As of January 6, 2012, this guidance applies to federal savings associations in addition to national banks.*

Comptroller of the Currency
Administrator of National Banks

Asset Management Operations and Controls

Comptroller's Handbook

January 2011

*References in this guidance to national banks or banks generally should be read to include federal savings associations (FSA). If statutes, regulations, or other OCC guidance is referenced herein, please consult those sources to determine applicability to FSAs. If you have questions about how to apply this guidance, please contact your OCC supervisory office.

AM

Asset Management Operations and Controls

Table of Contents

Asset Management Operations and Controls — Overview

This booklet provides guidance applicable to core Asset Management operations functions and to internal controls and processes used by national banks to manage risks associated with Asset Management activities. One of a series of specialized booklets in the *Comptroller's Handbook*, this booklet supplements the overall guidance provided in the "Large Bank Supervision," "Community Bank Supervision," and "Asset Management" booklets of the *Comptroller's Handbook*. This booklet provides expanded examination procedures when specific products or risks warrant review beyond the core assessment. Related booklets in the *Comptroller's Handbook* include "Personal Fiduciary Services," "Retirement Plan Services," "Custody Services," "Investment Management Services," "Internal and External Audits," and "Internal Control."

Background

Asset Management consists of an array of bank services, such as custody, investment management, trust and estate administration, retirement plan administration and participant record keeping, and corporate trust administration. The types of Asset Management customers serviced by a bank are diverse (e.g., individuals, retirement plans, corporations, mutual funds, investment managers, insurance companies, endowments, and foundations), as are the capacities in which a bank acts on behalf of these customers (e.g., trustee, agent, or custodian). Many of these customer and account types have specialized legal, processing, accounting, and reporting requirements. This booklet focuses on core processes applicable to most account types.

Asset Management operations serves as the "back office" for a bank's Asset Management activities and plays an important role in fulfilling a bank's strategic goals. Asset Management operations should implement efficient processes and systems capable of supporting the types of Asset Management accounts, clients, and assets that the bank services. These processes and systems should be capable of providing timely and detailed account information to management, customers, regulatory agencies, and other authorized parties, such as accountants or co-fiduciaries.

Asset Management operations moves and controls cash balances, marketable securities, and tangible assets. This results in a heightened risk of loss due to error or theft. The market volatility of assets being processed may increase the impact of such losses. As a result, a strong system of internal controls is required. In addition, Asset Management operations often supports systems and processes integral to overall risk management and compliance processes for Asset Management services.

This booklet provides guidance related to core Asset Management operations functions and core Asset Management accounting systems. These core functions include safeguarding assets, servicing securities, processing cash and securities transactions, maintaining internal controls, record keeping and reporting, and record retention. This booklet addresses these functions in detail.

Core Asset Management accounting systems support these core functions by maintaining

- account and asset master files,
- account level asset and cash positions,
- department-level asset and cash positions, and
- securities movement and control (SMAC) capabilities.

These systems process such transactions as interest and dividend payments, cash receipts, disbursements, and fees. They can track key events and produce client statements and regulatory and management reports.

Banks may also rely on specialized systems for specific lines of business, services, asset types, or functions. Examples include retirement plan participant recordkeeping, document custody, natural resource accounting, tax preparation, performance measurement, performance attribution, or fund accounting. Many of these systems have automated data feeds or interfaces with the core Asset Management accounting system and therefore affect core functions. While this booklet does not specifically address these specialized functions and systems, the principles discussed are applicable.

Asset Management operations may be performed in-house or outsourced, fully or in part, to an affiliate[1] or to an unaffiliated third party. Regardless of

---

[1] If the bank provides Asset Management operations through an affiliated entity for which the OCC is not the primary functional regulator, the supervisory approach should be discussed with the Asset Management examiner and bank examiner-in-charge (EIC) before commencing any type of examination activity for such an entity. The "Large Bank Supervision," "Asset Management,"

where specific operational functions are performed, the board and management are responsible for the oversight of Asset Management operations. This includes maintaining a strong control environment, effective policies and procedures, a robust audit process, and a sound vendor management program.

The size and complexity of a bank's Asset Management activities affect a bank's specific organizational structure, internal processes, and choice of Asset Management accounting systems. The resulting systems and controls should accomplish the following:

- adequately safeguard assets;
- ensure the accuracy and reliability of accounting data;
- provide timely information for management and clients;
- maintain adequate levels of operating efficiency;
- ensure compliance with laws, rules, regulations, and bank policies; and
- accommodate new financial products/services and future growth.

Certain basic controls should always be present. These include separation of duties, effective accounting controls, joint custody or control of assets, appropriate delineation of authority, and an effective SMAC system.

Risks Associated With Asset Management Operations

Risk, from the OCC's supervisory perspective, is the potential that events, expected or unexpected, may adversely affect a bank's capital, earnings, or franchise/enterprise value. Asset Management activities can expose the bank to direct financial loss when a bank fails to fulfill its fiduciary or contractual responsibilities. Asset Management activities can also lead to litigation, lost business, and failed strategic business initiatives. Losses from Asset Management operations are typically the direct result of error, fraud, or theft. Most can be attributed to inadequate internal controls, weak risk management systems, inadequate training, or deficient board and management oversight. The "Asset Management" booklet of the *Comptroller's Handbook* provides extensive guidance on the risks associated with offering Asset Management services. The booklet also explains the OCC's expectations for effective risk

---

"Investment Management Services," and "Related Organizations" booklets of the *Comptroller's Handbook* and the *Comptroller's Handbook for Asset Management* provide OCC supervisory policies relating to functional supervision.

management for Asset Management activities. Asset Management operations plays an integral role in a bank's risk management through the use of effective internal controls, the execution of many aspects of the bank's product delivery and strategic initiatives, and by providing appropriate management information systems (MIS) reports that support effective management oversight.

Within the framework of the OCC's risk assessment system, national bank Asset Management activities expose a bank to operational, reputation, strategic, compliance, and credit risk. Effective Asset Management operations can limit exposure to operational risk and assist in the management and mitigation of other risks associated with Asset Management activities.

Operational Risk

Operational risk is the risk to current or anticipated earnings or capital arising from inadequate or failed internal processes or systems, the misconduct or errors of people, and adverse external events. The Asset Management products and services offered by a bank, and, specifically, the functions performed by Asset Management operations, have inherent operational risk. Many of these functions, particularly those related to securities processing, include high-volume and time-sensitive transactions. Because Asset Management operations controls the movement of cash and securities, effective internal controls are needed to minimize losses due to error, omissions, and fraud.

Losses and litigation from Asset Management operations are typically the result of

- errors or delays in processing trades, corporate actions, and other transactions;
- improper controls over reconciliations;
- fraud;
- inadequate integration of mergers/acquisitions;
- inadequate due diligence and oversight of third-party technology products and services; and
- systems that do not adequately address the specific business requirements or volume of Asset Management services offered.

Such losses, individually and in the aggregate, can potentially be significant.

As with other lines of business, effective oversight of product development, product delivery, transaction processing, systems development, and processing systems is essential to operational risk management for Asset Management. Poor product delivery, inadequate systems, and inadequate information security programs can create liability or result in lost business.

Banks that are subject to the Advanced Measurement Approach (AMA) for Operational Risk under Basel II must calculate an Operational Risk capital charge. To determine the required capital charge under the AMA framework, banks must use internal loss data, external loss data, business environment and internal-control factors, and scenario analysis. The use of internal loss data requires the bank to capture and categorize internal operations losses, including those associated with Asset Management activities. See OCC Regulation 12 CFR 3, Appendix C "Capital Adequacy Guidelines for Banks."

Reputation Risk

Reputation risk is the risk to current or anticipated earnings, capital, or franchise/enterprise value arising from negative public opinion. A bank's failure to properly service an Asset Management account, or, when applicable, a bank's failure to meet its fiduciary obligations can damage the bank's reputation and expose the institution to litigation, financial loss, or the loss of current or prospective customers.

Asset Management operations encompasses highly visible transaction-based aspects of Asset Management services, including the systems that house information obtained from or reported to customers. As a result, Asset Management operations can be a source of reputation risk. A lack of security over customer information, either internally or through a third-party service provider, not only exposes a bank to reputation risk but also may elevate compliance risk.

Strategic Risk

Strategic risk is the current and prospective risk to earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. The risk level depends on the compatibility of an organization's strategic goals with the business strategies developed to achieve these goals, the resources deployed toward these goals, and the effectiveness with which business strategies are implemented. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capabilities. An Asset Management organization's ability to effectively deploy new products, benefit from emerging technology, and meet growth and efficiency objectives is dependent on a well-managed operations group with sufficient, qualified staffing and other resources to carry out these initiatives.

Compliance Risk

Compliance risk is the risk arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, internal policies and procedures, client agreements and other contractual arrangements, or ethical standards. Compliance risk is a significant factor in the overall risk management framework for Asset Management activities. OCC Regulation 12 CFR 9 provides comprehensive requirements for fiduciary accounts, which are also subject to fiduciary principles and other applicable law. Various booklets of the Comptroller's Handbook and OCC Bulletins set forth OCC expectations for Asset Management activities and are referenced at the end of this booklet. The Asset Management area is also impacted by a number of other federal and state laws and regulations, such as the Employee Retirement Income Security Act (ERISA), the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) laws, tax laws, information security and privacy laws, securities laws, and Internal Revenue Service (IRS) and U.S. Department of Labor regulations.

Asset Management operations is typically responsible for maintaining the systems and data required to produce and safeguard the reports and records needed to comply with the various laws and regulations applicable to a bank's Asset Management activities. Examples include

- reports to meet OCC Regulation 12 CFR 12 record keeping and confirmation requirements.
- Schedule RC-T "Fiduciary and Related Services" of the bank's Consolidated Reports of Condition and Income.
- reports to comply with record keeping and reporting requirements of the Bank Secrecy Act.
- IRS withholding and information reports (1099s, 5500s, etc.).
- court accountings.
- state escheatment reports.

- quarterly information reports filed with the U.S. Securities Exchange Commission (SEC).
- shareholder communication reports.

Asset Management operations also produces reports that enable management to identify exceptions to laws, regulations, and internal policies and procedures and to monitor compliance with specific guidelines or thresholds set by management. Failure to maintain proper records and file the necessary reports may result in monetary penalties or other regulatory sanctions and may also damage a bank's reputation.

Credit Risk

Credit risk is the risk arising from an obligor's failure to meet the terms of any contract with a bank or otherwise perform as agreed. Credit risk is present in activities that depend on a counterparty, issuer, or borrower to meet contractual obligations. Credit risk arises when funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether reflected on or off the balance sheet. Asset Management operations activities may expose a bank to counterparty credit risk. For example, banks may incur credit risk when settling trades on behalf of clients, advancing payments to client accounts, even on an intra-day basis, or permitting overdrafts in client accounts. Exposure to credit risk should be considered when selecting settlement arrangements and evaluating the use of depositories and third-party custodians. Exposure to counterparties through Asset Management operations should be considered as part of the bank's overall credit risk management program.

Board and Management Supervision

A bank's board of directors must establish the bank's strategic direction and risk tolerances. In carrying out these responsibilities, the board should approve policies that set operational standards and risk limits. Well-designed monitoring systems allow the board to hold management accountable for operating within established tolerances. Bank management is responsible for the implementation, integrity, and maintenance of risk management systems. Management should establish and maintain effective risk management and compliance programs that enable the bank to meet statutory and regulatory requirements. The programs should include effective policy guidance and an effective system of internal controls in the Asset Management area. The programs should provide the capability to respond to changes in the bank's operating environment and conditions, changes in market conditions, and changes in laws or regulations.

The board should ensure that its internal audit program provides an objective and independent review of Asset Management activities, internal controls, and management information systems. A national bank that exercises fiduciary powers must, under the direction of its fiduciary audit committee, arrange for a suitable risk-based audit of its significant fiduciary activities as described in OCC Regulation 12 CFR 9.9. Further, Asset Management activities should be considered in determining the scope of independent testing required by the BSA. For additional discussion of audits and internal controls see the "Internal Control" and "Internal and External Audit" booklets in the *Comptroller's Handbook*.

Risk Management

The risk profile of Asset Management operations is affected by the volume of transactions and accounts; the complexity of the bank's Asset Management products; and the capabilities of its processes, systems, and people. Management is responsible for the implementation, integrity, and maintenance of risk management systems commensurate with the risk profile of Asset Management operations. Management must

- keep the board of directors adequately informed about risk-taking activities;
- implement the bank's strategy;
- ensure that strategic directions and risk tolerances are effectively communicated and adhered to; and
- oversee the development and maintenance of a Management Information System to ensure that information is timely, accurate and pertinent.

Risks within Asset Management operations should be considered when determining the appropriate level of fidelity, errors and omission, fiduciary liability, or other types of insurance at the bank or holding company level.

Management should develop and implement and the board should approve well-defined policies commensurate with the nature, size, and complexity of the bank's Asset Management activities. Policies should set standards and may recommend courses of action. These policies should be reflected in procedures that set forth how daily activities are carried out. They should include or be supplemented by efficient workflows with appropriate segregation of duties, independent controls, and the ability to measure how well these processes and controls are managing core functions. Policies and procedures should make clear which persons are authorized to perform or approve various actions, how policy exceptions should be reported, and who is authorized to approve such exceptions.

The information technology (IT) environment supporting Asset Management operations has a significant impact on the risk profile of Asset Management operations, affecting the level of operational, strategic, and reputation risk. Various components of this environment may be controlled by an enterprise level IT area, within Asset Management operations, or by a third-party servicer. Asset Operations should ensure that those aspects of the IT environment it controls, either directly or through oversight of a third-party servicer, conform to the bank's policies, standards, procedures, and to applicable banking regulations and guidance. Because IT projects, upgrades, enhancements, and the selection and oversight of IT service providers may be controlled at the enterprise level, effective communication between management in Asset Management operations and the IT area is critical to ensure that strategic business objectives are being met and enterprise standards are being adhered to.

Strategic initiatives—such as mergers, acquisitions, consolidations, outsourcing initiatives, the introduction of new technology-enabled products, and technology upgrades and enhancements—affect the risk profile of Asset Management operations. Management should ensure that these initiatives are implemented effectively with appropriate due diligence and project management and that the necessary oversight, resources, staffing, training, procedures, and controls are provided.

For additional discussion of risk assessment and the internal-control environment, refer to the "Bank Supervision Process," "Large Bank Supervision," "Community Bank Supervision," and "Internal Control" booklets of the *Comptroller's Handbook* and OCC Bulletin 2004-20 "Risk Management of New, Expanded, or Modified Bank Products or Services."

Compliance Management

Management should develop and implement and the board should approve policies, procedures, and monitoring systems designed to ensure that a bank's Asset Management activities comply with applicable laws and regulations. (See the Laws and Regulations headings in the Reference section of this booklet.) All laws and regulations applicable to the Asset Management line of business should be identified, addressed in policies and procedures, and communicated to the appropriate personnel. The bank should have systems to monitor compliance with applicable laws and regulations, including those listed below. Some of these laws and regulations apply directly to Asset Management operations. Other laws and regulations may be applicable to Asset Management account administration or investment management activities, but the systems to monitor compliance are often administered or supported by Asset Management operations.

