



Good Practice Note No. 23

Management of Liquid Assets

Part of a series of notes to help Centers and their internal auditors review their own Center internal management processes from the point of view of managing risks and promoting value for money, and to identify where improvement efforts could be focused. The good practices described in this series of notes should not be interpreted as minimum standards as not all may be applicable to every Center.

SUMMARY

The purpose of this note is to provide Centers with advice about good practice in terms of the management of the risks relating to managing liquid assets. Liquid assets cover all those financial assets of the Center, which include cash in hand, cash at bank and cash invested in various instruments to earn income when not immediately required for the Center's operations.

This note highlights the following good practices for Centers in relation to the management of liquid assets:

Investments

- Centers should have Board approved investment policies which set out the risk parameters within which investment activity is approved, and define the roles and responsibilities related to investment activities.
- Investment parameters should be established based on portfolio objectives and performance should be periodically reviewed against benchmarks relevant to each portfolio.
- Investment activities should be reviewed and approved by an Investment Committee of Center staff.
- Investment activity reports should be prepared periodically, at least quarterly.
- Conflict of interest policies applicable to members of the Investment Committee should be determined.
- Investment consultants hired by the Center should be independent and hired under conditions that ensure their objectivity.



Managing Foreign Exchange

- Foreign exchange risks should be actively considered and managed

Cash at Bank

- Opening and closing of official bank accounts, and advice of account signatories, should be controlled centrally within the Center. Authority for these transactions should be clearly stated in a Center policy document or delegation of authority instrument.
- Center policies should indicate the criteria for selecting banks for keeping the official accounts for investment and operating purposes
- Idle bank accounts should be subject to periodic review to decide if they should be closed
- Closing of official bank accounts should be managed to ensure there are no pending or unreconciled transactions for the account, and formal confirmation of closure should be obtained from the bank
- Official bank accounts should, where possible, be operated under a dual signatory arrangement. Preferably staff responsible for accounting and bank reconciliations should not be granted signatory authority, but where this segregation is not possible should only be granted authority under a dual signatory arrangement.
- In determining the official bank account signatories, the Center should give appropriate consideration to the need for backup signatories in case the primary signatories are unavailable.
- Bank account balances should be individually tracked in the Center accounting system, and balances regularly reconciled to original bank statements by persons other than the account signatories
- Reconciling items in bank reconciliations should be followed up with a view to their prompt resolution. Long outstanding reconciling items and actions taken to resolve the items should be periodically reported to the Director of Finance or Financial Controller for further review.
- Centers should manage the level of funds in operating accounts based on forecasted liquidity needs, to manage liquidity, foreign exchange and financial institution risks as well as opportunities to earn income on funds surplus to day-to-day requirements.
- Official bank accounts managed by outposted offices should be controlled through an imprest system, whereby replenishments are subject to a pre-defined and structured accounting for transactions since the previous replenishment
- Where outposted imprest account transactions are posted in the Center's accounting system by Headquarters, there should be a process whereby the postings are reported back to, and reviewed by the outposted office to provide assurance that the postings are made correctly. The communication lines and responsibilities for resolution of errors should be clear.



- Centers should adopt a risk-based approach to the retention or shipping to Headquarters of original vouchers supporting the financial transactions of the outposted offices.
- Check books should be subject to physical control against misuse.
- Wire transfer requests should be sequentially numbered, cross referenced in the accounts and copied as part of the supporting documents for such transactions.
- Minimize the use of “cash” checks.
- The use of ATM cards for making transactions on official bank accounts should be avoided.
- Programmed and other security controls over electronic banking should be strictly applied.
- Where official bank accounts must be kept in the name of staff members, these should be subject to the same level of control as accounts in the name of the Center.
- Centers should adequately monitor and be aware of any special restrictions for making payments through banking channels established by the host countries in which the banks are located or headquartered.

Petty Cash

- Cash on hand should be controlled as authorized petty cash funds approved by the Center’s Finance Department and replenished in a manner that ensures all funds are recorded in the books of the Center.
- Accountability for a petty cash fund should be assigned to one employee, designated as the fund custodian, and the cash stored in a secured way such that only the custodian should have access to the cash at any time, or that any alternative access under emergency situations is clearly traceable.
- Petty cash balances should be individually tracked in the Center accounting system, and balances regularly reconciled to actual cash independently of the petty cash custodian.
- Petty cash transactions should always be supported by payment vouchers and receipts.
- The purposes and upper limits on amounts of petty cash transactions should be established and communicated.
- Petty cash should be managed as a float subject to imprest procedures.



Good Practice Note No. 23

Management of Liquid Assets

INTRODUCTION

Liquid assets are the financial assets of the Center, which include cash in hand, cash at bank and cash invested in various instruments to earn income when not immediately required for the Center's operations. They are essential to the running of a Center and they underpin the computation of liquidity indicator which, among others, is used to monitor the financial health of Centers.

Liquid assets are held by Centers in three broad categories:

- Short-, medium- and long-term investments in interest-bearing instruments;
- Current accounts kept in banks and managed by Headquarters or outreach offices and remote stations, used to receive income deposits and make disbursements for operations by check or electronic funds transfers; and
- Petty cash floats kept at headquarters and in outreach offices (regional, country or project offices) or remote experimental stations, used for making small expenditures and advances related to day to day operations.

