AUDIT GUIDELINES
ELECTRONIC FUNDS TRANSFER

November 2003

The Audit Guidelines (the "guidelines") are intended to provide members of the Securities Industry Association ("SIA"), Internal Auditors Division with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including SIA or any of its divisions or affiliates. Neither SIA, nor any of its divisions or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit.

TABLE OF CONTENTS

I. INTRODUCTION TO ELECTRONIC FUNDS TRANSFER

General Background

The internal Audit Guidelines for Electronic Funds Transfer ("EFT") is a tool designed to facilitate the internal auditors' determination and assessment of the potential risks inherent in an EFT environment and the related controls which an organization may use to manage, monitor, and evaluate those risks. Also included are possible work steps that the Internal Auditor may perform to assess the adequacy and effectiveness of controls and processes used in the monitoring of a firm's EFT function. Although the guidelines were designed to evaluate the risks of a U.S. broker/dealer, many of the principles underlying the guidelines are also applicable to other financial services entities (e.g., investment managers, banks, and other custodians).

EFT is a cost and time efficient method of settling obligations. However, it also represents a substantially higher level of risk as compared to the largely paper method it replaced. Simply put, you cannot stop payment on the transfer once it is made. The same day funds environment requires greater controls than the "two signature" checks of the past. The financial services industry, in varying degrees and at various times, has moved from paper funds transfer to electronic funds transfer.

Common Platforms

Bank to bank funds transfer has been electronic since 1971 through a system known as CHIPS (Clearing House Inter-bank Payment System). In 1971, CHIPS' first full year of operation, there were fifteen customers who performed roughly 800,000 transactions for a total sum in excess of $1 billion. In 2002 there were fifty-four customers, who performed 63,000,000 transactions for a total sum in excess of $300 billion.

Structured messages, such as those used by SWIFT (Standard For Worldwide Inter-bank Financial Telecommunications) allow for straight through processing between international as well as domestic financial institutions. A broker/dealer in the U.S. can transmit a message over the SWIFT network to its bank in Tokyo, instructing it to receive funds from a third party and directing the bank as to which of its accounts are to be credited with the funds. These particular messages, known as the 200 series, are used for instructing fund movement. Other series are used for other financial purposes such as the 500 series for security movement. Swift processes over 7 million messages per day.

Broker/dealers and other non-bank financial institutions make use of the Federal Reserve wire system (FedWire) to settle money transfers. The FedWire, also known as "fed funds" and "same day funds," is used to settle street side as well as customer side transactions and is the principal system used by broker/dealers to move funds. Since only banks have direct access to the FedWire system, broker/dealers must conduct their FedWire activity through an affiliated or non-affiliated member bank.

Virtually all parts of a broker/dealer's business are involved in EFT in some way. Some of the more common areas that require the use of EFT are discussed below.

Individual Clients (Retail)

The majority of retail accounts maintain cash balances at their broker/dealer that are invested in money market funds. Some of these money market funds are internal to the firm, necessitating the movement of money through internal journals; others use mutual fund companies or mutual fund divisions of the firm requiring the movement of funds between entities. Broker/dealers that are affiliated with a bank might accomplish this movement through a daily automated sweep program that moves idle cash into the affiliated bank.

Retail firms may have many branches spread out over a wide geographical area. Clients may deposit funds into their account or withdraw funds from their account via an EFT. When clients deposit funds into their account via check or other cash equivalent, there is usually a process whereby the funds received from clients are mailed to a central point, such as a regional or home office. When money is received at a branch it is usually deposited in a local bank and then 'drawn down' by the firm's Treasury Department into a central cash management account via CHIPS or FedWire. This enables a firm to better control and manage their cash balances and have faster access to funds.

Institutional Clients

Institutional accounts (e.g., DVP/RVP accounts) use the services of a custodian bank or prime broker to maintain and service their portfolios. Money transfers between broker/dealers and a custodian bank or prime broker are accomplished through EFT in the settlement of institutional customer trades. For example in the settlement of a sale transaction, the custodial bank instructs the Depository Trust Company ("DTC") to deliver stock that has been sold by the institution to the selling broker that acted on its behalf. The movement of the stock on DTC's records is accomplished electronically between the accounts maintained on behalf of the institution and the account of the broker/dealer. The money settlement for the transaction is accomplished at the end of the day on a net basis. The actual money is moved by the commercial bank or prime broker representing the broker/ dealer to DTC (on instructions from the broker/dealer), which in turn pays the custodian bank. This too is accomplished through an electronic funds transfer.