These laws and regulations include

- 12 USC 92a, which governs the trust powers of national banks.
- OCC Regulation 12 CFR 9, which governs the fiduciary activities of national banks.
- laws and regulations implementing ERISA requirements for employee benefit accounts.
- various SEC regulations governing shareholder communications, investment adviser reporting, investment adviser custody, lost and stolen securities reporting, registered transfer-agent activities, and bank exceptions and exemptions from registration as a broker-dealer.
- BSA/AML record-keeping and reporting requirements, including customer identification and suspicious activity monitoring.
- Office of Foreign Assets Control (OFAC) regulations requiring that banks, block accounts and other property of specified countries, entities, and individuals, and that banks prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.
- information security and customer privacy requirements under the Gramm-Leach-Bliley Act (GLBA).
- OCC Regulation 12 CFR 12 transaction record keeping and confirmation requirements.
- 12 USC 161, which requires board attestation of reports of condition, including Consolidated Reports of Condition and Income Schedule RC-T "Fiduciary and Related Services."
- federal and state tax withholding and reporting requirements.
- state-abandoned property laws.
- state laws for transfer of real property.
- various applicable state laws governing fiduciary activities, including Uniform Principal and Interest laws, which provide guidance when the governing instrument is silent as to whether certain transactions are properly posted to a trust account's income or principal portfolio and

which address inherent conflicts between income and principal beneficiaries.
- domestic and foreign laws for cross-border activities.
- foreign tax regulations and reclaim practices.

Staffing

Capable management and appropriate staffing are key elements of effective risk management. If Asset Management operations staffing is inadequate, transactions may be poorly executed and controlled. The result may be losses due to error, increased exposure to internal fraud, litigation or settlements with clients, or loss of current or future business.

Recruitment and retention of experienced staff, adequate training, and the ability to manage turnover play a major role in a bank's ability to consistently provide high-quality and cost-effective performance in operations. When determining Asset Management operations staffing requirements, management should carefully consider the volume of business, the range and complexity of the services offered, and the bank's automation capabilities and related IT support requirements. When some or all of the Asset Management operations functions are outsourced, management should perform due diligence to ensure that the third-party service provider maintains adequate staffing and that sufficient staffing is retained in-house to oversee the service provider and to perform the functions that management has determined should remain in-house.

Oversight of IT and Third-Party Service Providers

Asset Management operations relies heavily on IT to accomplish its core functions and to provide information to management, clients, and other parties. Operations may also use separate systems for specific activities, such as

- performance reporting,
- performance attribution analysis,
- employee-benefit record keeping,
- shareholder servicing,
- corporate trust transfer or paying agencies,
- document custody,
- real estate management,

- mineral interest accounting,
- farm management,
- fiduciary tax preparation,
- automated investment reviews,
- OFAC transaction screening,
- BSA/AML record keeping and reporting, and
- suspicious activity monitoring.

In many cases, there are automated interfaces or file transfers between these systems and the core Asset Management accounting system.

These systems are typically licensed from a vendor or operated off-site by a third-party servicer. Some Asset Management organizations use internally developed systems for either their core asset management accounting or for one or more specialized processes. Whether a system is developed in-house or by a third party and whether a system is housed and operated in-house or by an affiliate or third party, effective IT management is essential.

In overseeing IT systems used by Asset Management, the board and management should ensure that

- the systems and technology support the bank's strategic goals and objectives for Asset Management and have the capacity to support current and anticipated transaction volumes and product complexity.
- the information and reports provided by these systems are timely, accurate, reliable, consistent, complete, and relevant.
- bank and customer information are adequately protected from unauthorized disclosure or alteration and are available when needed.
- business resumption and contingency plans are adequate, and data retention requirements are met.

Additional information on IT oversight can be found in the "Community Bank Supervision" booklet of the *Comptroller's Handbook*, and the "Operations" and "Management" booklets of the *FFIEC (Federal Financial Institutions Examinations Council) Information Technology Examination Handbook*.

MIS Reporting

Appropriate MIS reports are an integral part of a bank's risk management and compliance programs for Asset Management. These reports should provide pertinent and timely information in a form that enables the board, management, staff, auditors, and examiners to carry out their respective responsibilities. These reports should also enable management to

- measure operational performance against designated benchmarks.
- better identify the level of risk in Asset Management.
- assess the effectiveness of the department's risk management and compliance programs.
- in conjunction with the bank's financial accounting system or general ledger (GL), enable management to determine the financial performance of the Asset Management business line.

MIS reports should inform management about such essential matters as key risk indicators, policy exceptions, variances from established guidelines or thresholds, volume trends and fluctuations, and how effectively internal controls are working. Asset Management accounting systems typically make available an array of standard reports, which banks should evaluate and consider producing at appropriate intervals. Most systems also provide custom reporting tools or data extracts that enable Asset Management operations to develop and produce additional reports as needed. Reports can be developed to flag potential errors or missing information such as pricing variance or stale pricing reports. To ensure the integrity of these reports, procedures should be in place to maintain accurate account-, asset-, and system-level coding. In addition, bank-defined parameters for vendor-designed, servicer-generated, and internally developed reports should be tested and validated.

Outsourcing and Vendor Management

Banks often use third-party servicers to provide IT systems and to perform various operational and administrative functions to achieve various strategic objectives. Through effective use of third-party relationships for Asset Management activities, a bank may be able to expand or enhance its product offerings, diversify revenue sources, and access superior expertise. The use of a third-party provider for such activities may enable the bank to devote scarce internal resources to core business processes, increase operational efficiency and accuracy, and have greater flexibility in how the Asset Management operations area is structured. Management should ensure that when it chooses to use third-party servicers, it selects only those that meet management's requirements. The OCC expects banks to have an effective process to manage third-party service arrangements involving products or services used for Asset Management activities. For guidance on oversight of third-party servicers, refer to the "Outsourcing Technology Services" booklet of the *FFIEC Information Technology Examination Handbook*, OCC Bulletin 2001-47 "Third-Party Relationships," and OCC Bulletin 2002-16 "Bank Use of Foreign-Based Third-Party Service Providers."

Banks that use affiliated third-party service providers must have processes in place to ensure that such arrangements also comply with 12 USC 371c, "Banking Affiliates," and 12 USC 371c-1 "Restrictions on transactions with affiliates" as implemented by 12 CFR 223 (Regulation W) "Transactions between member banks and their affiliates." For example, affiliated third-party service provider arrangements must generally comply with the "market terms" requirement of Regulation W.

Business Continuity and Contingency Planning

A business continuity and contingency plan is an extension of a bank's system of internal controls and physical security. The plan should include provisions for recovery and continuity of operations in the event that such threats as terrorist acts or natural disasters damage or disrupt a bank's ability to operate. A bank that relies on a third-party servicer for data processing or other core business functions should take steps to determine whether the servicer's contingency plans, when combined with those of the bank, meet the bank's recovery requirements. Periodic testing of the plans is necessary.

A bank's board of directors is responsible for overseeing business continuity planning for all business lines, including Asset Management. Asset Management operations activities should be an integral part of a bank's business continuity plans for Asset Management services. The board should review and approve the bank's contingency plans annually. See the "Business Continuity Planning" booklet of the *FFIEC Information Technology Examination Handbook* for further information.

Information Security

Information security programs generally have two objectives, to protect the bank and to protect its customers. A fiduciary's duties of care and loyalty require that it protect the confidentiality of client information. In addition, all Asset Management activities of national banks are subject to OCC Regulation 12 CFR 30, Appendix B, "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" mandated by Section 501 of the GLBA. These guidelines require each institution to design a written information security program that suits its particular size and complexity and the nature and scope of its activities. The guidelines include a requirement that the board of directors, or appropriate committee of the board, approve the bank's information security program and oversee the program's development, implementation, and oversight.

The program should include oversight of the measures taken by service providers to protect customer information. Asset Management operations should be considered in the bank's risk assessment and in the development of the bank's information security program mandated by the GLBA.

Asset Management operations is typically instrumental in implementing the bank's information security program within Asset Management, particularly with respect to those aspects of the IT environment for which it is responsible. Often, Asset Management operations may also share responsibility for the design or operation of the information security program.

For further information, see the "Information Security" booklet of the *FFIEC Information Technology Examination Handbook,* OCC Bulletin 2001-8 "Guidelines Establishing Standards for Safeguarding Customer Information," OCC Bulletin 2001-35 "Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information," and OCC Bulletin 2005-44 "Small Entity Compliance Guide for the Interagency Guidelines for Establishing Information Security Standards."

Operational Controls

Management and the board of directors should ensure that there is a framework of policies, procedures, and workflows that establish effective internal control in all phases of Asset Management operations. OCC Regulation 12 CFR 30, Appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness," sets forth general operational and managerial standards for internal controls and information systems as well as internal audit systems that are applicable to both fiduciary and non-fiduciary accounts. A bank's failure to ensure adequate internal control over Asset Management operations is an unsafe and unsound practice. Additional information can be found in the "Internal Control" booklet of the *Comptroller's Handbook*. OCC Regulation 12 CFR 9 defines and sets forth a number of specific requirements for fiduciary accounts, several of which are directly applicable to Asset Management operations. For example, 12 CFR 9.13(a) requires joint custody over fiduciary assets and 12 USC 92a(c) and 12

CFR 9.13(b) require the separation of fiduciary assets from the assets of the bank.

To develop an effective system of internal controls, management should analyze and assess the nature of the specific operational activities and risks associated with Asset Management. Management should develop an overall system of policies, procedures, and practices that minimizes the likelihood of fraud and errors; enables timely detection of fraud and errors; and minimizes the adverse impact to the bank and its clients from fraud and errors.

Operational controls need to be comprehensive to ensure that the bank provides safe and sound support for the administration of client accounts. These controls need to be determined in light of the volume, complexity, and time sensitivity of Asset Management transactions. Key principles and specific regulatory requirements for Asset Management operational controls are summarized below.

Separation of Trust and Bank Assets

OCC Regulation 12 CFR 9.13 and 12 USC 92a(c) require that fiduciary account assets be kept separate from bank assets. To keep fiduciary and other client assets separate from the assets of the bank while on-premises, they should be maintained in an in-house vault facility controlled by Asset Management operations. Book-entry assets and assets maintained off-premises should not be comingled with bank assets. The records maintained and receipts issued by depositories, third-party custodians, or book-entry issuers must clearly indicate that securities are being held for the Asset Management clients of the bank, or when permissible by applicable law, registered in a nominee established for this purpose.

Note: The OCC has permitted banks to place their own investment portfolio assets under the control of a bank's own Asset Management division by establishing a formal custodial account for the bank, which is identified clearly as such on the Asset Management division's records. These securities may be placed along with other Asset Management customer securities with outside depositories or custodians. Under this arrangement, the outside depositories or custodians should only be permitted to recognize instructions from duly authorized Asset Management operations personnel under the joint custody procedures described below.

Segregation of Duties

Fundamental to effective internal control is the segregation of duties, which can reduce the risk of internal fraud and errors. No single person should be permitted to handle all aspects of a transaction or sensitive data changes.

A bank should segregate its administrative and portfolio management (front office) functions from its operational (back office) functions. Asset Management administrative and portfolio management functions relate to the fulfillment of the duties and responsibilities set forth in an account agreement. Examples of front office responsibilities include

- determining and directing distributions of funds to a trust beneficiary.
- gathering the assets in the estate of a decedent.
- determining how to carry out the responsibilities created in the account agreement.
- determining and implementing an account's investment objective.
- determining specific assets to be purchased, sold, or distributed.
- determining the appropriate response to voluntary corporate actions.
- initiating action and follow-up to ensure the bank fulfills its fiduciary duties.

In general, the front office authorizes transactions. Increasingly, banks are establishing "middle office" groups to improve controls by providing centralized expertise and further segregating certain activities from both the front and back office.

Asset Management operations (back office) functions typically include

- moving cash and securities at the direction of the front office.
- reporting and processing trades.
- posting transactions to internal accounting systems.
- maintaining account, asset and beneficiary data on internal accounting systems.
- safeguarding assets.
- preparing reports for clients, supervisory authorities, and management.
- performing internal-control functions such as reconciliations.

Within Asset Management operations, functions should be segregated so that no Asset Management operations staff members can move cash or assets on their own and that control processes, such as reconcilements, are performed by persons independent of those who process transactions.

Management should assess the risks and the control environment within Asset Management to ensure that appropriate policies, procedures, workflows, and system access controls establish an adequate segregation of duties. Segregation of duties can be accomplished through carefully designed workflows, procedures, and controls. Examples of effective controls include

- establishing system user profiles that limit user rights based on job functions.
- establishing multiple online approval levels for specific types of activities.
- restricting physical access to securities, checks, and online terminals.
- establishing independent written approval requirements for manual transactions.

In small organizations, certain functions may need to be performed by non-Asset Management employees to accomplish effective segregation of duties. When such segregation is impractical, management should demonstrate the implementation of effective compensating controls.

Joint Custody or Control

Another key internal control is joint custody or control, also referred to as dual control. Joint custody or control requires that assets (whether cash, securities, or tangible assets) are handled by, and transactions resulting in the movement of funds or assets are effected by, at least two authorized individuals. OCC Regulation 12 CFR 9.13 specifically requires that a national bank place assets of *fiduciary* accounts in the joint custody or control of no fewer than two of the fiduciary officers or employees who have been designated for that purpose by the board of directors. Physical items that represent substantial fraud risk, such as unissued checks, automated check-signing equipment, Medallion signature guarantee devices, and unissued securities held by corporate transfer agents, should also be maintained under joint custody or control.

Joint custody or control procedures are intended to ensure that one person, acting alone, does not have the ability to move or transfer funds or assets. This principle should be reflected in control procedures for physical securities from the time they are received from the client or client's agent until their ultimate authorized distribution. This principle also applies to securities processing and control functions that can lead to the disbursement of cash, or transfer of securities to or from a depository, sub-custodian, or book-entry account.

Asset Management accounting systems typically include "front-end" capabilities that can assist a bank in maintaining joint control over cash and securities. For example, systems may be configured to require the completion of two steps by different individuals to effect transactions that result in the disbursement of funds or in the movement of securities. Management should ensure that these system capabilities are fully understood and that workflows, system parameters, and user profiles are established to ensure joint custody of client assets on a day-to-day basis. To the extent that system controls are not available or are impractical, manual safeguards should be implemented to ensure joint custody.

System Administration

Limiting employee access to specific functions within the systems is an essential part of a bank's internal control system and can facilitate the segregation of duties and joint custody of assets. Determination of appropriate user profiles should be made based on a thorough analysis of the system's capabilities and the Asset Management division's risks, workflows, procedures, and internal control environment. To be effective, this analysis should consider all of the systems to which an individual may be granted access. For example, in many organizations, securities transactions can be initiated through both the Asset Management accounting system and through online access to a depository or sub-custodian's system. System records, such as transaction histories, logs, audit trails or similar reports, should be sufficiently detailed to determine which individuals have performed specific actions and when.

User profiles should be reviewed periodically, particularly as systems and workflows change. Management should approve these profiles and the assignment of profiles to specific individuals. Procedures should require that user access is promptly revoked or changed whenever a user's employment ends or assigned duties change and that user profiles assigned to each user are periodically reviewed. Refer to the "Information Security" booklet of the *FFIEC Information Technology Examination Handbook* for guidance on establishing and administering user passwords and other authentication mechanisms.

Individuals designated to input and monitor employee system access are often referred to as "security administrators." Because they have the ability to change system access, security administrators also have the ability to access and alter records. As a result, procedures should require timely and independent review of all activity entered by a security administrator (user setups and terminations, assignment of profiles to users, and specific profile changes). System logs or audit trails, which record the date and nature of specific activities taken by system administrators, are an important part of this process.

Internal Accounting Controls

Combined with appropriate segregation of duties and effective joint custody procedures, internal accounting controls should be implemented to ensure the accuracy of accounting records and the safety of assets. Internal accounting controls are used to monitor and control workflows, ensure the accuracy of those workflows, and flag unauthorized transactions. Internal accounting controls include input controls and reconcilements of cash, asset positions, asset changes, and suspense accounts. Internal accounting controls are among the core functions of Asset Management operations, to be discussed in detail in the next section.