Centers manage these liquid assets through what are collectively referred to as treasury operations and CGIAR Financial Guideline No. 1 (FG1) sets out the overall principles that Centers should follow for these operations. The purpose of this Good Practice Note is to provide Centers with information on good practices in implementing the FG1 principles, whereby they can effectively manage the risks associated with various treasury operations.

OBJECTIVES OF MANAGING LIQUID ASSETS

The objective of liquid assets management is to deploy the Center's liquid assets in such a way that prudently strikes a balance between:

- Protecting against loss;
- Ensuring adequate liquidity for day-to-day operations; and
- Investing surplus cash profitably.

There are tradeoffs to be made among these objectives, with the first two objectives having priority. FG1 provides that, in general, Center investment policies should be conservative. This recognizes that the majority of the funds which form the liquid assets of a Center at any particular time come from



donors who are providing them to implement, in the short, medium or long term, the Center's research plans.

INVESTMENTS

Good practice

Centers should have Board approved investment policies which set out the risk parameters within which investment activity is approved, and define the roles and responsibilities related to investment activities.

FG1 provides that Centers will have a formal investment policy approved by the Board of Trustees and that through this policy the Board delegates' investment authority within defined risk parameters.

According to FG1, the policy should set out:

- The objectives of the investing activity;
- The basis for selecting between short-, medium- and long-term investment instruments;
- Criteria to be used for determining such matters as the selection of financial institutions, and the degree of concentration of investments in any one financial institution or in any one type of instrument or currency;
- Requirements with regard to the minimum quality of instruments to be selected for investments; and principal protection;
- Manner in which proposed investment transactions will be controlled within the Center (review and approval processes); any financial limits above which transactions require pre-approval, consultation or reporting to the Finance/Audit Committee or Board; and
- Requirements for reporting of investment activities to the Finance/Audit Committee and Board.

The Policy could also mention particular activities such as investment in equities and active foreign currency speculation (investing in currencies not required for operational reasons solely for the purpose of earning income on exchange rate gains) where principal is not protected; and the procedures to be followed in the event of non-compliance, in particular where as a result significant financial risk exposures arise.

As the financial environment in which the Center operates is prone to rapid changes, the policy should be reviewed periodically, at least every year.



Investment in government treasury bonds would appear to be a safe investment. However, the value of these bonds fluctuates with the market interest rate movements and there is the risk of potential loss if such bonds are held for trading. Therefore, investment should normally be made in government treasury bonds only if they are intended to be held till maturity.

Bonds held in held-till-maturity portfolio should not be traded because this would attract “mark-to-market” provision which may require the center to value the entire portfolio at market value at the end of the year, running the risk of having to write-off/provide for any possible unrealized losses.

The accounting treatment for investments and income thereon should comply with CGIAR FG 2.

Responsibility for the safe physical custody of investment instruments should be defined.

Good practice

Investment parameters should be established based on portfolio objectives and performance should be periodically reviewed against benchmarks relevant to each portfolio.

For the purpose of assessing performance, the investment portfolio could be segregated between short term, and medium/long term. In short-term portfolio, safety and liquidity are the primary objectives, followed by returns. In medium/long-term portfolio, besides safety and returns, liquidity should also be a significant consideration. Types of investments that would typically be allowed in the portfolio include:

Short-term

- Money market funds
- Bank Savings accounts

Short, medium and long-term

- Certificates of Deposit
- Government Treasury Bills
- Commercial Paper rated AAA
- Government Fixed Income bonds



Different benchmarks could be applied to these two sub-portfolios e.g. Government Treasury Bill/Euribor/Libor Rates for the first and average bond indices for the other.

Good practice

Investment activities should be reviewed and approved by an Investment Committee of Center staff

Investments should be subject to guidance and oversight of an Investment Committee comprising of senior officials. Investment Committees ensure that no single person is responsible for investment decisions and acts as a control to ensure transactions comply with the Board-approved policy. The role of an Investment Committee is to:

- Decides on the level/amount of investments in accordance with parameters set by the Board including the terms and conditions, and identifies banks where investments will be made;
- Provides the Board Audit Committee reports on investment status on a quarterly basis;
- Reviews the Investment Policy at least annually and recommends changes to the Finance and Audit Committee;
- Recommends to the Finance and Audit Committee the appointment and termination of appointment of consultants and other third party advisers as may be necessary or desirable to assist in the implementation of this policy.

Minutes should be kept of Investment Committee decisions.

Good practice

Investment activity reports should be prepared periodically, at least quarterly.

Periodic (at least quarterly) reports of investment activities should be prepared and these should form the basis of reports to the Audit Committee of the Board.(see CGIAR IAU's Good Practice Note on Audit Committee Terms of Reference). The objective of the reports should be to inform the Board about the exposure to financial risks, the effectiveness of treasury management in addressing these risks, and the likely impact on the Center's financial performance. These reports should provide sufficient information to confirm compliance with the Center's investment policy and could include details such as the types of investments made, financial institutions selected, maturity profile, returns earned, exchange gains/losses – realized as well as unrealized, currency exposure and hedging instruments employed.



Good practice

Conflict of interest policies applicable to members of the Investment Committee should be determined.

The conflict of interest requirements on Investment Committee members, as they participate in investment decision making, should be well defined. The Center's Investment Policy could indicate that Committee members refrain from personal business activity that could impair their ability to make impartial decisions, and from doing personal business with the same persons with whom business is conducted on CIAT's behalf. Members may be required to annually certify compliance with the conflict of interest policies.

