparency and effectiveness within internal controls.

Management comments

The recommendation is accepted. During the financial year the audit committee was not established and functioning, therefore, the GM took that responsibility in order to ensure that the internal control is in place. The audit committee was created during the board meeting on 3-4 April 2008 and this committee will take over this task from the GM.

Implementation date

June 2008

Individual responsible for the implementation

Audit committee

5.4 No formal audit follow-up schedule

Condition

We understand that points from the prior period's findings ought to be followed up in the current period visit by the Internal Auditor. However, we noted that there is no formal follow up schedule produced by the internal audit department to draw attention to management's performance and provide evidence for previous work done.

Implication

Absence of proper preparation of a follow up report indicates improper management action. Management may be not aware whether previous recommendations have been implemented and will not be able to ensure that the action taken is sufficient.

Recommendation

We recommend that a formal follow up report should be prepared to ensure that the Branch Manager is aware of the status of the previous year's findings.

Management comments

In year 2007 IA department conducted follow-up audit, but internal audit didn't issue audit report because audit follow-up was found in the implementation of the previous recommendation. However, during year 2007, IA department paid attention on loan disbursement and repayment therefore audit schedule was not followed.

Implementation date

June 2008

Individual responsible for the implementation

IA department

6. INFORMATION TECHNOLOGY: GENERAL CONTROLS

6.1 Backup and recovery procedures

Condition

i. We noted an absence of documented procedures detailing day to day backup operations to ensure the completeness of the backup.

ii. There are currently no procedures in place to perform testing of backups to check for completeness on restoration, to ensure effective and timely recovery in the event that restoration is required.

Implication

i. Absence of documented backup procedures could have an impact on the availability of critical data as there are no agreed and clear instructions on backup strategy, storage of backup media and restoration procedures.

ii. Lack of proper controls to ensure the integrity and completeness of the backups performed, as well as successful recovery and restoration of the data backed up, could lead to potential business failure in the event that PRASAC is unable to rely on these backup CDs for emergency use.

Recommendation

To ensure availability of business data in a timely and efficient manner, we recommend that:

- Daily backup operations should be documented to provide step by step instructions to the IT staff on scheduling backups, labeling, storage and restoration of these tapes or CDs when required.
- A process of randomly restoring a backup tape to ensure the validity and completeness of its contents should be implemented on a monthly basis
- The weekly backup tapes should be stored at an offsite location with proper labels.

Management comments

Full backup are performed daily from Monday to Friday. The backup performed, labeled and checked for completeness by IT staff before kept in fireproof safe. Another external storage backup is replaced to continue the backup process for the following week. The draft procedure and policy is also in place and it will be finalised.

Implementation date

June 2008

Individual responsible for the implementation

IT Manager

6.2 Lack of a comprehensive IT Disaster Recovery Plan

Condition

We found that there is no Disaster Recovery Plan (DRP) in place to assure the recovery of business activities in a timely manner in the event of a major failure or disaster.

Implication

In the event of a disruption such as fire or equipment failure, the lack of a comprehensive Disaster Recovery Plan could result in severe disruption to critical business operations.

Recommendation

We recommend that management assess the criticality of all the applications and what a loss of the computer facilities would mean to the continuity of the business. An effective Disaster Recovery Plan should be developed that encompasses all elements likely to be affected by a disaster to ensure the continuity of all critical business functions during the recovery period.

It is essential that the plan be developed in a co-coordinated effort between system support and critical business functions.

A comprehensive plan should include, but not be limited to:

i. Objectives of the plan.
ii. Documentation in the plan regarding its development, review, and approval by management.
iii. A list of all authorised personnel to whom the plan will be distributed. One copy of the plan should be kept in a secure, offsite location.
iv. A list of key personnel and their functions in the disaster recovery/contingency plan.
v. Relevant threats to the system, their impacts, and their likelihoods for each hardware platform (mainframe, local area network, freestanding PCs, etc.).
vi. The length of time the department could operate without access to computing services (i.e. the maximum acceptable downtime before management must implement contingency procedures).
vii. A list of "critical" functions, applications, hardware, and information required for operations, including an explanation of *why* each item is critical. This section may include a functional flowchart depicting key processes, and a "topographical" flowchart showing configuration of hardware and equipment in the department.
viii. A list of manual/alternative procedures necessary to continue critical operations in the event of a disaster.
ix. Security/control requirements for operations when alternate processing methods and/or facilities are used. These are particularly important to identify before a disaster.
x. A sequence of steps for restoring and recovering data once computing services are back online. The information captured by the user department must be the same as that needed to restore files once computing services are available again.
xi. A designated offsite area in which operations could be continued in the event that current facilities are inaccessible. This should take into account hardware, telecommunications, and environmental requirements necessary to support the critical workload.