Operations Core Functions

Safeguarding of Assets

Safeguarding client assets from loss, theft, or physical damage is a core function of Asset Management operations. Assets may be in physical or book-entry form and may be safe-kept either in-house or with a depository, third-party custodian (sub-custodian), or in a book-entry account with the issuer or its transfer agent. Asset Management operations is responsible for maintaining possession or control of assets and for accurately recording, on the Asset Management accounting system, the specific asset positions for each account, including a record of each asset's location and type of registration. In the course of settling purchases, sales, corporate actions, and other authorized transactions, Asset Management operations directs the receipt of assets from, and movement of assets to, authorized parties.

OCC Regulation 12 CFR 9.13 specifically requires that a bank maintain joint custody over assets held in a *fiduciary* account, that such assets be kept separate from bank assets, and that these assets are properly identified as the property of a particular account. U.S. Department of the Treasury Regulation 17 CFR 450, "Government Securities Act Regulations: Custodial Holdings of Government Securities," sets forth specific requirements for banks that hold government securities in a custodial capacity. This regulation provides an exemption from these requirements for national bank custodians if they have adopted policies and procedures that apply all of the requirements imposed by the OCC for government securities held in a *fiduciary* capacity to government securities held in a *custodial* capacity.

As a safe and sound practice, all client assets, whether held in a fiduciary or other capacity, should be maintained under joint custody or control, segregated from bank assets, and properly reflected on the Asset Management accounting system as the property of specific accounts. The custody of assets is addressed in detail in the "Custody Services" booklet of the *Comptroller's Handbook*.

On-Premises Custody

When physical assets are initially received from a customer, they are often, at least temporarily, safe-kept on-premises in a vault, safe, or similarly secure facility or cabinet ("vault"). From the time physical assets are received from the client or agent, they must be properly safeguarded and under the control of at least two employees. Typically, two front office employees take initial possession of physical assets, create a written record of the assets being received, and maintain joint custody until these assets are delivered to Asset Management operations. Asset Management operations is then responsible for safeguarding the assets under joint custody until the assets are either re-registered and filed for safekeeping in an on-premises dual-control vault or delivered to the appropriate off-premises safekeeping location. The on-premises dual control vault should provide security devices consistent with the minimum security requirements outlined in OCC Regulation 12 CFR 21, "Minimum Security Devices and Procedures, Reports of Suspicious Activities, and Bank Secrecy Act Compliance Program" and applicable law. In addition to security risks, physical hazards, such as fire and flood, should be considered when determining the location and physical characteristics of any vault used for on-premises asset safekeeping.

Vault custodians for fiduciary assets must be specifically designated by either name or title by the board of directors in accordance with OCC Regulation 12 CFR 9.13. Joint custody procedures should describe precisely the controls to ensure that any bank employee acting alone cannot physically have access to customer assets.

Tangible assets, such as coins, collectables, art, artifacts, and jewelry, should be placed in appropriate vaults or secured storage areas that ensure the safety of these assets and maintain their physical condition. Proper security movement and control records are needed to track movement of these assets in and out of vaults, including the temporary withdrawal of assets for appraisal or other authorized purposes.

Off-Premises Custody

To facilitate efficient securities processing, including timely and automated trade settlement, readily marketable physical securities are typically transferred to an off-premises depository or third-party custodian. There, to the extent that they are eligible, they are converted to book-entry securities registered in the name of the nominee partnership[2] (where authorized by applicable law) of the depository or third-party custodian. Physical securities that are not publicly traded are either safe-kept on-premises after being re-registered in the name of the bank's nominee partnership (where authorized by applicable law) or in the legal title of the account or are safe-kept in the vault of a sub-custodian. Procedures and workflows should be designed to ensure that proper control of assets is maintained throughout the process of re-registration and transfer of both marketable and closely held securities.

[2] Financial institutions typically establish one or more nominee partnerships, specifically for the purpose of registering securities held on behalf of its fiduciary and custody accounts in the name of the partnership, simplifying trade settlement and other aspects of securities processing. Nominee partnerships are discussed in detail later in this booklet.

OCC Regulation 12 CFR 9.13 permits a national bank to maintain fiduciary assets off-premises, if consistent with applicable law, and if the bank maintains adequate safeguards and controls. Banks typically use third-party depositories or custodians (sub-custodians) with access to depositories to provide cost-effective securities processing and to facilitate timely settlement of trades. These arrangements should be approved by the board of directors, which is responsible for ensuring that fiduciary assets are properly safeguarded and controlled.

When determining whether to use a depository or third-party custodian and when selecting a specific depository or third-party custodian, banks should consider the credit risk posed by this entity. If a depository or custodian fails, there is a chance that some or all of the cash or securities under the control of this entity may be at risk. As a result, banks considering off-premises custody must carefully evaluate the creditworthiness and market reputation of the organizations through which they settle trades and safe-keep the assets of their fiduciary and other clients. This assessment should consider membership standards, rules, and collateral requirements for depositories, as well as any applicable public or private insurance for third-party custodians. In addition to the guidance below, see Department of Labor Regulation 29 CFR 2550.412-1, "Rules and Regulations for Fiduciary Responsibility: Temporary bonding requirements" and Department of Labor Field Assistance Bulletin 2008-04 "Guidance Regarding ERISA Fidelity Bonding Requirements" for specific bonding requirements and exemptions for persons who handle ERISA property.

Off-site custody arrangements should be subject to initial and ongoing due diligence as well as a formal written custody agreement, which sets out the duties and responsibilities of the parties. Third-party depository and custody relationships should be managed in accordance with OCC Bulletin 2001-47 "Third-Party Relationships: Risk Management Principles," which sets forth the OCC's expectations for oversight and management of third-party relationships by the board of directors and bank management.

When using an off-premises depository or custodian, mutually agreed-upon procedures should be implemented by the off-site depository or sub-custodian to ensure adequate safeguards are in place and that the entity only moves securities at the direction of authorized Asset Management employees.

These assets should be maintained in an account that is designated for the bank's fiduciary and custodial clients, and by agreement with the third-party depository or custodian, should be free of all liens, charges, or other claims against the bank.

Depositories

Depositories were initially established to facilitate trading and securities processing by holding physical securities in a central location where changes in ownership were recorded on the books and records of the depository. This is commonly referred to as immobilization. Most marketable securities, including those issued in book-entry form, are now safe-kept in depositories because depositories provide efficient and cost-effective processes for securities safekeeping, trade settlement, income processing, and corporate action processing. The use of depositories has also accelerated the time between securities trades and settlement, reducing the risk of counter-party failure. Depositories can further mitigate counterparty risk by providing clearance and settlement services through which they employ various techniques to minimize exposure to participants and often act as a central counter-party. They impose rigorous membership standards, operating rules, and ongoing collateral requirements to secure each member's own obligations as well as certain liabilities of the depository in the event of another member's failure.

Over time, the evolution of the securities infrastructure in the United States has resulted in two major depositories—the Federal Reserve (for government securities) and the Depository Trust Company (DTC), a subsidiary of the Depository Trust and Clearing Corporation (DTCC) (for equities, corporate and municipal debt, government securities, collateralized mortgage obligations, exchange-traded funds, and other types of securities.) DTCC also provides clearing and settlement services through DTC, the National Securities Clearing Corporation (NSCC) and the Fixed Income Clearing Corporation (FICC).

There are a number of central securities depositories (CSD) outside the United States as well as international central securities depositories. These play an increasing role in the securities industry's migration toward automation, standardization, and streamlined settlement processes, not only in their various domestic markets but also with respect to cross-border trades.

Third-Party Custodians

Depending upon the volume and complexity of assets under management, the size and skill of its Asset Management operations staff, and the capabilities of a bank's Asset Management accounting system, it may not be cost-effective or appropriate for a bank to participate directly in a depository. As an alternative, many banks use other banks or registered broker-dealers that are direct participants in DTC or other depositories as sub-custodians. To facilitate cross-border securities settlement and servicing, local market sub-custodians or global custodians are typically used. Global custodians provide access to multiple local markets and CSDs throughout the world through a network of branches, affiliates and sub-custodians, also referred to as agent banks.

In considering whether it is preferable to access a depository directly or through a sub-custodian, management should compare the risks, costs, and benefits of direct participation in a depository with the risks, costs, and benefits of indirect participation through the use of a sub-custodian. This assessment should consider the Asset Management operations staffing levels and the internal expertise required under each arrangement.

When a bank utilizes one or more depositories or sub-custodians, the bank must establish an effective selection process and ensure that appropriate risk-mitigation controls are implemented and maintained. In addition to providing securities custody and settlement services, depositories and sub-custodians typically provide access to data-processing systems, which enable their clients to access information, transmit settlement instructions, and initiate the movement of securities or transfer of cash. These systems often interface with the bank's Asset Management accounting or other systems. Refer to the "Outsourcing Technology Service Provider" booklet of the *FFIEC Information Technology Examination Handbook*, for guidance on management and oversight of IT services, such as those provided by third-party custodians.

Banks that provide access to cross-border securities, either through direct participation in a local market CSD or by using overseas sub-custodians or a global custodian, should develop enhanced service provider selection, oversight, and reporting processes to cover the additional complexity and risks presented by overseas operations. These include divergent local settlement conventions, currencies, languages, financial regulations, and laws. Specific factors to consider when selecting a local market sub-custodian either directly or through a global custodian include the sub-custodian's position in the local market, its knowledge, experience, and expertise, and the likelihood of U.S. jurisdiction over, and the ability to enforce judgments against, a foreign sub-custodian.

Credit Risk/Bank Sub-Custodians

When using a domestic bank as a sub-custodian, the custody and related cash account at the sub-custodian should be titled in the name of the bank on behalf of its Asset Management clients so that assets remain segregated from any bank assets held by the custodian and applicable Federal Deposit Insurance Corporation (FDIC) insurance coverage is passed through to the beneficial owners of the cash balances. The movement of cash to settle trades on behalf of clients may result in balances in excess of FDIC coverage, exposing the bank or its clients to credit risk in the event of the sub-custodian's failure. Banks should refer to current FDIC insurance regulations for further guidance in assessing exposure to uninsured balances. Banks should monitor sub-custodian credit risk as part of their overall risk assessment program and should consider settlement arrangements that minimize this exposure. In the event of fraudulent or otherwise wrongful activity that results in the loss or misappropriation of assets by a sub-custodian, and the sub-custodian's subsequent failure, the bank may be dependent on the sub-custodian's private insurance coverage. As a result, an assessment of the adequacy of the sub-custodian's internal control environment, and its fidelity bond, errors and omissions policy, or other applicable coverage should be part of the ongoing due diligence process.

Credit Risk/Broker-Dealers as Sub-Custodians

Custody of assets may be maintained with an SEC-registered broker-dealer as a sub-custodian, provided the practice is consistent with applicable law and the bank maintains adequate safeguards and controls over the assets. If a bank elects to use a registered broker-dealer firm for custody of fiduciary assets, and if neither the provisions of the governing instrument nor relevant state statutes specifically authorize the practice, the bank should obtain an opinion of counsel to determine whether the practice is consistent with applicable law.

Prior to placing fiduciary or other client assets in the custody of a broker-dealer firm, the bank should complete a thorough risk assessment that considers credit and operational risks. This arrangement should be subject to a written agreement that

- provides that the broker-dealer firm accepts or releases funds or securities only upon receipt of instructions from authorized bank officers or employees provided in accordance with agreed-upon procedures.
- prohibits the broker-dealer firm from using the securities in a securities lending program without written permission from authorized bank officers or employees.
- does not restrict the bank to any specific broker for trading, so the bank can obtain best execution for its clients.

The agreement, including the specific manner in which the account is titled, should be reviewed by counsel with securities expertise. When entering into an arrangement with a broker-dealer as the sub-custodian for fiduciary or custody assets, a bank should review and consider current Security Investor Protection Corporation (SIPC) rules and coverage.

The bank's procedures should require adequate oversight of all asset movement by the broker-dealer firm as sub-custodian and the reconcilement, at least monthly, of all cash and securities held at the broker-dealer to the bank's records.

Other Asset Custody

Certain assets—such as open-end mutual funds, limited partnerships, bank certificates of deposit, or securities owned through the Direct Registration System (DRS) administered by DTCC—are customarily held in book-entry form. These assets are generally more effectively handled if they remain in the bank's direct control—that is, the books and records of the issuer or its transfer agent reflect the bank, in its capacity as fiduciary or agent, or the bank's nominee, as the owner of record. In these situations, policies and procedures should be in place to ensure that joint custody or control is maintained, along with the capability for timely execution of purchases and redemptions, timely receipt and reconciliation of statements or confirmations, and timely receipt of income. For open-end mutual funds, the NSCC, a subsidiary of DTCC, provides an array of services that include information exchanges between asset managers and the funds' transfer agents that facilitate order processing and settlement, income processing and position reconciliation.

Other assets, such as mineral interests, real estate, furniture, and furnishings, cannot realistically be placed in a vault. A bank should maintain all available evidence of title or possession of these assets in a reasonable manner and should take measures to ensure that they are properly insured and physically protected.

For additional information about safeguarding assets, refer to the "Custody Services" booklet of the *Comptroller's Handbook*.

Securities Servicing

Securities servicing encompasses asset setup, ongoing asset pricing, income processing, corporate action processing, class action processing, and shareholder servicing. Securities servicing relies on the use of appropriate internal and external information, including automated data sources, to accurately reflect detailed asset-level information and asset-related events on the Asset Management accounting system.

Asset Setup

For Asset Management operations to properly report, monitor, and service assets held in fiduciary and related accounts, each security should be established in the Asset Management accounting system's asset records. For publicly traded securities, a common asset record is established, while for certain unique asset types, detailed asset records are typically established at the account level. Some of these unique assets, such as income producing real estate, or natural resource interests, are also set up on specialized systems designed to support their specific processing and reporting requirements.

Complete and accurate asset coding is essential to ensure the accuracy of internal, client, and other external reporting. Asset coding is integral to many of the automated processes performed by Asset Management accounting systems, such as income processing, maturity processing, and tax reporting. When applicable, the asset should be identified by its industry-recognized ticker symbol or Committee on Uniform Securities Identification Procedures (CUSIP) number so that it can be automatically updated with external information, such as prices, dividend announcements, and corporate action notifications. CUSIP numbers and ticker symbols also facilitate automated processes that involve external parties, such as trade settlements, depository reconciliations, and proxy processing. A bank typically uses information provided by independent information sources to assist in asset setup for publicly traded securities. Many Asset Management accounting systems enable banks to set up model assets, which pre-fill many asset-level codes based on asset type, further reducing the risk of input error. Banks should have procedures to ensure the completeness and accuracy of asset coding.

Asset Pricing

Among the codes typically assigned to each asset when it is set up on an Asset Management accounting system are codes that determine the source and frequency of pricing. Accurate asset pricing is critical for a number of reasons. Asset prices determine the position and market values reported on client statements and on online client reporting systems. These market values may be relied on by portfolio managers when making investment decisions; may affect regulatory reports, such as Schedule RC-T "Fiduciary and Related Services" of the Consolidated Reports of Condition and Income; and may affect the amount of the bank's fee. Depending upon the type of account, the market value, as reflected on the Asset Management accounting system may be reportable in certain IRS filings; may determine the amount of distributions made to beneficiaries; and may be used by clients to prepare financial reports, including audited financial statements subject to generally accepted accounting principles (GAAP).