Good practice

Investment consultants hired by the Center should be independent and hired under conditions that ensure their objectivity.

Investment Consultant(s) may be hired on a retainer basis and shall assist Management with its investment decisions. If so, they should be independent, unrelated directly or indirectly with any organization dealing in investments.

Investment Consultant(s) shall provide the following services:

- Assistance in the ongoing review and revision of Investment Policy
- Assistance in the determination of asset allocation consistent with the Investment Policy
- Assistance in ensuring compliance/consistency of investment decisions with Investment Policy
- Assistance in other services that may be identified by Management

Whenever consultants are engaged for providing specialized advice on investment, remuneration should not be linked to the returns generated through such investment advice. Returns-linked remuneration may lead to aggressive investment practices.

MANAGING FOREIGN EXCHANGE

Liquid assets are exposed to exchange rate loss risks, as well as windfall exchange gains, because Centers receive and disburse funds in multiple currencies.



Good practice

Foreign exchange risks should be actively considered and managed.

Failure to identify and manage foreign exchange risks and opportunities can have significant adverse financial impacts on Centers. Hedging is a mechanism used to mitigate exchange risks relating to receiving and spending. Where income is received in a currency in similar amounts to that will be spent during the year in that currency, a “natural hedging” can be established. Where there are substantial differences in the currencies of income and expenditure then other hedging activities can be considered, e.g.:

- Converting receipts to other currencies in proportion to expected expenditures in the other currencies for a projected future period. This has advantages in that it brings predictability to funds management, and also helps manage the risk of loss in value when the expenditure currencies are appreciating against the income currency.
- Delaying conversion of receipts to other currencies until the expenditures in those currencies are required, when the currency of receipt is appreciating against the expenditure currencies. This allows for opportunities to increase value.
- Forward contracting. In a forward contract, a transaction pertaining to a future foreign currency inflow (or outflow) is contracted with the bank at a predetermined exchange rate. Forward contracting is useful if the likely date of the foreign currency inflow/outflow is known with reasonable certainty.
- Writing options. An options contract entails a right, but not the obligation to conclude a future transactions at a set price. Options are very effective instruments for hedging currency risks, but they are relatively expensive.
- The rate of interest for local currencies (in countries where CGIAR Centers operate) is often higher than that for USD. Therefore, it would appear tempting to maintain and invest cash in local currency over and above operational needs to earn higher returns. However holding funds more than necessary for operations in local currency to take advantage of higher interest rates may entail foreign exchange losses where the local currency is depreciating greater than the additional interest earned, or move into the realm of foreign currency speculation if the local currency is appreciating. If the rate at which the local currency is converted back to USD on maturity is pre-determined through a forward contract, the center can assess in advance the financial benefit that would accrue, and avoid the speculative dimension.

When the local currency shows an appreciating trend against the US dollar, budgetary estimates will be affected as USD converted at a future date will fetch less local currency. Here again, forward contract can be used to cover this risk. For instance, if a large local currency disbursement is anticipated say, three months later, the center may book a forward contract with the bank to fix an exchange rate to



convert USD into local currency around the expected date of disbursement. The rate should obviously be favorable comparable to the rate used in the budget estimates.

CASH AT BANK

Centers operate official bank accounts for both day to day operations (receipt of income and disbursements of expenditures) as well as for investment purposes. These accounts may be located in a number of countries. Operating accounts may be controlled either at Headquarters or in outposted locations. Investment accounts should normally be controlled centrally at Headquarters. Some exceptions exist for various reasons in which case Headquarters should incorporate these “remote” investment accounts in the monitoring and periodic reporting of investment activities.

Opening and closing of bank accounts

Good practice

Opening and closing of official bank accounts, and advice of account signatories, should be controlled centrally within the Center. Authority for these transactions should be clearly stated in a Center policy document or delegation of authority instrument.

The authority to open and close bank accounts currently varies among Centers. Some Centers require board resolution for opening new accounts, in other cases the Director General has full authority and in some cases the Director of Finance or equivalent is delegated authority. In general, the CGIAR IAU recommends that, at a minimum, the Director General should be the approving authority. In this case the opening and closing of bank accounts and changes in signatories can be periodically reported to the Board through the Audit Committee. This would meet the requirements for oversight without entailing too much micro-management by the Board.

Where the Director General is empowered to open and close bank accounts and approve account signatories, some financial institutions require a copy of a Board resolution granting that power. While the power may be already included in general delegations of authority approved by the Board, a specific Board resolution in this regard may be required in some jurisdictions.

In any case the board resolution or internal submission to the Director General seeking approval should state name of bank, type of account to be opened, authorized signatories, mode of operation, and conditions if any.

Proliferation of bank accounts should be avoided. Some donors insist on separate bank accounts to exclusively handle transactions in respect of projects financed by them or to hold the funds in the original currency until disbursements are made. Efforts should be made to persuade the donor to accept



the in built controls in bank account management and accounting mechanism to identify and track the project transactions. Donor funds should where possible only be received into Headquarters-operated bank accounts rather than any operated in outreach locations. Exceptions to this should be carefully examined and approved by Center management. Consolidating accounts helps maximize investment earnings and increases efficiencies with regard to investment pricing, safekeeping and administration.