6.2 Lack of a comprehensive IT Disaster Recovery Plan (continued)

xii. Backup policies, including the location of all backup tapes/disks. Backup copies should be kept in a secure, off-site location.
xiii. Documentation in the plan regarding testing procedures. The plan should be tested and evaluated periodically and updates to the plan should be made to reflect significant test results.
xiv. Procedures for updating the plan when there are changes in key personnel, hardware, critical operations, etc.

After a suitable plan has been developed and documented, it should be tested and personnel should be trained to ensure that systems and business units can be recovered within an acceptable timeframe.

Management comments

The recommendation is accepted. We will include this point in IT Security policy and the implementation process will perform with new MIS implementation.

Implementation date

September 2008.

Individual responsible for the implementation

IT Manager

6.3 Absence of implementation of user ID and password management procedure

Condition

We have identified several housekeeping issues which should be aligned with best practice in order to tighten security at user access level as follows:

- We noted that the MB Dos system has automatically set **a maximum password length of only four characters,** and that no procedures or policies required that users set a password as numeric or alpha or in combination. We also noted some users had logged into the LAN with a password of only three characters (Internal Audit Department).
- We noted no password control procedure for resetting an expired password.

Implication

Passwords are a common means of validating a user's identity to access an information system. The absence of a policy on password usage, specifically the policy **on *minimum password length and password expiry*** at application level, increases the probability of guessable passwords, thus also creating the potential risk of unauthorised access to sensitive data.

Recommendation

To maintain effective control over access to data, we recommend that PRASAC implements a password policy which governs the selection and usage of passwords. Ideally, a password should have a minimum length (at least six characters) and use unique alpha numeric combinations. In addition, passwords should be changed every six months.

Management comments

In MB DOS System password length is fixed of only four characters and it cannot be increase. A clear policy was stipulated in the MB User Manual.

Password expiry (every six months) and minimum length (at least six characters) were set and controlled by domain controller in server. The finding that internal auditor can logged into the LAN with a password of only three characters is not possible, therefore, this finding is acceptable (this finding is present in 2006 reports).

Implementation date

Since June 2007.

Individual responsible for the implementation

IT Manager

6.4 Absence of overall IT Security Policies and Procedures

Condition

There is an absence of overall IT security policies, procedures, and guidelines to be enforced across the MFI.

Implication

i. Without overall, well-defined IT security policies and procedures, the MFI is increasingly vulnerable to security threats and risks of deliberate system misuse. Security incidents such as system failures, loss or denial of service and breaches of information confidentiality are among the risks that the Microfinance Institution needs to consider when implementing its IT security policy.
ii. Without a written policy, the Microfinance Institution is increasingly vulnerable to virus attacks from external storage media usage by staff or through internet browsing. This might result in complete system failure.
iii. Due to the lack of a policy, employees will not able to follow any preventive measures in the case of a virus attack on the system.

Recommendation

We recommend that the MFI implements stringent overall IT security procedures and policies governing the network and IT infrastructure. These policies must be communicated to all employees and enforced for all departments.

The Policy need to be supported and approved by top management. As a minimum, the following guidance should be included:

- Definition of information security, its overall objectives and scope, as well as the importance of security as an enabling mechanism for information sharing;
- A statement of management intent, supporting the goals and principles of information security;
- Incident management procedures to ensure quick, orderly and effective responses to security incidents;
- A brief explanation of the security policies, principles, standards and compliance requirements;
- A clear statement of the use of antivirus software and updating antivirus definitions.

The Policy will also act as a document which will help employees to be aware of the steps required in the case of a virus attack on the system.

Management comments

Draft of Overall IT Security Policies and procedure was already present to Management for comments.

Implementation date

Since November 2007 and will be finalised September 2008.

Individual responsible for the implementation

IT Manager

6.5 Absence of firewall

Condition

We noted the absence of a firewall on PRASAC's server.

Implication

Absence of firewall settings on the server can affect company data security, increasing the risk of problems such as virus infections and spam. This condition also makes it especially easy for data to be hacked, and security of data on the server cannot be protected or controlled.

Recommendation

We recommend that PRASAC should set up a firewall to protect against loss of data, virus infections, spam, etc., especially from hackers, to ensure the security of sensitive data.

Management comments

The finding and recommendation is accepted.

Implementation date

May 2008

Individual responsible for the implementation

IT Manager

7. GENERAL CONTROLS

7.1 An up-to-date exchange rate source for translating and accrued technical assistance fee should be used rather than the previous year's rate

Condition

Though the technical assistance fee is accrued for on monthly basis, PRASAC uses the prior year end exchange rate to account for this expense rather than an up-to-date one.