Asset Management operations, in coordination with investment management, should have written asset pricing policies and procedures, which reflect specific sources, methods, and frequency of pricing, depending upon the nature of the asset, and the availability and cost of reliable pricing. For example, publicly traded securities can usually be priced daily, based on actual market activity, from automated data feeds provided by pricing services. Prices for more complex or less frequently traded assets are available from third parties such as pricing services and brokers, but their values may be based on theoretical models. Other assets, such as real estate or closely held businesses, are not readily priced, and valuations are often based on appraisals, models, audited financial statements, or committee estimates. Such valuations should be performed at reasonable intervals and whenever a material event occurs. For further guidance on asset valuation, refer to the "Investment Management Services" booklet in the *Comptroller's Handbook*.

Regardless of the asset type, bank policies and procedures should address valuation sources, methods, and frequency and should ensure that valuations are accurate and independently verifiable. They should address how pricing methodologies and frequencies are disclosed to clients on periodic statements and through other communication channels, such as Internet account access. These policies and procedures should address valuation practices in periods of market dislocation, including how significant discrepancies among pricing sources are addressed and escalated. As asset types increase in complexity, accurate prices often become more difficult to determine or expensive to obtain. Establishment of a valuation committee can be an effective way to oversee the bank's pricing and asset valuation policies and procedures, especially for banks that are responsible for pricing illiquid or hard to value assets.

Asset Management operations should implement processes to ensure that the specific codes that determine each asset's pricing source and frequency are accurate and consistent with the bank's pricing policy for various asset types. Asset Management operations should produce and review appropriate MIS reports to identify missing or stale prices, pricing sources or frequencies that do not conform to policy, and price fluctuations outside of established thresholds, which might be indicative of pricing errors. A bank should have procedures for resolving pricing exceptions and for authorizing overrides or adjustments to automated prices.

Income Processing

Asset Management operations is responsible for collecting and posting dividends, interest, and any other income payments or distributions from assets held in Asset Management accounts. Depending on the asset type, anticipated income may be readily determined based on either an agreed-upon payment schedule (e.g., bond interest) or routine publicly announced payments (e.g., stock dividends). Payments received on an irregular basis, such as mineral interest royalties or farm income, may be more challenging and labor-intensive to track and collect. Processes for monitoring and posting income range from highly automated to manual, based on the asset type and the capabilities of the Asset Management accounting system or subsystems.

Asset Management operations should have procedures to identify the amount and date that income is payable, post it to the appropriate accounts in a timely manner, and take appropriate action when anticipated payments are not received.

Income processing for publicly traded stocks and bonds is highly automated. Most Asset Management accounting systems interface with third-party servicers that provide automated income announcements and updates for publicly traded stocks and bonds based on CUSIP numbers. This data, in conjunction with income codes defined at asset setup, is used to generate reports of anticipated dividend and interest payments.

These multiple account processing (MAP) reports should identify which individual accounts are entitled to payment, the amount of the dividend or interest payment due each account, and the source from which payment is expected based on the asset's safekeeping location and/or registration code. Comparison of these reports to anticipated reports provided by custodians or depositories enables Asset Management operations to research and resolve discrepancies prior to posting. When Asset Management operations "releases" these MAPs, the appropriate client accounts are automatically credited and a designated suspense account is debited. By crediting the dividend or interest payment to the suspense account upon receipt, the suspense account item is cleared.

Exceptions occur when the anticipated income is not received on time or the amount received does not match the amount anticipated. Exceptions should be monitored, researched, and resolved in a timely manner, with escalation procedures based on the amount and age of exceptions.

Asset Management operations should identify the income characteristics of each asset type for which it is responsible, and, to the extent practical, use the capabilities of the Asset Management accounting system to automatically track and post income. When this is not practical, appropriate tickler systems or manual processes should be implemented.

Certain fiduciary accounts require segregation of income and principal. Banks must comply with the terms of the governing document and the Uniform Principal and Income Act (UPIA), or other applicable state law, when applying receipts to such accounts. For example, most states have specific requirements for the allocation between principal and income for such transactions as capital gain distributions, special stock dividends, and income from depleting assets (such as mineral interests). Procedures for assigning asset codes, account codes, and transaction codes or for manually determining whether a transaction is posted to income or to principal should reflect the requirements of the UPIA or other applicable state law.

For foreign securities, a portion of the income is often withheld for taxes payable to the issuing country. Various treaties may reduce or eliminate withholding requirements or may reduce the tax rates for certain types of securities or accounts. Banks should have procedures to ensure that they obtain the necessary documents from clients for whom they service foreign securities in order to establish the account's eligibility for reduced withholding or taxation. Asset Management operations should ensure that the necessary documents and information are provided to the appropriate sub-custodian. Foreign tax withholding should be monitored, and when applicable, tax reclamation forms should be submitted and tracked. This process, typically handled by the local market sub-custodian or global custodian, can be detailed and time-consuming and is addressed in greater detail in the "Custody Services" booklet of the *Comptroller's Handbook*.

Corporate Action Processing

A corporate action is an event initiated by a company that affects securities (equity or debt) issued by that company. Examples of corporate actions include

- name changes.
- exchange of securities.
- mergers and acquisitions.
- tender offers.
- offering of subscription rights, warrants, stock options, or stock dividends.
- stock splits.
- spin-offs and liquidations.
- full or partial bond calls.

Corporate actions are either mandatory or voluntary.

- **Mandatory corporate actions,** such as bond calls, mergers, name changes, stock splits, stock dividends, and reverse splits are events that occur based on the action of the issuer and do not require approval from the portfolio manager or the client. Asset Management operations should ensure that mandatory actions are promptly identified and posted to the Asset

Management accounting system on the designated payable or effective date so that asset positions and market values are accurate and that any resulting cash distributions are promptly invested. Policies and procedures should address the fair allocation of partial calls of bonds held by multiple accounts. When securities are held off-premises, operations needs to verify that the records of the depository or sub-custodian are updated promptly to reflect the mandatory event. Mandatory corporate actions may require the physical delivery of the securities to the transfer agent. Asset Management operations needs to ensure that, as applicable, securities are delivered to the transfer agent and replacement securities are received in a timely manner.

Failure to process a mandatory corporate action in a timely manner can lead to claims for compensation due to delays in reinvesting cash proceeds resulting from the event. Significantly inaccurate market values can result when stock splits or name changes are not processed in a timely manner. While a bank may receive corporate action information from depositories or custodians, these notices should not be relied on as the only source of timely information. To minimize the risk of a missed event, and to ensure that the depository or custodian is properly handling these transactions, many banks avail themselves of other corporate action notification services. As part of its risk oversight program, management should ensure that operations has adequate procedures and has access to accurate and timely mandatory corporate action information.

- **Voluntary corporate actions,** such as tender offers or rights offerings require a response to the issuer's agent by a specific deadline. As with mandatory actions, obtaining timely notification is essential. In the case of voluntary actions, however, procedures also are needed to promptly forward the notification to the party with voting authority for each account (e.g., the investment committee, the investment manager, or the client) and to ensure that a decision is made and that the result is communicated to the issuer's agent by the specified deadline. A bank's failure to notify the party (or parties) with voting authority and to process responses to voluntary corporate actions by the required deadlines can have substantial adverse financial consequences for the customer, resulting in claims against the bank.

The processes for voluntary corporate actions include

- ensuring that notifications/announcements are received.
- comparing notifications/announcements to asset holdings.
- notifying appropriate persons of voluntary corporate actions.
- receiving instructions from authorized persons.
- balancing responses received to units held.
- executing the instructions.

Best practices in these high-risk processes include

- establishing cut-off times and follow-up steps that give employees time to act on the corporate action.
- when possible, obtaining written responses to requests for direction on a voluntary corporate action.
- if relying on a telephone response, using a recorded line with authentication controls.
- requiring that someone independent of the person who compiled and prepared the corporate action responses review the compilation for accuracy before submitting the responses to the issuer, third-party custodian or depository.

Once an action is submitted that commits an account to tender shares, there is a risk these securities might be erroneously sold before they are actually tendered, creating risk for financial loss. To limit this exposure, these shares should be appropriately "flagged" or "frozen" on the system used by portfolio managers and traders. For events such as mergers, exchanges, and tender offers, the resulting transactions can be complex combinations of asset and cash distributions, which require expertise to ensure proper posting. When processing these transactions, in addition to ensuring that the correct amounts of shares and cash are credited to each account, Asset Management operations should ensure that these transactions appropriately affect the cost basis, tax and investment performance measurement reports, and are consistent with the requirements of the state's UPIA.

Because improperly handled mandatory and voluntary corporate actions have been a significant source of losses for Asset Management operations, banks and vendors have developed a number of automated corporate action notification and processing capabilities to assist in identifying corporate actions, notifying appropriate parties, tracking responses for voluntary actions, and posting resulting transactions to the core Asset Management accounting system.

Management should ensure the use of appropriate procedures, internal controls, and automation capabilities that adequately control the risks associated with corporate action processing. These risks are heightened for corporate actions of foreign issuers. For more information regarding domestic and foreign corporate action processing, refer to the "Custody Services" booklet of the *Comptroller's Handbook*.

Class Action and Fair Fund Settlement Processing

A class action is a form of lawsuit that may be initiated when a large number of people allege they have been injured by a common act or set of actions. A common example would be a lawsuit filed by a group of investors in a particular stock who allege that they have incurred investment losses as a result of fraudulent earnings reports from the issuing company.

Once a court certifies a class action, meaning that the suit has met certain legal standards, members of the class must be given notice and the opportunity to join or to be excluded from the proceeding. Although class members who exclude themselves from the proceedings do not share in the resulting settlement, they are also not bound by the judgment in the case and may pursue independent action.

Because class actions are often subject to a lengthy litigation process, it can take years from inception to final resolution. Once there is a proposed settlement, the court typically directs that a settlement notice be sent to participating class members. Class members must file a settlement claim to share in the resulting proceeds. While many class action settlements are quite large, the legal expenses and the number of members in the class may result in very small payouts to individual class members.

If an Asset Management account owned shares during the time period defined in the class action notice, it may be eligible to join a certified class action and to share in a resulting settlement. Both the class action notice and the governing instrument should be reviewed carefully to determine whether the bank is eligible and/or obligated to file on behalf of an account, including an account that has closed. When the bank is not eligible or obligated to file, the bank may still be obligated to forward the notice to the client, successor fiduciary, or other authorized party. While the research to determine which accounts may be eligible to participate in class action litigation is often manual and laborious, automated services are increasingly available for all or part of this process.

Whether and how a bank responds to a class action notice may have significant financial consequences to its clients, and therefore represent litigation and reputation risk to the bank. Class members who do not exclude themselves from the class by a specified date lose their right to pursue independent action. Class members who do not file a settlement claim by a specified date lose their rights to share in the class settlement. Banks should implement procedures and controls to ensure that class action notifications are identified, received, analyzed, acted upon, and monitored in accordance with applicable fiduciary and contractual obligations. These procedures should include

- a process for determining which current and former accounts are eligible to participate.
- a process to determine whether participation in any particular action is appropriate for discretionary accounts.
- a process for determining the bank's eligibility and obligation to file on behalf of each account, or its obligation to notify a successor fiduciary, client, or authorized party.
- a process for monitoring key response deadlines for class action notices.
- a process for monitoring pending class action settlements to ensure that funds due as a result of class action judgments are collected and credited to participating accounts or clients.
- criteria for determining whether the bank may be compensated for processing class action notifications, and for determining the amount of such compensation.
- criteria and process for determining when the prospective proceeds from a particular class action suit is de minimis in relation to prospective payments and need not be pursued.

Section 308 of the Sarbanes-Oxley Act, the Federal Account for Investor Restitution provision (commonly referred to as the Fair Funds provision), allows the SEC to combine civil monetary penalties and other donations to disgorgement funds for the benefit of investors who suffer losses resulting from fraud or other securities violations. Such funds are eventually distributed to investors through the SEC's Office of Collections and Distributions. Banks should have procedures in place to ensure that Fair Fund remittances from the SEC or other regulatory settlements are promptly researched for allocation and payment to affected accounts.

Shareholder Communications and Proxy Processing

The Shareholder Communications Act of 1985 and SEC regulations address proxy processing requirements for banks and other financial intermediaries. These rules are designed to ensure that beneficial owners (those authorized to vote on behalf of an account) of securities are provided proxy materials and other corporate communications promptly. SEC Rule 17 CFR 240.14b-2, "Obligation of banks, associations and other entities that exercise fiduciary powers in connection with the prompt forwarding of certain communications to beneficial owners" and 17 CFR 240.14c-7, "Providing copies of material for certain beneficial owners" govern the distribution of proxy materials and the disclosure of information about shareholders whose securities are registered in a bank nominee name.

Most Asset Management accounting systems provide interface capabilities with proxy service providers, which automate the distribution of proxy materials to beneficial owners and enable banks to automatically respond to issuers who request the names and addresses of the beneficial owners of their securities who do not object to such disclosure. To comply with these requirements, appropriate options need to be activated on the Asset Management accounting system, and account and beneficiary records must be properly coded to identify each account's beneficial owner(s) and reflect each beneficial owner's objection or non-objection to disclosure of their identity to issuers.

When a bank has the authority to vote proxies, account and beneficiary records should be coded so that proxies and related materials are routed to the appropriate area within Asset Management. Authorized individuals should vote these proxies in accordance with well defined bank policies and applicable law. Such policies should provide general guidance for voting proxies on behalf of fiduciary accounts, and establish a process for voting non-routine proxies. Typically, either the investment committee or a specially designated proxy committee is responsible for determining how to vote on non-routine proxies. Refer to the "Retirement Services" booklet of the Comptroller's Handbook and to Department of Labor Interpretive Bulletin 2509.94-2, "Written Statements of Investment Policy, Including Proxy Voting Policy" for specific guidance applicable to ERISA accounts.

When a national bank holds own-bank stock as sole trustee, the bank is prohibited under 12 USC 61 from voting these shares in the election of directors. Co-trustees, and, to the extent to which it is specified in the governing instrument, the account's grantor or beneficiaries may be empowered to vote these shares. Most asset management accounting systems enable banks to establish one or more specific beneficial owners at the specific asset level, enabling banks that would otherwise have proxy voting authority to automate the distribution of own-bank stock proxy materials to appropriate parties. For further guidance, refer to the "Conflicts of Interest" booklet in the *Comptroller's Handbook*.

Securities Transaction Processing

Securities transaction processing encompasses the settlement of purchases and sales as well as "free" receipts and deliveries of securities. Asset Management operations is responsible for ensuring that there is an effective SMAC system in place and that transactions are completed in a secure and timely manner and in accordance with industry standards.

Securities Movement and Control (SMAC)

SMAC systems and procedures originally were developed to control physical securities. SMAC systems were designed to ensure that these securities could be properly monitored and safeguarded as trades were settled, transfers completed, corporate actions processed, and free receipts and deliveries completed. Effective SMAC capabilities remain an important requirement for Asset Management operations, although it is now primarily an automated process used to monitor and control both physical and book-entry securities.

Securities Industry Automation and Standardization

The sheer volume of securities trading and settlement activities and related costs and risks have led the industry to undertake a number of initiatives achieve cost efficiencies and mitigate risk. These include book-entry securities, net settlement of trades, shortened settlement times, central counter-parties, and increased automation of post-trade pre-settlement processes. Key participants in the securities processing infrastructure include securities exchanges (trade execution), DTCC (post-trade communication and confirmation, clearance and settlement, custody, and asset servicing) and large financial institutions acting as intermediaries for institutional clients and other financial institutions. The industry continues to evolve due to the influence of globalization, innovative security issuances, industry and regulatory focus on both firm-wide and systemic risk management, and ongoing developments in technology.