Broker/dealers will also utilize EFT in the settlement of contracts, such as OTC derivatives contracts.

Trade Settlement

In the execution of their daily routines, broker/dealers must settle securities transactions with various clearing entities. The money side of these settlements is completed via an EFT.

Similarly, settlement of derivative and other contractual type transactions will also involve the use of EFT either through a clearing organization or firm to firm.

Firm Financing and Expenditures

Another aspect of a broker/dealer's operations greatly impacted by EFT is the financing function. Typically a broker/dealer will finance its short-term cash needs by entering into repurchase agreements. Settlement of repurchase transactions is accomplished through a simultaneous exchange of funds and securities, the funds moving through EFT.

Long-term financing transactions, such as commercial paper and bank borrowings, will typically settle through an electronic funds transfer on both the financing side and on the repayment side.

Many repetitive type expenditures will also be made through an EFT. Some typical transactions included in this category are reimbursement of payroll accounts, payment of insurance premiums and leasehold payments.

Process

A common method used to better control EFT is to centralize the processing of transfers in one location, such as the Treasury Department or an operations cash management control group. The group responsible for processing funds transfers will act upon approved written or electronic requests from various departments in the firm. Many of these transactions are repetitive in nature, occurring daily or weekly. Accordingly, standing payment instructions will be set up in the funds transfer system, avoiding the necessity of having to enter repetitive instruction information while enhancing the overall control environment. The key to a well controlled EFT environment is the separation of the responsibilities of origination, approval, transmission (release) and reconciliation of wire activity. It is also extremely important that system access be strictly controlled to protect against unauthorized activity. The ability to validate the authenticity of instructions, particularly non- repetitive instructions received by telephone or facsimile, is of critical importance. Separation of duties and system access requirements should be set forth in clear EFT policies and procedures that have been communicated and are understood by all parties involved in EFT.

Regulation

As in all other areas of their business, broker/dealers are subject to rules and regulations concerning EFT. In particular, the passage of the USA Patriot Act has placed a much higher regulatory focus on the movement of money into and out of financial institutions. As a result, the electronic funds transfer system must have sufficient controls to ensure that funds are not transmitted to parties designated as "Specially Designated Nationals (SDN's) and Blocked Persons" or to countries subject to sanctions and embargos.

In 1995 the Treasury Department promulgated a "Joint Rule" and related "Travel Rule" under the Bank Secrecy Act. Among other things it requires all financial institutions to maintain certain information regarding funds transfers of $3,000 or more and to include the required information in the transmittal of funds.

For further information and guidance concerning anti-money laundering requirements reference is made to the Audit Guidelines for Anti-Money Laundering, dated April, 2002.

Risks

Frequently individual transactions in an electronic funds transfer environment represent significant monetary value. When coupled with the liquid nature of the assets involved and the speed with which the transactions take place, it is apparent that electronic funds transfer will represent a high-risk area to most firms. For purposes of this Guideline the risks have been separated into four general categories.

Operational/accounting and fraud risk is the potential for an organization to suffer unexpected financial loss or to have inaccurate books and records. Fraud risk, which could result in significant financial loss, is a particular concern in an EFT environment. Once funds have been erroneously or fraudulently moved it may be difficult, if not impossible, to recover them. At a minimum, the organization is likely to incur financing costs during the time that the funds are being recovered.

Regulatory risk is particularly prevalent in the current time because of the regulatory focus on anti-money laundering. The rapidity, complexity and relative anonymity of electronic funds transfers make it an attractive vehicle for illegal enterprises to move money.

Reputational risk exists when firms are not able to execute customer requests to transfer funds timely. In addition, high profile problems with monetary transactions, such as not detecting money laundering activities or fraudulent funds transfers, can severely damage a firm's reputation and erode the confidence of its customer base.

Technology risk is pervasive in electronic funds transfer since it is a systems driven process. Ensuring that only authorized individuals can affect money movements and that adequate segregation of duties exists to prevent one individual from having end-to-end control of the process is imperative.