Where feasible, centralization of non-petty cash payments for different locations should be considered to limit the number of bank accounts required for both Headquarters and outposted locations. This helps reduce transaction costs and risks associated with having numerous bank accounts and maximizes the amount of funds available for investment.

The Center should maintain a register of official bank accounts and account signatories, and hold, in readily accessible file(s), copies of the bank correspondence on the opening of the accounts and advice of signatories and specimen signatures.

The list of authorized signatories should be periodically reviewed by the Center's Finance Department at least annually. A statement from each bank should be obtained at the beginning of each year confirming the currently valid list of authorized signatories. This could be done in conjunction with the annual financial audit confirmation of balances exercise. The statement should be carefully reviewed for currentness and conformity with the signing authority in force.

Good practice

Center policies should indicate the criteria for selecting banks for keeping the official accounts for investment and operating purposes.

While opening bank accounts, sufficient care should be taken to ensure that the bank is financially sound, reputed and capable of delivering required services to the Center. For international financial institutions where investment funds will be kept, credit ratings from independent rating agencies will be the primary criteria. The following sub-criteria could be considered when choosing or evaluating whether to switch local banks for operating purposes:

Financial soundness

- Credit ratings from independent rating agencies when available
- Capital adequacy
- Size
- Minimum 3 years' consistent profitability



- Extent of non performing assets as a percentage of total deposits
- Rankings published by respectable dailies/magazines/journals

Reputation

References from other organizations, especially other Centers or other international nonprofit organizations who may require similar services

Service

Quality of service (low volume of bank mis-postings, delays in posting transactions and delays in production of bank statements, quality bank statements) – this can be an important factor for operating accounts in countries with weak banking systems

- Branch network
- Technology
- International presence/correspondent relationships

Good practice

Idle bank accounts should be subject to periodic review to decide if they should be closed.

The number of bank accounts should be reviewed at least annually and non-operative/idle accounts should be considered for closure. If a bank account has not been operated for twelve months, chances are that the account no longer needed.

Good practice

Closing of official bank accounts should be managed to ensure there are no pending or unreconciled transactions for the account, and formal confirmation of closure should be obtained from the bank.

Before closing a bank account, it must be ensured that the bank account is no longer in need or alternative better banking arrangement is already in place. A reconciliation of the bank account just prior to closure should be carried out and it should be ensured that there are no unreconciled items outstanding. If there are any unpresented checks outstanding, they should be recalled from the payee



and fresh check on another operative bank account issued. If there are any other unreconciled items such as checks deposited not credited, the account should be closed only after such items are cleared. All unused check leaves/books should be reconciled and surrendered to the bank.

Bank signatory arrangements

Good practice

Official bank accounts should, where possible, be operated under a dual signatory arrangement. Preferably staff responsible for accounting and bank reconciliations should not be granted signatory authority, but where this segregation is not possible should only be granted authority under a dual signatory arrangement.

A situation where one person operates the bank and is responsible for the accounting of the transactions and the reconciliation between the bank records and the accounting records creates a significant control exposure. In some outposted locations where there are limited staff it is unavoidable, but the compensating control of a dual signatory arrangement should always be in place in such circumstances. In addition, Headquarters should exercise closer monitoring of the operations of the account, including independent bank reconciliation.

Based on some recent experiences Centers have encountered, positive confirmation should be obtained from the bank that the dual signatory arrangement will be fully honoured by the bank and that under no circumstances will the bank accept a single signatory where a dual signatory arrangement is in place. The bank should accept liability for failure to enforce this if this occurs and allows a fraudulent act to take place by one of the account signatories acting alone.

Good practice

In determining the official bank account signatories, the Center should give appropriate consideration to the need for backup signatories in case the primary signatories are unavailable.

The CGIAR IAU recommends that all official bank accounts should have back up signatories to the primary ones, and in the case of bank accounts operated at outposted locations, the backup signatories include persons at Headquarters.



Bank reconciliations

Good practice

Bank account balances should be individually tracked in the Center accounting system, and balances regularly reconciled to original bank statements by persons other than the account signatories

The most important controls over the operation of official bank accounts are to register all of them in the accounting system and subject them to regular, timely reconciliation between the accounting balances and those appearing on the bank statements. Bank accounts should be reconciled at least on a monthly basis. These should be done within the following month after the end of the month being reported. Timeliness of bank account reconciliations should be monitored by the Director of Finance or Financial Controller and any delays investigated.

The reconciliation should be done by personnel independent of bank account maintenance and accounting. If in outreach locations, the number of staff does not allow for segregation of these responsibilities, the reconciliation statement should be verified and signed by another person who is not directly involved in bank account maintenance and accounting.

All bank reconciliations should be ultimately done using original bank statements, or where electronic banking is used, bank statements which are downloaded directly from the bank's system by the persons responsible for preparing and verifying the bank reconciliations. Interim reconciliations made against faxed or downloaded bank statements should be followed up eventually with final reconciliations against original statements. The original statements should be filed with the bank reconciliation records, for subsequent audit purposes.

It is very important to keep effective monitoring at Headquarters level of bank account reconciliation for all locations. The monthly reconciliation statements should be followed up and carefully verified. Long outstanding items and unusual transactions if any should be investigated and satisfactory explanation obtained.

With regard to controls over fraud, while verifying bank reconciliation statements, special attention should be given to entries representing credits not reflected in the bank statement and debits figuring in the bank statement not reflecting in the ledger account.