Whether as a direct participant in these infrastructure initiatives or an indirect participant through depositories, third-party custodians, or other service providers, banks need to ensure that Asset Management operations keeps abreast of current industry standards for securities processing. Based on the nature and scope of the bank's Asset Management activities, management needs to ensure that resources are available and processes are in place to provide appropriate securities safekeeping, servicing, and settlement capabilities and controls.

Purchases and Sales

It is the role of the front office (investment managers, relationship managers, and administrators) to ensure that all purchases and sales are properly authorized, and, when the bank's role is to initiate trades, to provide instructions to the designated trading area. For purchases and sales of depository eligible securities, the role of Asset Management operations begins post-trade. Operations functions include ensuring that the trade is settled at the designated location (depository or sub-custodian), that the appropriate exchange of funds occurs, and that the transaction is posted to the Asset Management accounting system. For depository-eligible securities, these processes are typically highly automated. Reports of "failed trades" (trades that have not settled as scheduled) should be reviewed at least daily, and processes should be in place for prompt escalation of exceptions.

Asset Management operations needs to comply with the minimum record keeping, record retention, and confirmation requirements of OCC Regulation 12 CFR 12 for securities transactions effected by national banks for customers. These requirements are addressed in the Record Keeping and Reporting section of this booklet.

In the case of assets not traded through exchanges, such as certificates of deposits, limited partnerships, or open-end mutual funds, management may designate Asset Management operations to effect the transaction with the issuer. In those cases, controls and procedures for these asset types should ensure that transactions are effected in a timely manner and that the bank maintains adequate safeguards and controls, including the proper segregation of duties.

Management needs to periodically review Asset Management operations processes for securities settlement, making informed decisions as to whether trades are posted to client accounts on an actual or contractual basis. They should consider the practices and obligations of sub-custodians, depositories and counterparties, as well as agreed upon arrangements for the transfer of funds. Any resulting credit exposure from the bank's settlement practices needs to be effectively monitored and managed.

Depository Interfaces

Many Asset Management accounting systems interface with depository and sub-custodian systems and with post-trade processing systems. These interfaces can provide Asset Management operations with opportunities to combine tasks, such as entering a purchase or sale transaction on the Asset Management accounting system and providing instructions to the depository or custodian to settle the trade. When used with an automated trade order entry system, these interfaces support the automation of trade matching, affirmation, and posting. Most depository and custodian interfaces can also provide electronic data feeds for interest and dividend payments and asset position files, which facilitate automated income processing and position reconciliation. While these and similar capabilities can dramatically streamline processing and minimize manual data entry errors, they should be used in conjunction with appropriate workflows, system access controls, reconciliations, and verification procedures to ensure that the principles of joint custody and segregation of duties are maintained.

Disbursement of Assets—Free Deliveries

"Free delivery" occurs when assets are removed from an account without the receipt of cash. A free delivery might occur under the following circumstances: account closing (including transfers to successor fiduciaries); gifts from the account; customer requests for the return of assets; the transfer of the asset to a party specified in a trust agreement; or the transfer of assets from one account to another. Free-delivery transactions require particular vigilance and proper safeguards to ensure that an unauthorized asset delivery does not occur, as the potential loss could be substantial. Free deliveries should be subject to joint custody or control requirements. No person should be able to release securities from a depository without an independent check on the validity of the transaction.

The front office is responsible for initiating free deliveries and ensuring that all free deliveries are authorized by the proper parties in accordance with the governing document and bank policy. The authorization of two designated front office employees (typically including either the relationship manager or administrative officer) should be provided to Asset Management operations along with detailed instructions for the delivery of the asset(s).

The actual movement of securities is effected by Asset Management operations. Banks need to assess the extent to which the system(s) they are using can be configured to require two authorizations for the free movement of securities and to ensure the effective use of either these capabilities or manual controls. In designing these processes, banks should segregate the capability to change asset location codes on the Asset Management accounting system from the capability to effect or post free deliveries, as improper location codes changes could potentially conceal improper free deliveries. When free deliveries are made by mailing physical securities, adequate controls and insurance coverage should be provided.

When applicable, banks need to provide transfer statements that meet the requirements of IRS regulation 26 CFR 1.6045A-1, "Statements of information required in connection with transfers of securities." These requirements include providing adjusted cost basis information for "covered securities" as defined in the regulation.

Automated Customer Account Transfer Service

Automated Customer Account Transfer Service (ACATS) is provided by the NSCC and automates, expedites, and standardizes procedures for the transfer of many types of securities (including mutual funds) in a customer account from one brokerage firm and/or bank to another. Participation by broker-dealers is mandatory and is subject to rules of the Financial Industry Regulatory Authority (FINRA) and the NSCC. These rules include indemnification of the transferor if a requested transfer is later determined to be unauthorized. As a result, for ACATS transfers between FINRA regulated firms, the requesting firm does not typically provide authorization documents.[3]

[3] In a broker to broker transfer, the authorizing documents are typically retained by the broker requesting the transfer.

A bank with the appropriate type of DTCC membership is permitted by the NSCC to participate in ACATS. While participating banks agree to abide by NSCC rules, they are not subject to FINRA rules. As a result, many banks that have chosen to participate in ACATS continue to require documentation to confirm that the requested transfer is properly authorized, particularly in the case of fiduciary accounts. A bank's decision to participate in ACATS, and its policies and procedures determining whether the bank continues to require authorizing documentation prior to transferring securities, should be based on a thorough risk assessment, which includes an analysis of applicable NSCC membership documents and applicable rules, including timeframes. In addition, a bank may only use ACATS for the transfer of fiduciary assets if bank counsel opines that the use of ACATS complies with the bank's fiduciary responsibilities as determined by applicable law.

Receipt of Assets—Free Receipts

A "free receipt," also referred to as a "receipt in-kind," occurs when assets are received and no payment is exchanged in return. A free receipt may occur when assets are received from the client or their agent to fund a new account; the client or agent adds assets to an existing account; or the account is the recipient of a gift or in-kind distribution. Free receipts may be accomplished by either the physical delivery of securities to the bank or a book-entry transfer.

Policies and procedures should be adopted that require that physical securities are under joint custody or control from the time they are received from the client or agent until they are re-registered and either filed for safekeeping in the on-premises joint custody vault or delivered to an appropriate safekeeping location. For tangible assets (such as jewelry or coins), and other assets (such as partnership interests or real estate), sound policies should describe when and how such assets are controlled from the time they are received from clients or their agents. When a bank receives physical securities, it may be required to make inquiries as to whether the securities have been reported lost or stolen, per SEC Rule 17f-1, described later in this section.

Book-entry assets may either be securities transferred from the depository or sub-custodian account of another financial institution or may be assets registered directly on the books of the issuer or its transfer agent, such as open-end mutual funds, dividend reinvestment accounts, and some certificates of deposit. In anticipation of the free receipt of book-entry assets, the front office typically provides Asset Management operations with an inventory of the expected assets, providing such details as cost basis, and the authorization documents needed to transfer the assets. Until the anticipated transfer of these assets to the bank's depository or sub-custodian account or to a properly re-registered book-entry account under the control of Asset Management operations is complete, these pending transfers should be monitored. Procedures should be in place for timely follow-up and escalation of any delays or discrepancies.

Lost and Stolen Securities

SEC Rule 17 CFR 240.17f-1, "Requirements for reporting and inquiry with respect to missing, lost, counterfeit or stolen securities," requires banks, brokers, and other institutions that deal with or process securities to report lost, stolen, or counterfeit securities to a central information facility, the Securities Information Center (SIC). As a result, banks that handle securities must register, either directly or indirectly through another institution, with the SIC. A bank must also inquire with the SIC regarding any physical security that comes into its possession and is part of a transaction of $10,000 or more to determine whether the security has been reported lost or stolen, subject to a number of exceptions (such as securities received from another reporting institution). Asset Management operations needs to be familiar with the requirements of and exceptions to Rule 17 CFR 240.17f-1 and must report lost or stolen securities and make inquiries regarding incoming securities in compliance with this rule.

Securities Transfers and the Securities Transfer Agent Medallion Program (STAMP)

To complete the re-registration of physical securities or book-entry assets, such as dividend reinvestment accounts, a bank needs to provide a stock or bond power, signed by an authorized party (client or authorized agent), to the transfer agent. In accordance with SEC Regulation 17 CFR 240.17Ad-15, "Signature Guarantees" transfer agents must immediately accept signatures that have been guaranteed by an industry-recognized Medallion Signature Guarantee Program and may reject requests that do not contain such a guarantee. The use of a Medallion guarantees the authenticity of the signature and the legal authority of the signer and guarantees that the signer had legal capacity. As a result, the use of a Medallion guarantee expedites securities transfers requested in the course of administering Asset Management accounts. The use of a Medallion, however, presents risks to the bank as guarantor. Prior to enrollment in a STAMP, management should assess its business needs along with the risks and contractual responsibilities associated with the use of the Medallion and establish appropriate policies and procedures.

Foreign Securities Transactions

While the global investment needs of many clients can be met with American Depository Receipts (ADR) or international mutual funds, large customers, particularly institutional investors, may wish to invest directly in foreign securities. Investment in foreign securities provides additional challenges for trade settlement, securities servicing (especially corporate action processing), and may require additional Asset Management accounting system capabilities to handle multiple currencies. In addition, a portion of the income from foreign securities may need to be withheld for taxes payable to the issuing country.

Before accepting an account that holds or is expected to hold foreign securities, management should ensure that it has the necessary expertise, access to global custody services, Asset Management accounting system capabilities, and internal policies and procedures needed to properly service and manage the risks associated with processing these securities. These risks include country risk—the risk that economic, social, and political conditions and events in a foreign country will affect an institution—which is addressed in the "Country Risk" booklet of the *Comptroller's Handbook*. The "Custody Services" booklet of the *Comptroller's Handbook* provides additional information on global custody and related securities processing activities.

Cash Transaction Processing

Cash transaction processing, which includes cash disbursements, cash receipts, and fee processing, is a core function of Asset Management operations. Asset Management operations is responsible for ensuring that cash transactions are processed in an accurate and timely manner, and are subject to appropriate internal controls.

Disbursement Authorization and Processing

A major function of Asset Management operations is to process disbursements from accounts. Policies, procedures, and workflows for disbursement processing should ensure that

- these payments are subject to joint custody or control;
- there is proper segregation of duties between the front office, which authorizes disbursements, and operations, which processes disbursements;
- there is appropriate delineation of authority for approval of disbursements; and
- the bank complies with BSA/AML record-keeping and reporting requirements.

Disbursements to, or on behalf of, Asset Management clients or beneficiaries include

- periodic income payments.
- routine bill payments.
- retirement plan benefit payments.
- discretionary distributions.
- directed disbursements.
- tax payments.
- charitable bequests.

Essential to an Asset Management division's internal controls are policies and procedures that ensure that all disbursements—both those for which the bank has discretion and those that are directed by clients—are properly authorized and documented. The types of authorization required may be based on the size and nature of the disbursement, whether it is a one-time or recurring event and the capacity in which the bank is acting. The front office should ensure that disbursements are authorized in accordance with policies and procedures, as well as with the terms of the governing document, and that sufficient funds are available in the client's account. Authorizations should include payment disposition instructions (e.g., mailing address, wire transfer instructions, etc.).

Approved disbursement requests should be communicated to Asset Management operations through signed documents or properly authenticated electronic transmissions and should be based on proper front office approval as set forth in the bank's policies and procedures. Payee information should be sufficiently detailed so that funds are credited to the proper party and that disbursement transactions can be effectively screened for OFAC-prohibited transactions. For guidance on OFAC transaction screening, see the BSA/AML section of this booklet. If the Asset Management accounting system utilizes client name and address records to create payment transactions, appropriate controls over the creation and maintenance of these records should be implemented to ensure that payee information is sufficiently detailed and changes are properly authorized to minimize the risk that fraudulent payees could be established.

Upon receipt of an authorized request, Asset Management operations typically posts the transaction to the Asset Management accounting system. Depending upon the bank's workflows and systems, this might occur in a variety of ways, such as releasing electronic transactions prepared by administration, entering cash transactions on the Asset Management accounting system based on paper input forms, scheduling disbursements on the Asset Management accounting system via tickler, or releasing previously scheduled disbursement ticklers.

Disbursements—Money Movement

Asset Management operations is responsible for effecting the actual movement of funds as directed on the approved disbursement request. Payment methods include check, internal transfer, wire transfer, and Automatic Clearing House (ACH) transactions. Because banks are prohibited by OFAC from disbursing funds to certain countries, organizations, and individuals, they should have procedures to ensure that the payee or payment destinations are not on the prohibited list. See the BSA/AML OFAC screening section later in this booklet for further guidance.

Checks

Checks issued on behalf of Asset Management accounts are typically drawn on an internal or external account in the name of the bank, signed by one or more designated bank officers, and are therefore considered to be “treasury” or “official checks,” representing an obligation of the bank. Asset Management operations, or a designated area independent of administration personnel, should control the storage, preparation, and issuance of Asset Management checks. Policies and procedures should ensure that checks are stored and prepared in a joint custody or control environment and that appropriate records are maintained for checks on hand, checks issued, and checks voided or destroyed.

Policies and procedures should grant appropriate levels of check-signing authority to designated individuals. These individuals should be independent from those authorizing disbursements, posting transactions, or preparing checks, and this authority should be promptly revoked when appropriate. A facsimile signing device may be used for Asset Management checks provided that there are adequate policies and procedures to authorize and control its use. These include imprinting a maximum valid dollar amount for facsimile signatures on the signature plates and adequately storing the plates. Checks, along with any accompanying remittance documentation, should be mailed to the designated payee by Asset Management operations. Appropriate controls should exist for checks that are returned undeliverable.

At the time a check is issued, funds are typically transferred from the demand deposit account or GL account for uninvested Asset Management cash to a separate demand deposit account or GL account designated for checks issued but not yet presented for payment. For guidance on the reconciliation of this account, refer to the reconciliation section under Internal Accounting Controls in this booklet. Policies and procedures should address requests for stop payments on these checks, which, because they are considered “official checks,” are subject to special rules in accordance with applicable state law.

Wire Transfers

Asset Management operations is often directed to execute disbursements via wire transfer. Controls over wire transfers are especially important since the finality of payment and frequent use of wire transfers for large dollar transactions result in heightened risk of loss due to error and internal or external fraud. Wire transfers are customarily sent via written, electronic, or telephone request from Asset Management operations to an internal or correspondent bank wire transfer area from which the wire is actually sent.

Policies and procedures should designate individuals authorized to direct the wire transfer area to execute wires from Asset Management accounts. Typically, individual authority is subject to dollar limits, and designated amounts may require the authorization of two individuals. Appropriate call-back or other verification procedures should be used to validate instructions communicated via telephone or facsimile transmission.

Wire transfers are subject to record-keeping requirements and other rules to comply with BSA/AML and OFAC requirements. For further guidance, refer to the BSA/AML section later in this booklet and the FFIEC's *Bank Secrecy Act/Anti-Money Laundering Examination Manual*.

ACH

ACH is a nationwide electronic funds transfer network that enables participating financial institutions to originate electronic credit and debit entries to accounts at other institutions. Many Asset Management accounting systems have the capability to produce ACH credit origination files to disburse funds from Asset Management accounts to external bank accounts. These disbursements should be subject to Asset Management's normal disbursement authorization process. Procedures should be in place to ensure that there is proper control over the release and transmission of these transaction files over the ACH network and that the reconciliation of internal ACH clearing accounts is independently performed. Banks using ACH origination systems that permit manual entry of transactions should have controls to ensure that all such entries are properly authorized. For further guidance, refer to OCC Bulletin 2006-39, "Automated Clearing House Activities" and the "Retail Payments Systems" booklet of the *FFIEC Information Technology Examination Handbook*.