Audit Guidelines

The following guidelines are presented to assist the internal auditor in conducting a review of electronic funds transfer activities. It is important to note that these guidelines are general in nature and do not necessarily represent an exhaustive set of procedures for auditing electronic funds transfer. Judgment should be exercised when determining the specific procedures to be performed and those procedures should be tailored to the environment being reviewed. Certain activities covered in this Guideline may be addressed in a more comprehensive manner in other Guidelines dealing specifically with the subject activity (e.g., Anti-Money Laundering).

II A. AUDIT GUIDELINES

This guideline is intended to provide members of the Securities Industry Association, Internal Auditors Division, with information for the purpose of developing or improving internal audit programs. The information is designed to provide guidance to member firms in the preparation of procedures tailored to the specific needs of their individual environment. Internal auditors should always use professional judgment in determining the specific procedures to complete audit steps.

The numbered references in the "Risks to be Managed" section of the following tables are a cross-reference to the "Electronic Funds Transfer Flowchart" included on page 15. These references are included for informational purposes and can be used to determine the potential areas of electronic funds transfer that may be affected.

Operational/Accounting and Fraud Risk

Risks to be Managed	***Types of Controls to Manage or Eliminate Risks***	***Potential Audit Work Step***
Erroneous or fraudulent wire transfers may be transmitted • Transfers are not supported by properly authorized documentation. • Access to the electronic funds transfer system is not restricted to authorized personnel. • The wire transfer process does not adequately provide for segregation of duties between request, authorization, input and transmittal. • Wire transfer amounts are not recorded properly on the books and records. • Reconciling differences and suspense amounts are not researched and resolved on a timely basis. (1 - 14, 20 – 23)	• Funds transferred are supported by properly prepared and approved requests completed by the business unit. • Call back procedures are employed to verify instructions received via facsimile or telephone or for amounts in excess of pre-determined levels. • Secondary approvals are required for funds transfers exceeding pre-established amounts.	• Select a sample of funds transfers originating from various business units and: ♦ Determine that transfers have been properly requested and approved. ♦ Evaluate whether or not approval levels are adequate in light of the dollar level of transfers. ♦ Verify that call back procedures have been followed in all applicable circumstances. ♦ Compare funds transfer details to confirmation sent to the customer. ♦ Ascertain that confirmations/call back procedures are performed by someone independent of funds transfer processing.

Operational/Accounting and Fraud Risk

Risks to be Managed	*Types of Controls to Manage or Eliminate Risks*	*Potential Audit Work Step*
	• The funds transfer system may only be accessed by authorized individuals. • The functions of input, verification, approval and transmittal are appropriately segregated.	• Verify that the funds transfer system may only be accessed by authorized individuals. • Review system reports detailing individuals wiring funds to determine that only authorized personnel are, in fact, doing so. • Through observation and testing ascertain that the functions of input, verification, approval and transmittal are segregated.
	• Standing payment instructions are: ♦ Only established or modified by someone independent of funds transfer processing. ♦ Must be supported by written instructions from the payee.	• Obtain a report of standing payment instructions established in the funds transfer system: ♦ Determine that the instructions have been properly set up. ♦ Verify that the instructions have been properly approved. ♦ Compare instructions to written request from payee and verify that the request was signed by a duly authorized individual. ♦ Determine that individuals who establish standing payment instructions are independent of funds transfer processing.
	• Adequate security exists over funds transfer terminals: ♦ Terminals are located in restricted access areas. ♦ Terminals have automatic time out functions when not in use.	• Observe physical security over terminal access and determine that: ♦ Terminals are located in areas that are restricted to authorized personnel. ♦ Terminals are equipped with automatic time out functionality when not in use. ♦ Passwords are masked during input. ♦ Passwords are not openly displayed elsewhere.