Bank Reconciliations Procedures

The format of the monthly bank reconciliation should clearly identify reconciliation between the bank statement balance at the end of the month, and the accounting balance, as follows:

Starting balance for the month per the accounting system (general ledger account for the bank account)

- + Deposits made during the month, recorded in current monthly accounting report
- Checks issued during the month, recorded in current monthly accounting report
- Other charges made by the bank (fees), recorded in current monthly accounting report
- = Ending balance for the month per the accounting system
- + Checks issued and included in the monthly accounting report(s) but not yet debited by bank in the bank statements ("unpresented" or "outstanding" checks)
- = Balance as per bank statement at end of month

Normally outstanding checks should be the only reconciling item. Exceptionally the reconciling items may include bank errors (items posted by the bank in error to the account), or deposits in transit (delays by the bank in posting deposits).

The bank reconciliation should be accompanied by a list describing the outstanding checks and any other reconciling items and their age.

Good practice

Reconciling items in bank reconciliations should be followed up with a view to their prompt resolution. Long outstanding reconciling items and actions taken to resolve the items should be periodically reported to the Director of Finance or Financial Controller for further review.

Long outstanding checks should be followed up with payees to find out why they have not presented the checks. Delays in posting of transactions on the bank statements and bank errors should be followed up with the banks. Reconciling items which cannot be readily explained should be subject to detailed, independent investigation to ensure that they are not manifestations of fraudulent activity. Items outstanding for more than 12 months should be considered for provisioning or write off in the accounting records.



Validity of checks should be restricted to not more than 6 months, or as per local banking laws, whichever is shorter. Unpresented checks outstanding beyond the validity period should be followed up for replacement/cancellation as the case may be.

Cash balance management

Good practice

Centers should manage the level of funds in operating accounts based on forecasted liquidity needs, to manage liquidity, foreign exchange and financial institution risks as well as opportunities to earn income on funds surplus to day-to-day requirements.

Normally, operating accounts are maintained as non-interest bearing current accounts. The balances in the current account being idle assets, care should be taken to optimize the operating account balances. An annual cash flow forecast should be prepared, broken down into monthly plans, taking into account expected inflows and outflows based on which the cash required to be maintained to meet day-to-day needs should be determined. Cash flow forecasts should also factor in the expected receipt of pledges by unrestricted donors – in some cases these can be quite late in the year or even received in a following year. Surplus funds available should be invested.

Many banks provide “sweep” account facility wherein daily balances in excess of a specified minimum will be swept into an interest-bearing account, to be swept back as and when necessary. Centers should take advantage of the “sweep” account facility where these are available as they are a very effective way of managing short-term surplus cash.

Outreach locations maintaining bank accounts should also prepare monthly cashflow plan and submit to headquarters when placing funding requests in relation to the bank accounts.

The level of funds held in non-interest earning operating accounts should be reviewed at least monthly and take into account the:

- cash flow forecasts for the forthcoming month;
- exchange rate risks in relation to funds that must be converted from the main currencies of the Center in order to be held in local currency bank accounts. In the case of outposted accounts, the amount of local currency balance to be maintained should normally not exceed one month’s cash requirements plus a small cushion to cover unexpected, emergency requirements. In locations where the local currency tends to be volatile, a lower amount with a shorter replenishment cycle should be considered.
- extent of deposit insurance/guarantee applicable to the accounts.



Imprest account management

Good practice

Official bank accounts managed by outposted offices should be controlled through an imprest system, whereby replenishments are subject to a pre-defined and structured accounting for transactions since the previous replenishment.

When official office bank accounts are established in outposted locations, they are advanced funds from Headquarters and thereafter replenished on the basis of requests from the outposted office. Centers should establish procedures, applicable to all outposted offices, for standard reporting on the use of funds prior to replenishment. The reporting package should include:

- a report of transactions posted in the accounting system (local system or input into a corporate system) in the previous period;
- a bank reconciliation as at the date of the reporting, with original copy of the bank statements used for the reconciliation, and details of long outstanding reconciling items;
- a petty cash reconciliation as at the date of the reporting, to support the “funds advanced to petty cash” balance;
- a report on other advances made from the official account, which are receivables. This should preferably be accompanied by an age analysis; and
- a report on funds included in the account which are held on behalf of third parties such as other Centers and therefore payables

These reports should be checked at Headquarters as part of the approval process for replenishing the bank account.

Good practice

Where outposted imprest account transactions are posted in the Center’s accounting system by Headquarters, there should be a process whereby the postings are reported back to, and reviewed by the outposted office to provide assurance that the postings are made correctly. The communication lines and responsibilities for resolution of errors should be clear.

The persons at Headquarters responsible for the review and posting of imprest accounts should be known at all times by the outposted office financial/administrative staff. Any mispostings detected by the office should be resolved within the month after the reporting period.



Good practice

Centers should adopt a risk-based approach to the retention or shipping to Headquarters of original vouchers supporting the financial transactions of the outposted offices.

Shipping of vouchers can be a very expensive exercise. Local banking and taxation regulations may also require local retention of vouchers. Unless there is a risk that the vouchers may not otherwise be properly filed, that the vouchers may not be genuine or match what is accounted, it would be reasonable to allow local retention of the vouchers. These can be subject to periodic review or particular vouchers called in to Headquarters if external or internal audit require.

Controls over check stocks, and ATM cards

Good practice

Check books should be subject to physical control against misuse.