Internal Transfers

Properly authorized disbursements that transfer funds from one Asset Management account to another require entries to the Asset Management accounting system, but no actual movement of cash from the Asset Management demand deposit or GL account. Properly authorized transfers from an Asset Management account to an internal deposit account require entries to the Asset Management accounting system and a transfer of funds via check or other internal banking entry. The approval and processing functions for internal transfers should be properly segregated.

Cash Receipts

Cash receipts refer to incoming funds that are credited to an Asset Management account's cash balances. Funds may arrive in the form of check, wire transfer, or ACH credit. In addition to receipts related to securities servicing and securities transaction processing addressed in earlier sections of this booklet, cash receipts include initial and subsequent account funding from clients, retirement plan contributions, incoming transfers from other Asset Management accounts, tax refunds, and other cash flows that the client may direct to the account. When receipts can be anticipated, the use of receipt ticklers to track incoming payments is a useful control to ensure that payments are properly identified and posted and that missing amounts are appropriately researched.

Administrative input is often needed to ensure proper transaction descriptions, tax codes, and for accounts subject to UPIA or a similar state law, to ensure that the transaction is properly allocated between income and principal cash. As determined by the bank's policies and procedures, this input may be in the form of ticklers for recurring transactions, or paper or electronic input forms. Cash receipts are typically posted to the Asset Management accounting system by Asset Management operations, where the incoming payments are credited to the demand deposit or GL account for uninvested Asset Management cash. Policies and procedures should provide for appropriate controls over incoming payments to ensure that they are applied promptly and accurately to the appropriate account. Cash receipts are subject to the input controls and reconciliations discussed in greater detail below.

Note: Banks should have procedures for the rare occasions when currency is received for accounts, typically in the course of estate administration. These procedures should be designed to establish and maintain joint control and to ensure that cash is deposited to the Asset Management cash demand deposit account or GL account through a bank teller and therefore subject to the bank's currency transaction reporting policies and procedures.

Fee Processing

Asset Management clients typically compensate a bank for services provided through fees, which are either charged to the client's account or collected via invoice. Fees are based on published fee schedules as well as the express terms of the governing instrument. Fee schedules can be based on many factors, such as market value, income collected, and the volume of various types of activities. Most Asset Management accounting systems house multiple fee schedules, each of which generates various types of fees at assigned rates. Once approved by management, these detailed fee schedules are typically set up on the system by either Asset Management operations or the system administrator. The front office typically assigns fee schedules to specific accounts. Because these schedules can be very complex and are dependent upon other codes within the system, they should be tested at set up and periodically thereafter.

Fees are typically computed and posted periodically, usually monthly. When fees are charged directly to a client account, cash is moved automatically from the client account to a designated fee suspense account within the Asset Management accounting system. These funds are then transferred to the appropriate GL account. Because the IRS requires banks to recognize Asset Management income on an accrual basis, the GL account credited may be either a fee income or, as is typical for fees collected less frequently than monthly, a fee accrual account.

Many Asset Management accounting systems are able to generate fee invoices. Typically, at the time invoices are created, a fee receivable is set up and remains outstanding until the payment is received. In some cases, due to either system limitations or a fee schedule that is based on events external to the Asset Management accounting system, fees are computed manually. Examples might be fees based on activity maintained on a separate participant record-keeping system, estate administration fees, or hourly fees for special services.

Management should establish proper controls over fee processing. Policies and procedures should be designed to ensure that

- appropriate fee schedules are assigned to accounts.
- fees are computed accurately.
- fees are collected promptly.
- delinquencies are reported and escalated to management.

- fee suspense accounts, fee accrual accounts, and fee receivable accounts are reconciled periodically by individuals other than those responsible for authorizing or posting fee transactions.

MIS reports should identify accounts with missing or incorrect fee schedules; fee exceptions, such as discounts or negotiated fees; past-due fees; out-of-balance suspense or accrual accounts; fee-collection trends, and unusual fluctuations in fees at the account and department levels.

Title II of GLBA defines which bank securities activities are permitted to be conducted within a bank and do not require registration as a broker or dealer under the Securities Exchange Act of 1934. Title II provides a number of specific exceptions and 12 CFR 218, Regulation R, "Definition of Terms and Exemptions Relating to the 'Broker Exceptions' for Banks" provides related definitions and additional exemptions for securities activities that a bank may engage in without being subject to such registration. Beginning with the first fiscal year commencing after September 30, 2008, banks engaged in securities activities were required to demonstrate that they comply with the requirements of applicable GLBA Title II exceptions and related definitions and additional exemptions as set forth in Regulation R. One of the GLBA broker exceptions applies to a bank's trust and fiduciary activities. Among the requirements for this exception is the basis on which the bank must be "chiefly compensated." As a result, banks relying on the fiduciary exception of GLBA need to demonstrate that they are chiefly compensated for securities transactions effected for trust and fiduciary customers from "relationship compensation" that is attributable to trust or fiduciary accounts, as defined in GLBA and Regulation R.

Asset Management Accounting and Internal Accounting Controls

A core function of Asset Management operations is to maintain detailed and accurate records of customer accounts, subject to appropriate internal accounting controls. Such records would include account characteristics, account owner and beneficiary characteristics, cash balances, asset characteristics and asset positions, and records of cash, non-cash, and securities transactions. Such records should support day to day activity, client reporting, management reporting, and compliance with applicable regulatory requirements.

Asset Management Accounting and Record-Keeping Systems

Sound and reliable asset management accounting and record-keeping systems are essential to maintaining accurate and detailed account records, efficiently processing the high volume of time-sensitive transactions typically associated with Asset Management accounts, and providing necessary reports to the board, management, staff, clients, regulators, and auditors. The wide range of capabilities that these systems provide include

- securities transaction processing.
- disbursement processing and check production.
- cash receipt processing.
- ticklers (event reminders and posting templates).
- accounting controls.
- depository interfaces.

The wide range of reports that these systems provide include

- detailed account-level and position-level reports.
- client statements.
- internal activity and exception reports.
- regulatory compliance reports.
- audit trails.

Many of these systems include interfaces with, or file transfers to and from, other systems, such as

- depositories and custodians,
- asset pricing vendors,
- internal deposit, ACH and wire transfer systems,
- corporate action notification and processing systems,
- retirement plan participant record-keeping systems,
- IRS reporting and tax preparation systems,
- portfolio management systems,
- performance measurement systems,
- shareholder communication systems,
- systems supporting customer identification and information sharing requirements of the USA PATRIOT Act, and
- OFAC screening and suspicious activity monitoring systems.

Asset Management accounting platforms include proprietary systems developed in-house, vendor-provided software systems operated in-house, and vendor-provided software operated off-site by a third-party service provider. Regardless of where it is operated, the Asset Management accounting system is typically made available to Asset Management staff via the bank's internal computer network.

A bank should select its Asset Management accounting system after a careful assessment of the system's capabilities in light of the bank's current and anticipated Asset Management business requirements, the security and integrity of the system, the ability to appropriately integrate with other bank systems and conform to bank technical standards, the reputation and financial viability of the system provider, and the cost of the system. An ongoing assessment should be performed to identify deficiencies that arise either through changes in the bank's requirements, environment, or the emergence or discovery of previously unidentified weaknesses. Management should ensure that appropriate mitigating controls are implemented to overcome identified weaknesses. At times, management may engage qualified third parties to review systems and applications for weaknesses or rely on the work of qualified third parties engaged by others. Likewise, management may engage or otherwise rely on qualified third parties to assess the control environment of system service providers and should implement controls to mitigate identified weaknesses.

The availability of interfaces to other systems should be part of management's assessment of an Asset Management accounting system's capabilities, controls, and security vulnerabilities, especially when the movement of money, securities, or private information is involved. Appropriate manual or automated controls should be implemented to ensure data integrity, to properly safeguard customer information, and to ensure that the movement of money and assets is subject to joint custody or control.

Banks that are using or considering the use of automated systems to assist in the performance of annual investment reviews for fiduciary accounts should refer to OCC Bulletin 2008-10 "Annual Reviews of Fiduciary Accounts Pursuant to 12 CFR 9.6(c)" for guidance.

Internal Accounting Controls

Input Controls

Internal accounting controls are used to verify that entries posted to the Asset Management accounting system that affect cash balances or asset positions are balanced and controlled and that non-monetary input (input affecting an account or an asset's master file) is authorized and accurate. For systems that use batch processing, three common types of accounting controls are batch controls, blotter controls, and system balancing.

- **Batch controls.** A batch is a group of transactions assembled for posting for which cash and unit/share control totals are computed. At posting, these batch control totals are compared with system batch control totals, enabling operations to identify and correct data entry errors immediately. Batch controls are also used to ensure that the entries posted to the Asset Management accounting system correspond to the entries posted to the corresponding demand deposit account or GL account designated for uninvested Asset Management account cash.

- **Blotter controls.** A blotter or batch balancing report is a list of all batches entered and their corresponding totals for a specified time period. This enables operations to account for all input to the Asset Management accounting system each day, whether manually entered, system generated, or as the result of an interface from another system. Daily blotter totals are used to perform system balancing as described below.

- **System balancing.** Operations should balance the daily blotter totals (input) to resulting systems change totals and balances (output) as of end of day. Totals for income and principal cash should be balanced.

In addition to ensuring that monetary entries (those affecting cash and asset balances) are properly controlled, appropriate risk-based controls are needed for non-monetary input. Workflows vary in terms of whether such input is performed centrally or locally or performed in the front office, middle office, or back office. Management should implement risk-based procedures to ensure that, when warranted from a quality-assurance or an internal-control perspective, either an independent person performs a comparison of source documents to system changes or that compensating controls are in place. Examples of particularly sensitive non-monetary input types include asset location code changes and name and address changes. The ability to customize user profiles and the availability of verification reports, such as audit trails from most Asset Management accounting systems, are useful in establishing proper controls for non-monetary input.

Reconcilements

Timely and independent completion and review of reconcilements is an essential control for Asset Management operations. The three major types of reconcilements are cash, securities positions, and suspense accounts. Reconcilements are used to ensure that the Asset Management accounting system records correspond to external or independent records, such as third-party custodian statements or to the Asset Management department's customer cash account (demand deposit account or GL). This process can identify missing, incorrect, or unauthorized transactions that affect these external accounts, as well as posting errors or improper entries that affect cash and asset positions on the Asset Management accounting system. Proper identification, reporting, tracking, timely correction, and appropriate escalation of reconciliation exceptions is an essential tool in ensuring accurate records, identifying processing weaknesses, and detecting potential internal or external fraud.

Systems are available that automate the reconciliation process by matching transactions based on defined criteria. When effectively implemented, these systems can increase reconcilement efficiency and reduce the chance of manual error. Whether the reconcilement process is manual or automated, banks should establish workflows, procedures, and standards to ensure that

- reconcilements are performed in a timely manner at established intervals.
- reconcilements are performed independently from those who authorize or post transactions.
- reports are provided that adequately describe exceptions so that they can be tracked, investigated, and documented.
- exceptions are resolved, aged, and escalated appropriately.

Cash Reconcilement

Uninvested cash balances are reflected in detail in each client account (sub-ledger) on the Asset Management accounting system, as aggregate totals on the Asset Management accounting system, and in the aggregate in either an omnibus demand deposit account or GL account on the books of the bank or its correspondent. The reconciliation of cash totals, as reflected on the Asset

Management accounting system, to the actual demand deposit account or GL account balance is a key accounting control in Asset Management operations. This reconciliation should be performed daily and should be performed by an individual independent of the transaction approval or posting process. Exceptions should be identified by date, amount, and a specific description until cleared.

When funds are disbursed from an Asset Management account via check, the funds are deducted from the account's cash balance on the Asset Management accounting system and an Asset Management department check or internal entry is prepared. Typically, when checks are issued, funds are transferred from the demand deposit account or GL for uninvested Asset Management customer cash to a separate demand deposit account or GL account designated for Asset Management department checks. The total amount of checks issued but not yet presented for payment should be reconciled to the balance in this account daily. Exceptions should be identified and resolved or escalated daily.

Asset Position Reconcilement

Asset position reconcilements should be performed at regular intervals by individuals who do not authorize or post asset transactions or direct the movement of securities. Asset Management accounting systems track assets by location and number of shares/units held at the account level and at the department level. In this way, both account- and department-level asset positions at any safekeeping location (depository, custodian, broker, bank etc.) can be determined from Asset Management accounting system reports. Department-level asset positions on the Asset Management accounting system should be reconciled to securities positions per the records provided by safekeeping agents.

Asset Management accounting systems are typically capable of interfacing with or accepting files from the systems of major depositories, such as the Federal Reserve, the DTC, and several large bank sub-custodians. As a result, these systems can produce automated reconciliation and exception reports, position change reports, or other reports to assist Asset Management operations in determining that asset positions are accurately reflected on both the Asset Management accounting system and on the safekeeping agent's records. Operations personnel should review these reports and promptly research, document, and resolve exceptions. Whether automated or manually performed, reconciliations for depositories and third-party custodians should be performed at least monthly and position changes monitored daily.

For book-entry assets, Asset Management operations should verify position changes and reconcile Asset Management accounting system asset positions to issuer statements or reports at appropriately designated intervals, depending upon asset size and activity levels and on the availability of external statements. Internal asset safekeeping locations, such as vaults, should be independently verified at least annually. Management should establish risk-based policies and procedures that indicate how and when each asset safekeeping location is reconciled or otherwise independently verified. Procedures should require escalation of large or aged exceptions to appropriate levels of management.

Suspense Account Reconcilement

Asset Management operations typically sets up and utilizes a number of suspense or house accounts within the Asset Management accounting system to automate and monitor various operational activities, such as dividend and interest payments, asset maturities, securities purchases and sales, corporate actions, and Asset Management fees collected from clients. Operations should maintain a complete list of all suspense/house accounts to ensure that each is properly authorized, reviewed, and reconciled.

The establishment of each suspense account should be authorized by management. The purpose of each suspense/house account should be documented and the types of transactions that are appropriate for the given account defined and documented. An individual who does not authorize or post transactions should be designated to monitor suspense accounts for inappropriate activity. At least monthly, an independent reconciliation of each account should be performed and outstanding items identified by amount, age, and description. Procedures should require appropriate management review, identification and reporting of suspicious activity, and escalation of large or aged items. Any GL or demand deposit suspense accounts used by Asset Management operations should be subject to these same requirements.

Record Keeping and Reporting

Record keeping and reporting are core Asset Management Operations functions. Asset Management operations is responsible for maintaining and retaining account and transaction records in accordance with applicable law, for ensuring that the transaction reporting requirements of 12 CFR 12 and applicable IRS reporting requirements are met, and for ensuring that accurate client statements are produced and appropriately distributed.

Record Keeping and Retention

In addition to maintaining an accurate and reliable accounting system, an Asset Management department needs to create other records to administer its accounts in a timely and cost-effective manner. OCC Regulation 12 CFR 9.8 requires that certain records be maintained for fiduciary accounts and that those records are separate and distinct from other records of the bank. Depending upon established policies, procedures, and workflows, these and other account records reside in either the administrative area or, when imaging systems are in use to store these records, often in operations. It is important to maintain those documents that substantiate fiduciary appointments and actions taken throughout the life of these accounts.