Operational/Accounting and Fraud Risk

Risks to be Managed	*Types of Controls to Manage or Eliminate Risks*	*Potential Audit Work Step*
	• The funds transfer system produces daily exception reports, such as wire rejects and DK's, and: ◆ Exceptions are researched and resolved timely. ◆ Someone independent of funds transfer processing reviews the reports and resolutions.	• Review a sample of daily exception reports and: ◆ Verify the accuracy of the reports. ◆ Determine that exceptions are researched and resolved correctly and on a timely basis. ◆ Ascertain that reports are reviewed and approved by someone independent of funds transfer processing.
	• Funds transferred are reconciled to accounting records and bank statements by someone independent of transfer processing. • Reconciliations are reviewed and approved by a supervisory person to ensure propriety and that differences are resolved timely. • Unreconciled differences are booked to suspense accounts after seven business days. • Management reports of aged suspense account items are produced and reviewed on a regular basis. • As a best practice, funds transfer employees should be: ◆ required to take two consecutive weeks of vacation. ◆ Subjected to periodic (e.g., annual) background check.	• Review and test reconciliations of funds transferred to accounting and bank statements: ◆ Determine that reconciliations are reviewed and approved by someone independent of funds transfer processing. ◆ Verify that reconciliations are accurate. ◆ Test accuracy and timeliness of difference resolution. ◆ Determine that unreconciled differences are booked to suspense accounts on a timely basis. ◆ Review suspense accounts for proper aging and investigate old outstanding items. ◆ Review management reports of aged suspense account items for completeness and accuracy. • If firm policy, verify that funds transfer employees: ◆ Have taken two consecutive weeks of vacation within a year. ◆ Have had background checks within the past year.

Regulatory Risk

Risks to be Managed	*Types of Controls to Manage or Eliminate Risks*	*Potential Audit Work Step*
Failure to comply with the rules and regulations regarding electronic funds transfer activities will expose the organization to regulatory sanctions. • Supervision and control (NYSE Rule 342) requires that all activities must be adequately supervised by a responsible individual and that written procedures must be maintained. • Unreconciled differences and suspense items might result in increased Net Capital charges (SEC Rule 15c3-1) or Reserve Requirements (SEC Rule 15c3-3). • The USA Patriot Act requires financial institutions to verify that the recipients of funds transfers do not appear on OFAC lists.	• EFT activities are supervised by a responsible individual with no funds transfer responsibilities. Supervisory activities include: ♦ Review of exception reports. ♦ Review of reconciliations. ♦ Approval of system authority levels. • Written procedures are complete and up to date, outlining roles and responsibilities. • USA Patriot Act and Bank Secrecy Act compliance: ♦ For customer funds transfers equal to or greater than $3,000 the appropriate information is forwarded to the recipient bank. Information that must be forwarded includes the name and account number of the transmittor, the identity of the transmittor's financial institution and the identity of the recipient's financial institution. For further information reference is made to NASD Notice to Members 97-13. ♦ The funds transfer system prohibits the wiring or receiving of funds to or from anyone appearing on the OFAC lists.	• Review supervisory controls over EFT activity: ♦ Verify management review and approval of exception reports and reconciliations. ♦ Review process over granting authorization to users. ♦ Confirm that supervisory individual has no funds transfer processing capability. • Assess adequacy of written procedures and determine that they are being followed. • Determine that capital charges are accurately taken for aged differences. • Test a sample of funds transfers of $3,000 and over to determine that appropriate information is obtained and transmitted. • Evaluate the effectiveness of system controls over identification and blocking of wires to recipients on the OFAC list. • Review results of the independent review of compliance with the USA Patriot Act to ascertain if there were any issues related to funds transfer activities.

Regulatory Risk

Risks to be Managed	*Types of Controls to Manage or Eliminate Risks*	*Potential Audit Work Step*
• Bank Secrecy Act requirements to collect and transmit certain information on fund transfers of $3,000 or more ('Travel Rule'). • Customer information is not adequately protected from misappropriation. (Entire flow)	♦ See Anti-Money Laundering Audit Guideline for further information on risks, controls and audit work steps, including the identification, escalation and reporting of suspicious activity. • Privacy of customer information: ♦ Customer information is safeguarded from misappropriation. ♦ Individuals requesting customer information are required to provide data known only to the customer (e.g., personal identification number) prior to the release of the requested information.	• Ascertain that physical safeguarding of customer information is adequate to prevent unauthorized access. • Verify that customer information is only provided after authentication of the requestor.