Controls over the custody, issue and use of check books is important to mitigate the risk of misuse of checks for unauthorized bank transactions.

When a stock of check books is received from the bank, the details should be entered in a register showing date of receipt, listing each check book with the check book number ranges in each book and the signature of the person receiving the stock. Stock of check books should be kept in a safe.

Upon receipt, check books should be verified for the sequential completeness of check leaves as indicated in the bank record of what was supplied and any discrepancy should be notified to the bank immediately.

Working stocks of check books required for day-to-day use should be issued only to the staff authorized to process check issue. Issues should be noted in the check book stock register and the signature of receiving staff should be obtained. Unused checkbooks should be returned at the end of the day and stored in the safe.

Checks should be used sequentially for each bank account to facilitate bank reconciliations and early detection of misuse of checks.



Cancelled checks should be defaced with the words ‘Cancelled’ written prominently across the face of the check and the check should be stapled to the respective check leaf stub. Cancelled checks should be recorded in the accounting records to facilitate reconciliation of the use of the checkbooks.

Security controls over writing checks, that are applicable to the country in which the account is maintained, should be implemented. Common examples are the crossing of checks (i.e., made payable only through a bank account, and making checks out to “order” by striking out “bearer” after the name of the payee. All information should be completed on the check stub.

Good practice

Wire transfer requests should be sequentially numbered, cross referenced in the accounts and copied as part of the supporting documents for such transactions.

Wire transfer requests should be subject to the same controls as for issue of checks. Wire transfer requests should be sequentially numbered and the number cited in the transaction description in the system. Copies of signed wire transfer requests should be carefully preserved.

Good practice

Minimize the use of “cash” checks.

Control over disbursements is stronger when the transaction can be linked in the payment system in a non-deniable way to a specific payee. Issuing “cash” checks weakens this linkage and if there is a problem makes it more difficult to determine to whom the money went. “Cash” checks should be avoided except to replenish petty cash funds, though it is realized in some locations the cash economy is very strong due to a weak banking system, and so cash payment is required by suppliers in many cases. Where cash payments cannot be avoided, getting receipts which identify payee is important.

An associated area where controls should be carefully monitored is the carrying of large amounts of cash by staff for payments such as workshop per diems. Where possible these should be transferred to the payees through bank transfers or money wiring services. Aside from security issues, transport of large sums of cash over international borders triggers currency import reporting requirements.

Good practice

The use of ATM cards for making transactions on official bank accounts should be avoided.



ATM Cards are relatively more vulnerable to misuse and fraudulent transactions compared with checks and electronic funds transfer requests. It is much more difficult to enforce watertight controls over the custody and use of the cards as well as the cash drawn using them, and therefore should not be used for transacting on official bank accounts. Where banks offer to issue these, they should be declined and the bank instructed in writing to not issue the cards directly to any signatory.

Controls over electronic banking

Good practice

Programmed and other security controls over electronic banking should be strictly applied.

As electronic banking is a relatively recent area and many centers still do not have established procedures and guidelines, this section is dealt with in more detail,

Electronic banking activities can be broadly classified into three groups with distinct risk profiles:

- Informational--Offers information about the bank's products and services ("brochureware") - Low risk
- Communicative--Offers account-related information in view mode – Low risk.
- Transactional--Allows updates to static data (such as addresses and execution of financial transactions such as funds transfer remotely – High risk. Online transactions are often irrevocable once executed.

Electronic banking access is usually either by way of direct dial-in access over a private network or by network access through the Internet. Although the former may be more secure than the latter, both types of connections are vulnerable to interception and alteration.

The main risks of electronic banking are the online theft of the user id and password, loss, abuse or unauthorized disclosure of information, including misdirection of funds transfers and the unauthorized removal of funds from the accounts. These risks cannot be altogether eliminated, but mitigated through a combination of sound internal controls and safe practices using technological tools for authentication, authorization, privacy and data integrity.

Electronic banking can be transacted either through the bank's system software installed on the Center computer or via the internet. In either case, the basic controls are similar. In the former case, it should be ensured that the Administrator user privileges does in no way compromise the operational controls.



Authentication

Authentication will apply to both the parties involved in the transaction – the bank and the customer.

For authenticating the bank, technology used for online transactions should be carefully evaluated before electronic banking arrangement is established. Browsers and application software should support Secure Sockets Layer (SSL) 128-bit encryption or a higher encryption standard to protect the transmission of information submitted or when online forms are used. Secured websites begin with a “https://” url.

It should also be ensured that the Bank uses a digital certificate to authenticate the genuineness of the website. While logging on, the browser should challenge the bank website to prove its identity using the digital certificate. It should be ensured that this identity check has occurred. In Microsoft Internet Explorer, ensuring that the image of a yellow lock is seen at the bottom of the browser window and double-clicking it allows one to view the digital certificate.

Customer authentication methodologies involve three basic factors - something the user knows (e.g., password, PIN), something the user has (e.g., ATM card, smart card); and something the user is (e.g., biometric characteristic, such as a fingerprint).

Authentication methods that depend on more than one factor should be used in electronic banking transactions as they are more difficult to compromise than single-factor methods. While passwords should be used as the primary factor, the second factor should be chosen from a range of methods discussed below:

Tokens are physical authentication devices and include USB token device, a smart card and password generating tokens. Smart cards are hard to duplicate and are generally tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. Their main disadvantage is that they require the installation of a hardware reader and associated software drivers. A password-generating token produces a unique pass-code, also known as a one-time password (OTP) each time it is used. Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (something a person is). Scratch cards are less-expensive, “low-tech” versions of the OTP generating tokens. OTP devices are commonly made available by banks for multifactor authentication and should be the minimum second factor authentication mechanism Centers should use.