The effectiveness of a bank's records management system may affect both its efficiency and its risk profile. A bank with an effective records management system may be less likely to incur financial losses due to critical missing documents, be better able to defend itself against potential litigation, be less vulnerable to gaps in service as a result of employee turnover, and be better able to respond to audits and inquiries from federal and state tax authorities.

Banks should have policies and procedures that identify the proper retention periods for various records and should ensure that these records are stored, and at the appropriate time disposed of, with an appropriate level of information security. Record retention periods should conform to the requirements of applicable law. For example, OCC Regulation 12 CFR 9.8(b) requires a national bank to retain account records for a period of three years from the later of the termination of the account or the termination of any litigation relating to the account. Longer retention periods may be required by applicable state law. The BSA/AML rules also include record keeping, reporting, and record retention requirements. (See the BSA/AML and OFAC Requirements section later in the booklet and the FFIEC's *Bank Secrecy Act/Anti-Money Laundering Examination Manual*.)

Securities Transaction Reporting—12 CFR 12

OCC Regulation 12 CFR 12 includes minimum record keeping, record retention, and confirmation requirements for securities transactions effected by national banks for customers. It is applicable to both fiduciary and non-fiduciary accounts. The regulation defines the specific information that must be recorded and retained for each affected securities transaction. The regulation also defines specific information about securities transactions that must be provided to customers within designated time frames. There are alternative notification procedures and time frames based on the type of client relationship and the terms of the client agreement. Asset Management operations needs to ensure that internal reports and records of securities transactions comply with the record-keeping and record-retention requirements of OCC Regulation 12 CFR 12 and that, when automated customer confirmation notices are produced by the Asset Management accounting system, accounts are properly coded to produce the proper notice within the required time frame.

Client Statements

In general, all accounts should receive statements that report activity and asset positions at least annually; quarterly or monthly statements are more common. Administrative (front office) staff should not have direct access to client statements prior to mailing because of the potential for fraud. Bank staff, independent of the front office staff, should mail client statements, or this process should be outsourced to a third-party servicer under proper oversight. Changes to client name and address records and statement frequency codes should be properly controlled to prevent improper changes that would prevent a client from receiving statements and detecting unauthorized account activity.

Bank procedures should provide that, under certain circumstances, specific accounts are subject to oversight by a sufficiently independent qualified party or internal control unit. These circumstances include accounts for which clients have requested that the bank hold statements; accounts for which no statement is sent to an external party; accounts that appear to be dormant or abandoned; and accounts for which the only account beneficiaries are minors, persons declared incompetent by a court, or other persons known to lack the capacity to review an account statement.

Some banks offer clients Internet access to their Asset Management accounts. For guidance on developing appropriate safeguards to mitigate the risks associated with Internet banking, refer to OCC Bulletin 2005-35 "Authentication in an Internet Banking Environment" and OCC Bulletin 2006-35 "Authentication in an Internet Banking Environment – Frequently Asked Questions," as well as the "E-Banking" booklet of the FFIEC's *Information Technology Examination Handbook.*

Tax Reporting and Processing

Because there are multiple types of Asset Management accounts and client types, Asset Management accounts may be subject to various IRS information reporting and tax return filing requirements. Depending upon the account type, the client type, and the activity in the account, banks may be required to file reports such as Forms 1099-Int, 1099-Div, 1099-B, 1099-Misc, 1099-OID, 1099R, or 5498. The IRS may fine a bank for failing to file these reports with the IRS or for failing to provide reports to bank clients in an accurate and timely manner. These reports are typically produced by the Asset Management accounting system or by a separate tax system that is receiving data directly from the Asset Management accounting system. Proper coding is needed at the account, asset, and transaction levels to produce accurate reports. A coordinated effort by Asset Management operations, administration, and internal or external tax specialists is needed to ensure timely and accurate production and submission of these IRS reports.

For many accounts, fiduciary, estate, gift, or other tax returns are required. Failure to file or arrange for the filing of accurate and timely tax returns on behalf of fiduciary clients can result in significant penalties and reputation risk. Asset Management accounting systems typically either produce tax ledger reports or transmit data to tax preparation systems that significantly automate the tax preparation process. The accuracy of these reports is dependent upon account-, asset-, and transaction-level coding. Banks need to ensure that fiduciary tax returns are prepared by qualified professionals supported by adequate automation capabilities. Banks that use tax preparation system service providers or other third parties to prepare fiduciary tax returns should implement adequate vendor oversight and management.

Procedures and workflows should ensure that monetary transactions related to fiduciary tax returns, such as estimated tax payments, tax payments due at filing, tax refunds, and retirement plan distribution tax withholding payments, are properly controlled.

Other Processes, Controls, or Regulatory Requirements

This section addresses a number of Asset Management processes, controls or regulatory requirements typically assigned to or supported by Asset Management operations because of the information available through the Asset Management accounting system or the role Asset Management plays in transaction processing.

Cash Accounting and Overdraft Reporting

Depending on the type of account and applicable law, each account's cash balances should be reported on the Asset Management accounting system as a single cash portfolio, segregated between income cash and principal cash, or as segregated among income cash, principal cash, and invested income cash.

Overdrafts exist when the account's combined cash position is negative. In addition, when the governing trust instrument does not permit combining or netting principal and income cash, overdrafts exist when either principal or net income cash is overdrawn. Overdrafts are an extension of credit to the overdrawn account and its beneficiaries and generally should not be permitted in Asset Management accounts. Overdrafts are prohibited in accounts subject to ERISA unless they are exempted under Prohibited Transaction Exemption 80-26 or qualify as an ancillary service under Department of Labor Advisory Opinion 2003-02A. When the grantor or beneficiary of the account is an officer, director, or related entity, the account may be subject to the insider lending restriction and reporting requirements of OCC Regulation 12 CFR 31.2, which requires national bank compliance with Federal Reserve Regulation O. Overdrafts in fiduciary accounts are subject to the insider lending restriction of 12 USC 92a(h), which prohibits a bank from lending to an officer, director, or employee of the bank any funds held in trust.

Overdrafts in custodial accounts may be the result of "free riding" when customers buy and sell securities, usually on the same day, in amounts greatly exceeding the amount allowed under margin collateral requirements. Free riding can expose a bank to credit risk and may violate Federal Reserve Regulation 12 CFR 221, "Credit by Banks and Persons other than Brokers or Dealers for the Purpose of Purchasing or Carrying Margin Stock (Regulation U)." (For further guidance on free riding, refer to OCC Banking Circular – 275.)

Current Asset Management accounting system capabilities, including automated cash management, enable banks to avoid routine daily overdrafts, which may merely be the result of timing differences. Banks should analyze the automated posting schedules for the Asset Management accounting system, the purchase and sale cut-off times for their cash management investment vehicles, and customer and other business requirements to design workflows and processing schedules that minimize overdrafts.

Overdraft reports should be produced at least daily, as of the end of the banking day. Many banks also produce intraday overdraft reports to identify situations in which manual cash management investment vehicle transactions or other funds transfers can clear an overdraft prior to the end of the banking day. Asset Management operations should provide administration and management with reports that include the amount and age of each overdraft. These reports should be reviewed to determine the cause of the overdraft and identify the necessary action to clear it. Policies and procedures should provide for exception escalation based on the age and amount of the overdraft.

Regulation D (Reserve Requirements of Depository Institutions, Federal Reserve Regulation 12 CFR 204) requires banks to maintain reserves on a certain portion of their deposit accounts. Because a bank's omnibus demand deposit account/GL account balance reflects the *net* total of uninvested cash and overdrafts for all of the Asset Management sub-accounts, the aggregate reportable balance for reserve purposes is generally understated. A bank needs to adjust this balance based on the detailed cash balances reflected on the Asset Management accounting system. In addition, negative balances in individual portfolios should not be netted with other portfolios within the account unless permitted by law (either the governing instrument or the applicable state principal and interest law).

Banks should also monitor cash balances in accounts to identify situations when cash balances are not being promptly swept or otherwise invested and should review these situations for compliance with applicable law. With respect to fiduciary accounts for which a bank has investment discretion or discretion over distributions, the bank may not allow funds awaiting investment or distribution to remain uninvested and undistributed any longer than is reasonable for the proper management of the account and consistent with applicable law.

Cash sweep practices should be consistent with the bank's policies and procedures to address the investment of funds held as fiduciary, including short-term investments and the treatment of fiduciary funds awaiting investment or distribution, which banks are required to adopt in accordance with OCC Regulation 12 CFR 9.5(e). To the extent that the bank sweeps fiduciary funds into bank deposit accounts, proprietary funds, or third-party investments for which the bank receives fees or expense reimbursements, the bank's policies, procedures, and practices should reflect the requirements of OCC Regulation 12 CRF 9.12(a) relating to self-dealing and conflicts of interest in the investment of fiduciary funds. Refer to the "Conflicts of Interest" booklet of the *Comptroller's Handbook* and OCC Bulletin 2010-37, "Fiduciary Activities of National Banks: Self-Deposit of Fiduciary Funds" for further guidance.

Pledge Requirements

A national bank may deposit fiduciary funds that are awaiting investment or distribution in the commercial, savings, or other department of the bank, unless prohibited by applicable law. To the extent these funds are not FDIC-insured, the bank must set aside collateral as security, under the control of appropriate fiduciary officers and employees. This pledge requirement under OCC Regulation 12 CFR 9.10 is intended to protect fiduciary funds on deposit at the fiduciary bank in the event the bank fails. A national bank may set aside collateral as security for fiduciary funds awaiting investment or distribution deposited by or with an affiliated insured depository institution, unless prohibited by applicable law.

Eligible collateral is defined in OCC Regulation 12 CFR 9.10(b)(2) and includes, among other acceptable collateral, direct obligations of the United States and securities that qualify as eligible for investment by national banks pursuant to OCC Regulation 12 CFR 1. The market value of the collateral set aside must at all times equal or exceed the amount of the uninsured fiduciary funds awaiting investment or distribution. Pledged collateral is typically held in a depository (usually the Federal Reserve) account specifically designated for this purpose. Asset Management operations is typically responsible for, or provides information that supports, the calculation of the required pledge amount. Asset Management operations or other designated fiduciary officers or employees are responsible for controlling the collateral.

To calculate the total amount of collateral required for its fiduciary accounts, the bank must include the following balances to the extent that they are self-deposited and exceed applicable FDIC insurance coverage:

- aggregate cash balances in fiduciary accounts as reflected on the Asset Management accounting system,[4]
- interest bearing accounts (reflected as assets on the Asset Management accounting system) consisting of fiduciary funds awaiting investment or distribution,[5]
- funds for checks which have been issued on behalf of fiduciary accounts but have not yet been paid, and
- other cash balances in suspense or operating accounts that can be identified as belonging to one or more specific fiduciary accounts.

The bank should adopt and implement procedures to ensure that the required pledge amount is accurately computed; the pledged collateral is eligible under 12 CFR 9.10(b)(2); the collateral has a market value that at all times equals or exceeds the required amount; and the collateral is under the control of appropriate fiduciary officers and employees. Insufficient pledged collateral can result in noncompliance with law and regulation and can place fiduciary client funds at risk. Conversely, pledged collateral significantly in excess of regulatory requirements can adversely affect a bank's liquidity by committing an unnecessary portion of the bank's investment portfolio to secure fiduciary deposits. For further discussion of self-deposited fiduciary funds, see OCC Bulletin 2010-37, "Fiduciary Activities of National Banks: Self-Deposit of Fiduciary Funds."

Nominee Registration

The use of the name of a nominee partnership for securities registration facilitates timely trade settlements and streamlines securities servicing. Most trust agreements authorize a bank to register securities in nominee form. While the vast majority of jurisdictions statutorily authorize the use of nominee registration, prior to using nominee registration, a bank must ensure

---

[4] Aggregate balances should *not* be reduced by the amount of account level overdrafts, or when netting between income and principal portfolios is not permitted, by the amount of portfolio level overdrafts.

[5] See Appendix G of the "Conflicts of Interest" booklet of the *Comptroller's Handbook* for guidance on distinguishing funds awaiting investment or distribution from funds *invested* in deposit accounts.

that applicable law authorizes its use.
Boards of directors typically authorize the execution of a nominee partnership agreement between designated officers or employees of the bank and the bank itself. The partnership agreement establishes a legal name that the bank should register with the appropriate state. The bank's nominee partnership agreement should be updated when a nominee partner is reassigned to another area or no longer employed by the bank.

Consolidated Reports of Income and Condition Schedule RC-T—Fiduciary and Related Services

Information about a bank's fiduciary activity must be reported in Schedule RC-T of the call report, based on the specific standards set forth by the FFIEC as required by 12 USC 161. The call report must be examined and attested to by at least three of the bank's directors.

Many Asset Management accounting systems provide automated reports that assist in the completion of various sections of Schedule RC-T. The accuracy of these reports is dependent upon account- and asset-level coding, accurate asset values, and accurate mapping of account and asset type codes on the Asset Management accounting system to the appropriate call report category.

Appropriate risk-based controls over account and asset coding and asset pricing are necessary to ensure the accuracy of information provided on the call report. System mapping, which assigns account and asset types to specific categories, should be periodically reviewed for accuracy and to ensure that call report data conforms to current instructions for the preparation of the call report, which can be found on the FFIEC Web site. The automated reports produced by the Asset Management accounting system should be reviewed for reasonableness and accuracy before the call report is finalized.

Securities Lending

Securities lending activities of national banks are subject to the requirements of OCC Banking Circular 196, "Securities Lending." This issuance establishes guidelines for securities lending programs, as endorsed by the FFIEC. Securities lending activities of national banks are addressed in the "Custody Services" booklet of the *Comptroller's Handbook*.

BSA/AML and OFAC Requirements

Asset Management is subject to BSA and OFAC requirements. These include the requirements listed below. Some are directly applicable to Asset Management operations and some involve activities for which Asset Management operations may be providing system or record retention support. For more information, refer to the FFIEC's *Bank Secrecy Act/Anti-Money Laundering Examination Manual* and the OFAC Web site.

- **General**

  An Asset Management area or limited purpose trust company must have a BSA/AML compliance program commensurate with its respective BSA/AML risk profile. BSA/AML compliance programs must be written, approved by the board of directors, and noted in the board minutes. Refer to the FFIEC's *Bank Secrecy Act/Anti-Money Laundering Examination Manual* core overview sections, "BSA/AML Compliance Program," and "BSA/AML Risk Assessment," for additional guidance on developing a BSA/AML compliance program and risk assessment, respectively.

  Some institutions incorporate Asset Management, including Asset Management operations, in the bank's overall BSA/AML compliance program. In such cases, Asset Management relationships and customer activities must be integrated into the institution's BSA/AML risk assessment, applicable policies and procedures, reporting and record-keeping processes, and suspicious activity reporting system. For instance, Asset Management relationships and customer activities should be included in the bank's OFAC screening, Customer Identification Program, and suspicious activity monitoring and reporting processes.

  In contrast, some national banks establish separate BSA/AML compliance program structures within Asset Management. In these instances, and in the case of limited purpose trust companies, the institution must ensure that the BSA/AML compliance program covering Asset Management addresses all applicable areas of the BSA and complies with the regulation.

- **Customer Information Program (CIP)**
  Asset Management operations may be supporting systems that access databases used by the front office to verify customer information to assist in compliance with Section 326 of the USA PATRIOT Act or to store documents relating to verification for the required time periods.

- **Suspicious Activity Monitoring**
  Some banks use systems that aggregate customer transactions across business lines to monitor Asset Management accounts for suspicious activity. These systems interface with the Asset Management accounting system, compare actual account activity with anticipated activity, and identify unusual transactions. Potentially suspicious activity is flagged for further review based on variances from anticipated transaction levels and activity type, as well as on the account's risk profile. When such systems are not used, transaction reports should be produced and reviewed to identify and report suspicious activity.