Reputational/Legal/Other Risks

Risks to be Managed	*Types of Controls to Manage or Eliminate Risks*	*Potential Audit Work Step*
• Reputational: Inability to process customer funds transfers accurately and timely can result in damage to a firm's reputation and loss of customer confidence.	• Electronic funds transfer requests are time stamped upon receipt and upon completion. • Electronic funds transfer requests are reconciled/verified to actual transfers. • See Regulatory Risk section for controls and procedures related to compliance with laws and regulations.	• Evaluate timeliness of completion of funds transfer requests. • Verify that totals of funds transferred are reconciled to transfer requests.
• Legal: Inadequate legal documentation may result in the inability of the organization to exert a legal claim. ♦ Legal contracts are not up to date or executed by both parties. ♦ Contracts have not been reviewed or approved by the Legal Department.	• Legal contracts are up to date and executed and have been approved by the Legal Department.	• Ensure that legal contracts are up to date, signed and approved by Legal.
• Insurance: Inadequate insurance coverage may prevent the firm from recovering losses incurred through fraudulent funds transfer activity. (Entire flow)	• Insurance coverage is sufficient in light of the size and level of activity. • Employees involved in funds transfer processing are bonded.	• Review adequacy of insurance coverage. • Verify that employees are properly bonded.

Technology Risk

Risks to be Managed	*Types of Controls to Manage or Eliminate Risks*	*Potential Audit Work Step*
Technology risk can lead to unauthorized system access and inappropriate authority levels as well as to loss of system availability: • System access is not appropriately restricted to authorized personnel. • Authorized users have the authority to perform functions that are not in line with their duties and responsibilities. • Authority levels do not provide proper segregation of duties between origination, verification, approval and transmission of wires. • System program changes are not sufficiently controlled.	• A responsible individual (e.g., system administrator) with no electronic funds transfer capability controls all system access. • Authority levels for users are established by the system administrator commensurate with their duties and responsibilities (i.e., no incompatible duties). • System access and authority level reports are periodically produced and reviewed by appropriate business managers to ensure access remains appropriate. • Individual user ID's and passwords are required. • ID's and passwords must be changed frequently. • The system limits the number of unsuccessful log-on attempts and rejected transfer input attempts. • Daily reports of all unsuccessful log on attempts are produced and reviewed by the system administrator. • Programmed controls automatically log system changes. • System changes are only made through an established change control process.	• Determine that the system administrator has no other EFT capability. • Obtain system reports of user access and authority and: ♦ Determine that only appropriate personnel have system access. ♦ Ensure that user authority levels are commensurate with their roles and responsibilities. ♦ Determine that an adequate segregation of duties exists with respect to the functions of input, verification, approval and transmittal. ♦ Ascertain that EFT personnel do not have access to bookkeeping and settlement systems. ♦ Reconcile access reports to payroll records. • Verify that system access reports are periodically produced and reviewed by appropriate business managers. • Select a sample of former employees who had system access and ascertain that their access was removed on a timely basis. • Ensure that user ID's and passwords are required and must be changed frequently. • Verify that the system limits log-on and input attempts. • Verify that system exception reports of failed log on's are reviewed daily. • Review logs of system changes and verify that changes are made through an established change control process.

Technology Risk

Risks to be Managed	*Types of Controls to Manage or Eliminate Risks*	*Potential Audit Work Step*
• Disaster recovery is not adequate to ensure continued EFT capability. (15, 16, 17, 18, 19)	• Where broker/dealers access their bank's EFT systems via the Internet, sufficient security is established. ♦ Either Secure Socket Layer SSL) or Public Key Encryption (PKI) is utilized for authentication. ♦ System messages are encrypted. • For SWIFT environments, secure keys are used to validate authenticity.	• Evaluate adequacy of system security over internet connections to the bank's EFT system. • Determine that secured keys are used to authenticate SWIFT users and that they are adequately safeguarded from unauthorized users.
	• Business continuity and disaster recovery plans exist and have been approved and tested	• Verify the existence and regular testing of a Business Contingency Plan. • Evaluate the adequacy of the back up plan in case of system unavailability.