The normal safeguards and controls on Passwords/PINs, listed below, apply even more stringently to electronic banking:

- Should be at least 6 digits or 6 alphanumeric characters.
- Should not use the same digit or character more than twice.
- Should not be based on user-id, personal telephone number, birthday or other personal information.



- Must be kept confidential at all times and not be divulged to anyone.
- Must be memorized and not be recorded anywhere.
- Should be changed regularly.
- Should not use the same password/PIN for different websites, applications or services, particularly when they relate to different entities.
- Should disable the 'AutoComplete' function to prevent others from seeing your logon information.

Transaction processing

Only personnel authorized to execute electronic banking transactions should be able to do so. The electronic banking application should have a three-tiered process for completing transactions. The first is transaction initiation/input, then verification/approval and finally, execution. These functions should be adequately segregated so that no single person could initiate, approve and execute transactions. Access security logs and audit trails should be systematically maintained.

Where electronic banking software is installed in a Center computer, the bank should provide appropriate measures in relation to any System Administrator access provided to Center staff, to manage the risk of “super user” over-ride of programmed controls.

Where electronic banking software is linked to Center accounts payable systems, appropriate controls should be in place to ensure payee account details are correctly transferred and not subject to unauthorized changes whereby the payments might be directed to another party.

To enhance online processing security, out-of-band confirmatory procedures in respect of transactions above pre-set values for high value transactions may be put in place as an additional control – the bank must obtain independent confirmation of the transactions through an alternative channel, either before or at the same time that the transaction is being processed by the Center. In such cases, positive confirmation should be obtained from the bank regarding enforcement of these precautions and acceptance of liability for failures to enforce.

Additional risk mitigation measures

Electronic banking is prone to several other security risks. Cybercriminals resort to a variety of techniques to gain access to confidential banking details. Some of the common methods include:

- Fraudulent or spoof websites - where customers are asked to input their personal information, mistaking it to be the bank's genuine website.
- Phishing - normally a spam e-mail containing a hyperlink to a log-on page, which requests online banking passwords. The page appears to be an official website but is actually a spoof website.



- Trojan software - a malicious code attached or embedded in software that is planted in a customer's PC by a fraudster to access the customer's personal information. A form of Trojan is "key-loggers" which monitor and record the keystrokes when a person types on the keyboard (e.g. user ID and password). This information can be passed back to an unauthorized person.
- Social engineering – persons posing as bank officials, security or investigative personnel (or other “plausible” roles) requesting confidential information such as passwords in person, by telephone or email.

Protection from such attacks can be had to a great extent by adopting the following practices:

- Install a personal firewall to prevent hackers from getting into the computer being used for electronic banking.
- Install and regularly update anti-virus and anti-spyware software to prevent viruses from infecting the computer.
- Remind staff never to respond to requests for password information and to contact the bank if they have received such a request. Regularly check the computer used for electronic banking to make sure it doesn't have any spyware, such as a keystroke collector, installed in the system.
- Always access the bank website by starting up a new browser session and typing in the address directly into the address bar or browser. Never follow a link in an email to the bank website. When accessing secure pages, ensure the padlock appears in the bottom right hand corner of the browser and that “https” is displayed in the browser's address bar.
- Prefer banks which use countermeasures against keystroke collectors, such as on-screen keyboards for entering passwords.
- Never leave the computer signed in to the internet when not required
- Use the Sign Off button when a session has finished
- Browser software often saves or "caches" pages in the computer's temporary memory. This means that even after logging off electronic banking, it is possible to view a version of a previously viewed page by clicking the Back button. To prevent this, the "Logoff" button should always be used to quit an electronic banking session, and the browser then closed. Use the Internet Options feature to make sure that all temporary files are deleted
- Make sure that the electronic banking application has a feature to disable online access following a certain number of unsuccessful logon attempts and re-enable only after a security procedure is gone through. It should also have a “session time-out” feature whereby if the session is idle for a given period of time, it is ended automatically.
- Use a dedicated machine for electronic banking, not to be used for regular internet access.



Official bank accounts in staff names

Good practice

Where official bank accounts must be kept in the name of staff members, these should be subject to the same level of control as accounts in the name of the Center.

Normally all official bank accounts should be opened in the name of the Center. However, in countries where Center is not recognized a legal entity, and using a host institution to make payments is not an option or not practicable, an official account may be opened in the personal name of a staff member (usually the office OIC). In such cases there are certain controls which should be in place:

- no mingling of personal and official funds or transactions in the account should be permitted;
- the same imprest and reporting requirements as for other official accounts should be applied;
- Headquarters should be particularly vigilant over operations of account and bank reconciliations; and
- Appropriate steps should be taken to protect the staff in relation to any local taxation or anti-money laundering laws (frequent, large funds coming into such accounts may attract the attention of fiscal or anti-money laundering agencies)
- Where amounts transferred may not be large, the funds may be better controlled as advances to staff rather than through special purpose bank accounts, and subject to advance liquidation procedures.

Banking transactions subject to special restrictions

Good practice

Centers should adequately monitor and be aware of any special restrictions for making payments through banking channels established by the host countries in which the banks are located or headquartered.