Implication

Failure to use an up-to-date exchange rate to accrue this expense means that the amount accrued at the last quarter is misstated. Although it is not a substantial amount, this does not indicate a good practice. Moreover, if such a practice occurs on a material account, the under accrued amount will be significant and this implies that PRASAC is overstating its profit.

Recommendation

PRASAC should use an up-to-date exchange rate to accrue expenses. In the case of this technical assistance fee, the exchange rate of the previous quarter from a bank should be used for the next quarter.

Management Comments

The expense amount in riel from last year 2006 was taken for accrual amount for year 2007, which result the different in exchange rate. The different between accrual amount and payment is charged to income statement. The different amount is not significant.

However, the technical assistance contract was terminated by the Company since March 2008 after completing privatisation plan for PRASAC MFI.

Implementation date

31 March 2008

Individual responsible for the implementation

Finance Manager

PRASAC MICROFINANCE INSTITUTION LTD

INTERNAL CONTROL REPORT
FOR THE YEAR ENDED 31 DECEMBER 2007

STATUS OF PRIOR YEAR'S RECOMMENDATIONS

	DESCRIPTIONS	STATUS	MANAGEMENT COMMENTS
1	**CASH IN HAND AND IN BANKS**		
1.1	**Daily cash count sheets should be properly certified as supporting evidence of responsibility in Kampong Chrey Sub-Branch** ***Recommendation*** We recommend that a monthly physical count of cash in hand should be fully performed and properly documented on cash count sheets signed by the custodian and by a person authorised to conduct and witness the count. The balance of cash in hand according to the count should be reconciled with the balance according to the general ledger and cash book. Any discrepancy should be investigated immediately. Adjustments should be recorded accordingly.	Implemented.	Will continue follow-up and improve.
1.2	**Cash count sheets should be prepared on a timely basis and reviewed by Branch Manager (BM) or Sub-Branch Manager (SBM) in Kong Pisey Sub-branch** ***Recommendation*** We recommend that a cash count sheet should be prepared once a day, signed by both the Cashier and the MB teller or SBM. The balance of cash in hand according to the count should be reconciled with the balance in the cash book and general ledger from the MB system. Any discrepancy should be reconciled and investigated immediately. The result of such an investigation should be documented and submitted to the Finance Department Manager for approval. Adjustments should be recorded accordingly.	Implemented.	
1.3	**No monthly bank reconciliation performed for January, March and April 2006 in Kompong Chrey branch** ***Recommendation*** We recommend that the bank reconciliation prepared at the end of the month be checked and reviewed by an authorised official, and initialed as evidence of the check and review.	Implemented	

	DESCRIPTIONS	STATUS	MANAGEMENT COMMENTS
2	**LOANS AND ADVANCES TO CUSTOMERS**		
2.1	**Properly prepared and updated loan files should be prepared on a timely basis according to the loan policy of PRASAC** ***Recommendation*** Compliance with PRASAC's loan policy should be implemented and useful information should be updated regularly to ensure that the requirement for up to date documents is fully satisfied and filing of loans is completed.	Implemented.	
3	**FIXED ASSETS**		
3.1	**FA register is not updated on a timely basis** ***Recommendation*** We recommend that the fixed asset register should contain a complete and up to date list of fixed assets, and that additions should be included and items disposed of excluded on time. The fixed asset register should contain at least the following information: Date of purchase Voucher number Description of assets Serial number Quantity Cost per unit Location Date of disposal Proceeds/Details of disposal	Implemented.	
3.2	**Fixed assets verification is not conducted on a regular basis** ***Recommendation*** A physical count and inspection of fixed assets should be performed at least quarterly and documented in a fixed assets inspection report, which should be signed by the person who performed the count and inspection and approved by an authorised person. The results of the	Implemented.	

	DESCRIPTIONS	STATUS	MANAGEMENT COMMENTS
	physical count should be reconciled with the balance in the fixed assets register and accounting records. Any discrepancy should be reconciled and investigated immediately. The results of this investigation and reconciliation should be documented in the fixed assets inspection report.		
3.3	**FA should be tagged properly** ***Recommendation*** Tagging PRASAC's assets is a key control to avoid misplacement or unauthorised use of these assets. For proper monitoring and to minimise the loss of fixed assets, we recommend that PRASAC should ensure that the procedures for labeling fixed assets are observed by PRASAC.	Not implemented. Refer to Point 2.2.	Implemented since May 2008.
4	**NON-COMPLIANCE WITH CENTRAL BANK'S PRAKAS**		
4.1	**Non-compliance with Central Bank's Prakas No. B795-001 on the calculation of foreign currency exposure and capital adequacy ratio** ***Recommendation*** We recommend that PRASAC take steps to ensure it complies with the Central Bank's Prakas in relation to foreign currency exposure and capital adequacy ratio.	Implemented.	
5	**INTERNAL AUDITORS' WORK**		
5.1	**No coverage of sample size of sample selection for each site visit** ***Recommendation*** We recommend that the internal auditors should follow the Internal Audit Manual and mention the total number and amount of loans for the period of audit.	Implemented	