II B. SEGREGATION OF DUTIES CHECKLIST

Introduction

Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will not be prevented and remain undetected. The basic idea underlying segregation of duties is that no one employee or group of employees should be in a position both to perpetrate and to conceal errors or irregularities in the normal course of their duties. Additionally, errors may occur due to inadequate supervision of employee activity. In general, the principal incompatible duties to be segregated are: authorization, custody of assets, and recording or reporting of transactions. In addition, the risk management function as well as other oversight functions (Controllers, Compliance, Legal, Credit) should be separated from the functions that are originating risk itself and the processing of a transaction.

A practical method for using this checklist is to list the names of individuals responsible for particular functions. Review the checklist for individuals whose names are listed more than once and then make a determination whether that represents a potential lack of segregation of duties. Also consider whether individuals are performing incompatible duties. Once an individual is identified as performing incompatible duties, all duties performed by that individual should be challenged as to whether the effectiveness of those duties is reduced or eliminated by the lack of segregation of duties identified. Larger organizations may find it sufficient to list only the department performing each of these duties or functional job titles, rather than the names of individuals. Those companies could then evaluate whether any departments were performing incompatible duties.

Keep in mind that not all instances where an individual performs more than one function represent a lack of segregation of duties. In addition, it is important to remember that there is a possibility of a lack of segregation of duties within the same category. Consequently, completion of this checklist is intended to highlight potentially conflicting duties, not to be the only method of identifying all such conflicting duties. The segregation of duties checklist is located on the following page.

SEGREGATION OF DUTIES CHECKLIST

System Access and Authority

Who is responsible for granting EFT system access? _____

Who establishes user authority levels? _____

Who approves system access and user authority levels? _____

Who reviews system access reports? _____

Who has access to EFT system terminals? _____

_____

Funds Transfer Initiation, Approval and Transmittal

Who initiates requests for wire transfers? _____

Who approves requests for wire transfers? _____

Who validates the authenticity of wire transfer requests? _____

Who inputs wire transfer requests? _____

Who verifies and authorizes wire requests after input? _____

Who transmits wire transfer requests? _____

Who reviews resolution of wire transfer exceptions? _____

_____

Standing Payment Instructions

Who requests establishment of standing payment instructions? _____

Who approves establishment of standing payment instructions? _____

Who establishes standing payment instructions? _____

Who verifies accuracy of standing payment instructions? _____

Who maintains standing payment instruction database? _____

_____

Booking and Accounting for EFT Transactions

Who reconciles funds transfer requests to the accounting records? _____

Who reconciles funds transfer bank accounts to bank statements? _____

Who reviews and approves reconciliations of funds transfer requests to accounting records and bank statements? _____