Centers should monitor and be aware of any special restrictions imposed by the countries in which its bank accounts are domiciled, or in which its banks are headquartered, to ensure appropriate steps are taken for compliance – either avoiding such transactions or obtaining the required licenses. These restrictions may include:

- Restrictions on payments to persons and entities in countries subject to UN Security Council sanctions related to terrorist financing or non-compliance with Security Council resolutions;



- Similar restrictions imposed unilaterally by the countries. For example, payments to certain countries, or particular individuals or entities in certain countries, using United States banks may require special licenses from the Office of Foreign Asset Control; payments to certain individuals or entities associated with narcotics trafficking (on the so-called “Clinton List”) are prohibited;

PETTY CASH CONTROL

Cash on hand is an idle (i.e. non-income earning) asset, but at the same time is very critical for day-to-day operations. It is needed for small incidental disbursements, where payment through banking systems would be expensive, cumbersome or impractical. It is also needed in certain countries where the banking system is limited or risky or many payees require receipt of payments in cash. Centers also hold emergency supplies of cash in some locations where the risk of civil disruption/bank closure is high. Because it earns no supplemental income, and by its nature subject to high risk of misappropriation, the amount of cash held should be kept to the minimum needed to meet the above requirements and facilitate smooth operations. However, due to the considerations mentioned above, the amount of cash on hand in some Centers, especially in particular locations, can be quite high.

Good practice

Cash on hand should be controlled as authorized petty cash funds approved by the Center’s Finance Department and replenished in a manner that ensures all funds are recorded in the books of the Center.

All petty cash funds, whether at Headquarters or in outreach locations/remote stations should be approved by the Headquarters Finance Unit, and replenished from Center bank accounts rather than through direct deposit of revenues. Finance should monitor operations of the petty cash funds through reviews of replenishment requests (for Headquarters funds) and outreach office/remote station financial reports. The proper operation of the funds should be tested by periodic, independent surprise cash counts.

Good practice

Accountability for a petty cash fund should be assigned to one employee, designated as the fund custodian, and the cash stored in a secured way such that only the custodian should have access to the cash at any time, or that any alternative access under emergency situations is clearly traceable.



Generally, petty cash should be kept in a safe or container to which only the custodian has access. To ensure access when the custodian is unexpectedly unavailable for an extended period, a spare key or combination should be kept in an envelope that is sealed such that its opening will be detectable and is in the custody of their supervisor or another more senior staff member.

Prior to the handover of custody when the custodian changes or goes on/returns from leave, there should be a formal handover/takeover comprising a cash count form signed by the incoming and outgoing custodians. This should list the cash and vouchers on hand and be retained for audit inspection purposes.

Good practice

Petty cash balances should be individually tracked in the Center accounting system, and balances regularly reconciled to actual cash independently of the petty cash custodian.

The general ledger chart of accounts should permit the tracking of individual cash balances by location, to facilitate analysis of cash holdings and their monitoring. Actual petty cash on hand should be periodically counted (at least each time a replenishment is requested) jointly by the petty cash custodian and another person (usually a Headquarters accounting staff or head of finance/administration in an outreach office/remote station), and the result reconciled to the ledger balance by accounting staff. This should include a count and reconciliation at the end of the financial year, to support the preparation and external audit of the Center's financial statements.

The Center should also implement a practice of periodic, surprise independent checks of the operation of the petty cash funds, to ensure that in between the scheduled reconciliations.

End of financial year cash counts should also be conducted and the records of these, signed by the petty cash custodian and another person, should be submitted to the Center's Finance Department and filed in the working papers supporting the preparation of the Center's annual financial statements, ready for review by the Center's external auditor.

Good practice

Petty cash transactions should always be supported by payment vouchers and receipts.

All disbursements from PCF should be supported by vouchers, duly authorized according to the Center's delegations of financial authority. The vouchers should be numbered and filed in sequential order, and for amounts above a certain amount required to be supported by supplier invoices/receipts. Receipts



should be issued for incoming cash and these should be pre-numbered and should be issued in sequence. Canceled receipts should be preserved on record.

Good practice

The purposes and upper limits on amounts of petty cash transactions should be established and communicated.

Given the potential for abuse, the types of transactions and ceiling of amounts to be paid through petty cash should be clear. New custodians should be oriented in these requirements and the consequences for use of the cash for private purposes or for temporary private loans.

Good practice

Petty cash should be managed as a float subject to imprest procedures.

Cash is most effectively managed as a float subject to imprest procedures. The features of this are:

- There is a fixed (“maintained”) balance to which the float is replenished, so that the replenishment amount is always equivalent to the actual petty cash expenditures reported since the last replenishment, less any cash receipts from such sources as returned unused travel advances;
- Major cash receipts are directly deposited in a bank account rather than used to replenish the cash float; and
- Petty cash reconciliations can always be made between the fixed balance and the amount of cash plus vouchers and receipts on hand

The level of cash float should be equivalent to the expected disbursements in one replenishment cycle, and so will be dependent on each center’s needs at individual locations. Given a monthly reporting cycle, a rule of thumb for frequency of the replenishment cycle is 15 days, so that there are at least two replenishments per reporting cycle.

First Exposure Draft: June 7, 2007
Authors: T.N. Menon & John Fitzsimon
First Edition: December 7, 2007
Updated by: T.N. Menon