	DESCRIPTIONS	STATUS	MANAGEMENT COMMENTS
5.2	**Some Internal Audit Reports have not been reviewed and approved by the General Manager and take a long time to be finalised** ***Recommendation*** We recommend that review and approval procedures should follow the Internal Audit Manual and management should take action if there is a postponement in the delivery of the report.	Implemented	
5.3	**The Internal Audit Report sent for BM's comment should be accepted and evidenced by BM's authorised signature** ***Recommendation*** We recommend that the review and approval procedures should follow the Internal Audit Manual and management should take action if there is a postponement in the delivery of the report.	Implemented	
5.4	**No formal follow up report prepared** ***Recommendation*** We recommend that a formal follow up report should be prepared to ensure that the BM is aware of the status of the previous year's findings.	Not implemented. Refer to 5.4.	Will implemented in 2008.
6	**INFORMATION TECHNOLOGY: GENERAL CONTROLS**		
6.1	**Lack of Environmental and Physical Security over the server room** ***Recommendation*** In order to prevent damage or compromise of assets and interruption to business activities, we recommend that the server room is locked at all times and any visitor access to the room is recorded. To prevent and minimise the potential damage in the event of a fire in the vicinity of the server, which may cause interruption to business activities, we recommend that PRASAC considers installing a smoke detector in the area, which should be readily accessible in the event of an emergency.	Implemented.	

	DESCRIPTIONS	STATUS	MANAGEMENT COMMENTS
6.2	**Absence of implementation of user ID and password management procedure** ***Recommendation*** To maintain effective control over access to data, we recommend that PRASAC implements a password policy which governs the selection and usage of passwords. Ideally, a password should have a minimum length (at least six characters) and use unique alpha numeric combinations. In addition, passwords should be changed every six months.	Not implemented. Refer to 6.3.	Implemented in September 2008.
6.3	**Absence of overall IT Security Policies and Procedures** ***Recommendation*** We recommend that the MFI implements stringent overall IT security procedures and policies governing the network and IT infrastructure. These policies must be communicated to all employees and enforced for all departments. The Policy needs to be supported and approved by top management. As a minimum, the following guidance should be included: ▪ Definition of information security, its overall objectives and scope, as well as the importance of security as an enabling mechanism for information sharing; ▪ A statement of management intent, supporting the goals and principles of information security; ▪ Incident management procedures to ensure quick, orderly and effective responses to security incidents; ▪ A brief explanation of the security policies, principles, standards and compliance requirements; ▪ A clear statement of the use of antivirus and updating antivirus definitions. The Policy will also act as a document which will help employees to be aware of the steps required in the case of a virus attack on the system.	Not implemented. Refer to 6.4.	

	DESCRIPTIONS	STATUS	MANAGEMENT COMMENTS
6.4	**Backup and Recovery Procedures** *Recommendation* To ensure availability of business data in a timely and efficient manner, we recommend that: • Daily backup operations should be documented to provide step by step instructions to the IT staff on scheduling backups, labeling, storage and restoration of these tapes or CDs when required. • A process of randomly restoring a backup tape to ensure the validity and completeness of its contents should be implemented on a monthly basis • The weekly backup tapes should be stored at an offsite location with proper labels.	Not implemented. Refer to 6.1.	Will implement in June 2008.
6.5	**Lack of a comprehensive IT Disaster Recovery Plan** ***Recommendation*** We recommend that management assess the criticality of all applications and what a loss of the computer facilities would mean to the continuity of the business. An effective Disaster Recovery Plan should be developed that encompasses all elements likely to be affected by a disaster to ensure the continuity of all critical business functions during the recovery period. It is essential that the plan be developed in a co-coordinated effort between system support and critical business functions.	Not implemented. Refer to 6.2.	
6.6	**Unauthorised software installation** ***Recommendation*** We recommend that PRASAC should prepare a formal procedure to detect unauthorised software installation. All PCs must be audited at least once a year. The IT officer has performed spot checks on PCs, but proper documentation of this procedure should also be prepared to show that all PCs have been audited during the year.	Implemented.	

	DESCRIPTIONS	STATUS	MANAGEMENT COMMENTS
6.7	**Absence of firewall** ***Recommendation*** We recommend that PRASAC should set up a firewall to protect against loss of data, virus infections, spam, etc., especially from hackers, to ensure the security of sensitive data.	Not implemented. Refer to 6.5.	Will be implemented in July 2008.