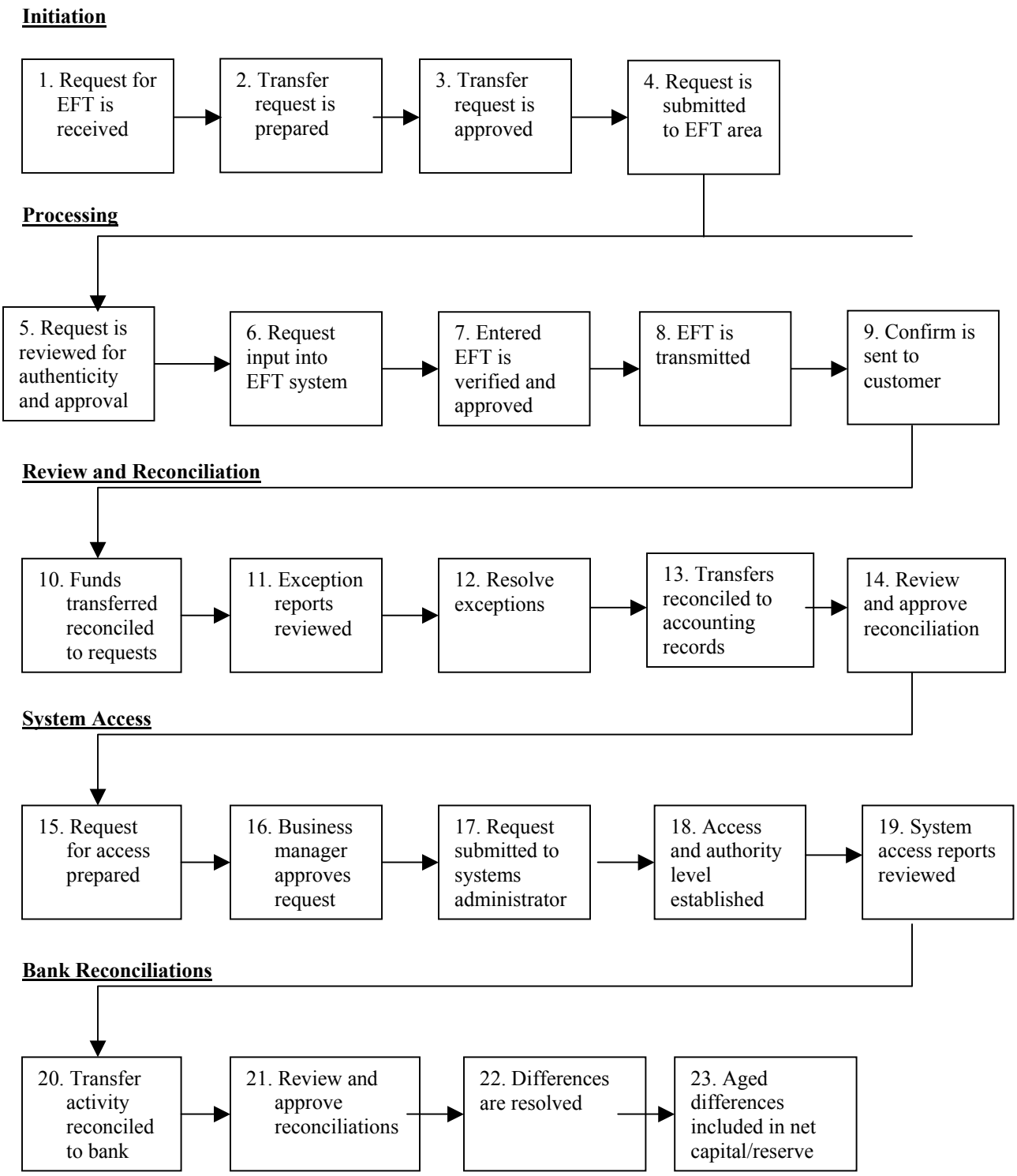
Who monitors resolution of differences and suspense items? _____

Who maintains the books and records concerning electronic funds transfers? _____

III. ELECTRONIC FUNDS TRANSFER FLOWCHART

The following flowchart illustrates some of the typical activities that take place in an electronic funds transfer environment. Definitions for the individual process steps are included below. Such definitions are numbered in order to cross-reference with the appropriate process steps.

Electronic Funds Transfer Diagram Flowchart



Definition of Process Steps

1. The business unit receives request for electronic funds transfer. May be received from customer or may arise out of routine business practices (e.g., government securities settlements, RVP transactions, etc.). Requests from customers should be in writing, signed by the customer.
2. Business unit prepares EFT request form.
3. Business unit manager approves EFT request form. Secondary approval may be required if monetary value exceeds preestablished levels.
4. Approved request is submitted to EFT processing group.
5. Request is reviewed for proper authenticity and approvals.
6. EFT is set up on the system.
7. Individual independent of input verifies accuracy of input and approves.
8. EFT is transmitted. This may be done by a third person who is independent from input and verification.
9. Confirmation of the transfer is sent to the customer. Typically the confirmation is generated automatically and sent by an independent group.
10. Daily reconciliation is performed of funds transferred to transfer requests.
11. Someone independent from input, verification and transmittal reviews exception reports of rejects and differences.
12. Exceptions are resolved and corrected.
13. Funds transferred are reconciled between system totals and accounting records by someone independent of transfer processing.
14. Reconciliation is reviewed and approved.
15. Request for system access form is prepared for individuals requiring access.
16. Appropriate business manager approves access request form.
17. Access request form is submitted to system administrator.
18. System access and authority level is established after determining that authority level is consistent with the individual's responsibilities.
19. System generated reports showing who successfully accessed system and who unsuccessfully attempted to access system are reviewed by the system administrator. Periodically, reports detailing who has system access and the level of their access are sent to the business managers for verification.
20. Someone independent of transfer processing duties reconciles transfer activity to the bank account.
21. Reconciliations are reviewed and approved.
22. Differences are resolved.
23. Aged reconciling and suspense items are included in the net capital computation and the reserve formula as appropriate.