- **OFAC Screening**
  There can be severe sanctions against a bank that conducts business with prohibited countries, organizations, or persons designated by OFAC. To manage this risk and identify transactions that may be prohibited by OFAC, banks typically develop policies and procedures for screening selected transactions (e.g., new customer records, receipts, and disbursements) posted to the Asset Management accounting system against a system or database of prohibited parties and locations. For additional information about OFAC compliance processes and managing OFAC compliance risk, see the FFIEC's *Bank Secrecy Act/Anti-Money Laundering Examination Manual* core overview section, "Office of Foreign Assets Control." A list of current OFAC sanction programs is contained on the OFAC Web site at www.treas.gov/ofac.

- **Information Sharing Between Law Enforcement and Financial Institutions**
  Under Section 314(a) of the USA PATRIOT Act and 31 CFR 103.100 (future 31 CFR 1010.520),[6] "Information sharing between Federal law enforcement agencies and financial institutions," a federal law enforcement agency investigating terrorist activity or money laundering may request that the Financial Crimes Enforcement Network (FinCEN) solicit, on its behalf, certain information from a financial institution or a

[6] Effective March 1, 2011, 31 CFR Part 103 will be moved to 31 CFR Chapter X, and renumbered.

group of financial institutions. FinCEN may then require a financial institution to conduct a one-time search of its records, including Asset Management records, to determine whether it maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization. Section 314(b) of the USA PATRIOT Act addresses information sharing between financial institutions. Banks should have systems or procedures that enable them to search the Asset Management accounting system in response to requests under Section 314(a) or 314(b) of the USA PATRIOT Act. See the Information Sharing section under Regulatory Requirements in the FFIEC's *Bank Secrecy Act/Anti-Money Laundering Examination Manual* for additional information.

- **Funds Transfers**
  31 CFR 103.33 (future 31 CFR 1010.410), "Records to be made and retained by financial institutions," requires each bank involved in a funds transfer of $3,000 or more to collect and retain certain information. The specific information varies based on whether the bank is the originator's (sender's) bank, an intermediary bank, or the beneficiary's (recipient's) bank, whether the originator is an established customer and whether the origination request is made in person. Procedures should exist to collect and retain this information when applicable.

  The "Travel Rule" under 31 CFR 103.33 (future 31 CFR 1010.410) requires that certain information be provided on all funds transfer orders of $3,000 or more at the time the order is sent to the receiving institution. Asset Management operations should be familiar with this rule and should verify that the required information is being provided for requests submitted to its internal or correspondent wire transfer area.

Unclaimed Property Laws

Abandoned or unclaimed property should be reported and remitted to the state in accordance with applicable laws, which vary from state to state. In Asset Management unclaimed property typically consists of: disbursement checks that have not been cashed; bonds and bond coupons that have not been redeemed; items held in certain suspense accounts; unassigned dividend or interest payments; and assets of missing or lost beneficiaries. Banks should have adequate controls over unclaimed property, which is susceptible to a heightened risk of fraud, and they should maintain records that enable them to comply with applicable escheatment and reporting requirements.

Banks should have procedures that identify the abandoned property requirements of applicable state laws, including situations in which the bank is located in a different state than the last known address of the beneficiary. To the extent required by law, operations should identify all abandoned property; prepare and forward required reports of abandoned property to the appropriate states; attempt to contact beneficiaries; and remit abandoned funds to the appropriate state by the date specified. When unclaimed property is associated with an ERISA account, ERISA requirements and the governing instrument should be consulted before a bank makes a determination that the property is escheatable.

Privacy of Consumer Financial Information—12 CFR 40

OCC Regulation 12 CFR 40, "Privacy of Consumer Financial Information," provides for disclosures to consumers of a financial institution's privacy policy and establishes the rights of consumers to direct their financial institution not to share their nonpublic personal information with third parties (opt out), except as specifically permitted by the regulation (such as when a third party is providing services to the bank or to their customers as the bank's agent). Customers must receive this notice annually.

- **Consumers** are individuals or their legal representatives who obtain a financial product or service from a financial institution. Consumers do not include persons who only have designated a financial institution as trustee; are beneficiaries of a bank trust account; or are beneficiaries in an employer-sponsored benefit plan for which the financial institution is trustee or fiduciary.

- **Customers** are consumers with a continuing relationship with a financial institution for financial products primarily used for personal, family, or household purposes (a "customer relationship").

While many fiduciary account grantors and beneficiaries are excluded from the definition of "customer," certain Asset Management accounts may be subject to the privacy policy disclosure and third-party disclosure opt-out provisions of this regulation. The Asset Management accounting system is often used to flag which Asset Management customers should receive the annual privacy notice. In consultation with the bank's compliance staff, Asset Management operations should implement procedures to identify the appropriate recipients of the annual privacy mailing and ensure that these notices are provided. For further information, see OCC Bulletin 2001-26, "Privacy of Consumer Financial Information."

Reports Filed With the SEC

- **Form 13F—Institutional Investment Managers**

  Institutional investment managers who exercise discretion over $100 million or more in "Section 13(f) securities," as defined by SEC Rule 17 CFR 240.13f-1(c), must report their holdings on Form 13F with the SEC.

  In general, an institutional investment manager is: (1) an entity that invests in, or buys and sells, securities for its own account; or (2) a person or an entity that exercises investment discretion over the account of any other person or entity. Institutional investment managers can include investment advisers, banks, insurance companies, broker-dealers, pension funds, and corporations.

  Form 13F requires disclosure of the names of institutional investment managers, the names of the securities they manage and the class of securities, the CUSIP number, the number of shares owned, and the total market value of each security.

- **Schedules 13D and 13G—Beneficial owner of more than 5% of an equity security**

  A bank that acquires "beneficial ownership" directly or indirectly on behalf of a customer of any equity security (defined in SEC Rule 13d-1(i) of the Securities and Exchange Act of 1934, 17 CFR 240.13d-1(i)) greater than 5 percent of the ownership of that class of equity security must, within 10 days after the acquisition, file with the SEC a statement containing the information required by Schedule 13D. A short-form statement can be filed on Schedule 13G, instead of the long-form Schedule 13D, depending on how the person acquired the securities. The Schedule 13G must be filed within 45 days after the end of the calendar year in which the person became obligated to report the customer's beneficial ownership.

Because many Asset Management accounting systems are capable of producing reports that assist in the preparation of Form 13F, Schedule 13D, or Schedule 13G, responsibility for providing these system reports to the investment management or for directly filing these reports with the SEC is often assigned to Asset Management operations. Banks should refer to applicable SEC regulations for specific guidance on preparing and filing these reports.

Notice of Change in Control (Bank Stock and Bank Holding Company Stock)

A bank that, through its fiduciary activities, acquires sole voting authority over 10 percent or more of any class of its own or another bank's outstanding stock must consider the regulatory requirements that may be applicable under the Bank Holding Company Act, 12 USC 1841, *et seq.,* and the Change in Bank Control Act, 12 USC 1817(j).

Federal Reserve Regulation Y, 12 CFR 225, Subpart B, implements the Bank Holding Company Act. The acquisition of voting control of bank or bank holding company securities generally requires an application. However, acquisition of voting securities by a bank or bank holding company in good faith and acting in a fiduciary capacity is generally excluded from this requirement except that

- in the event that the fiduciary has sole discretionary authority to vote the securities, and it retains the securities and the authority to vote the securities for more than two years, the fiduciary must then obtain board approval to hold the securities; or
- in the event that the fiduciary acquires the securities for the benefit of the acquiring bank or other company, or its shareholders, employees, or subsidiaries, the fiduciary must obtain board approval to hold the securities.

The OCC regulation implementing the Change in Bank Control Act, 12 CFR 5.50, exempts from its requirements certain fiduciary acquisitions covered by the Bank Holding Company Act. See 12 CFR 5.50(c)(2)(iv). National bank fiduciaries should examine these regulatory provisions carefully to ensure that the exemption applies to their specific transactions. For further guidance, see the "Change in Bank Control" booklet of the *Comptroller's Licensing Manual.*

Operations and Controls Examination Procedures

The following procedures are intended to assist examiners in determining the adequacy of a bank's policies, procedures, and internal controls for Asset Management operations. They supplement and amplify core assessment procedures found in the "Community Bank Supervision" and "Large Bank Supervision" booklets of the *Comptroller's Handbook*. Examiners should determine which of these procedures to perform during the examination planning process, based on the complexity and risks associated with the bank's Asset Management operations. The decision to use expanded procedures is coordinated with the Asset Management examiner responsible for planning fiduciary examination activities for the applicable bank and must be adequately documented in the work papers.

If the bank provides Asset Management operations through an entity for which the OCC is not the primary functional regulator, the supervisory approach should be discussed with the Asset Management team leader or functional examiner-in-charge (FEIC) for Asset Management and bank examiner-in-charge (EIC or portfolio manager) before commencing any type of examination activity for such an entity. The "Large Bank Supervision," "Asset Management," "Investment Management Services," and "Related Organizations" booklets of the *Comptroller's Handbook* provide OCC supervisory policies relating to functional supervision.

Planning Activities

Objective: To review the quantity of risk and the quality of risk management relating to Asset Management operations and controls to establish the timing, scope, and work plans for the supervisory activity.

1. Consult the following sources of information (if applicable and available) and gain an understanding of previous supervisory risk assessments:
    - Prior reports of examination and management letters covering Asset Management operations, analyses, related board and management responses, and work papers. Include OCC Bank Information Technology reviews.
    - Other applicable regulatory agency reports (e.g., holding company reviews, IT examination reports of technology service providers, Shared Application Software Reviews (SASR).

- OCC files:
  - Supervisory strategy.
  - EIC's scope memorandum.
  - Follow-up activities.
  - Periodic monitoring comments.
  - Risk assessment system ratings.
  - Uniform Interagency Trust Rating System (UITRS) ratings.
- Internal and external audit reports.
- Operational risk management reports.
- Credit risk management reports.
- Compliance reports.
- Any other internal or external information deemed pertinent.

2. Obtain the following from the bank EIC:

   - Relevant MIS reports or other information obtained from the bank as part of the ongoing supervision process.
   - Relevant information obtained from review of applicable board and committee minutes.
   - A list of board and executive or senior management committees that supervise Asset Management operations, including a list of members and meeting schedules; also obtain contact information for the bank employee who maintains copies of minutes.
   - Reports related to Asset Management operations that have been furnished to the bank's Trust Committee, Audit Committee, or any other applicable committee or to the board of directors.

3. Contact bank management to discuss the following, as appropriate:

   - Preference for obtaining the request letter information in secure digital form.
   - Examination's timing.
   - Examination's general scope and objectives.
   - General information about examination staffing levels, examiners' schedules, and projected time during which examiners plan to be at the bank.
   - Availability of key bank personnel during the examination.
   - Any significant changes in policies, procedures, computer systems, third-party service providers or personnel relating to operational activities or processes.

- Any recent or upcoming mergers, divestitures, conversions, or consolidations.
- Material changes in products, volume, or market focus.
- Significant levels and trends of exceptions, fails, and losses for each operational area.
- Results of audit and internal control reviews, any follow-up required by management, and audit staffing (verify that audit scope includes BSA/AML compliance.)
- Structure of the BSA/AML compliance program for Asset Management operations.
- Any material changes to internal or external audit's schedule or scope.
- Effects of new regulatory guidance.

Other issues that may affect the risk profile of Asset Management operations.

2. Determine which of the following lines of businesses, products, or services the bank provides and what, if any, separate systems (automated or manual) support them:

Product	Check if separate system
❑ Personal trust	______
❑ Agency accounts	______
❑ Investment management accounts	______
❑ Separately Managed Accounts	______
❑ Collective Investment or other pooled funds	______
❑ Custody	______
❑ Document Custody	______
❑ Retirement plan services	______
– IRA custody	______
– Participant record keeping	______
❑ Transfer agent (registered or not)	______
❑ Corporate trust	______
❑ Real estate management	______
❑ Farm management	______
❑ Mineral interest management	______
❑ Securities lending	______
❑ Global securities processing	______
❑ Internet access to AM accounts	______
❑ Payments (checks/wires/ACH)	______
❑ Other _____________________	______

Note: The Asset Management examiner should coordinate with personnel skilled in Bank Information Technology to assist in developing the scope and plan for examination of automated systems. When applicable, FFIEC IT examinations of technology service providers should be reviewed.

5. Develop a preliminary risk assessment and discuss it with the Asset Management functional EIC and/or the bank EIC for perspective and examination planning coordination.

6. Using what you have learned from these procedures and from discussions with the Asset Management and/or bank EIC, determine the scope of this examination and its objectives. Decisions concerning the use of expanded procedures should be clearly documented. Determine examination work assignments.

7. Discuss the examination plan with appropriate bank personnel and make suitable arrangements for on-site accommodations and additional information requests.

8. Prepare and send to the bank a request letter that provides the following:

   - Start and anticipated end dates of the examination.
   - Activity's scope and objectives.
   - Advance information the bank must provide to the examination team, including due dates for submission of requested items.
   - Information the bank must have available for examiners upon their arrival at the bank.
   - Name, postal address, e-mail address, and telephone number of the OCC contact.
   - Instructions regarding the delivery of digital files.

Note: Appendix A is a sample request letter for Asset Management operations examinations. The letter should be customized to reflect both the supervisory activity's scope and the bank's risk profile. For other expanded examinations of specialized areas, refer to the appropriate booklets of the *Comptroller's Handbook,* the FFIEC's *Information Technology Examination Handbook,* or the FFIEC's *Bank Secrecy Act/Anti-Money Laundering*

Examination Manual, which include minimum and expanded procedures for this area.

9. Review the requested information that has been provided by the bank and determine its completeness.

Operations and Controls Quantity of Risk

Conclusion: The quantity of risk is (low, moderate, high).

Objective: To determine the types and quantity of risk in Asset Management operations.

1. Identify actual or planned changes in the nature and extent of Asset Management operations activities, including:

   - New products.
   - New markets.
   - Changes in technology.
   - Acquisitions or divestitures.
   - Outsourcing arrangements.
   - Management changes.

2. Evaluate the total volume (dollars and numbers) of transactions processed and the volume and age of exceptions. Consider the following:

   - Volume of transactions settled daily.
   - Percentage of transactions requiring manual intervention.
   - Percentage of transactions that fail (rejects, trade fails, etc.).
   - Volume and age of reconciling items.
   - Daily cash movement.
   - Securities held by depositories or sub-custodians.
   - House accounts (suspense, receivables, taxes, etc.).
   - Number of accounts supported.

3. Obtain the total market value of assets serviced by Asset Management operations. Consider the nature and complexity of the assets serviced and assets with special processing requirements (real estate, notes, mineral interests, derivatives, mortgage-backed securities, private equity, etc.).

4. Evaluate the significance of system and technology risks identified in IT audits, Bank Information Technology examinations, and internal-control reviews.

5. Determine the volume and significance of losses, litigation, and customer complaints.

6. Evaluate the volume and significance of noncompliance and nonconformance with policies and procedures, laws, regulations, and prescribed practices.

7. Assess management's responsiveness to weaknesses or deficiencies identified by control systems or in prior examinations, audits, compliance reviews, or self-assessment reviews.

8. Review the types and volumes of products and transactions that expose the bank to counterparty credit risk to determine the level of credit risk associated with asset management operations. Consider:

   - Impact of contractual settlement of trades and contractual principal and income payment arrangements.
   - Whether bank is using settlement arrangements other than delivery vs. payment.
   - Whether the bank permits large intraday or overnight overdrafts in client accounts.
   - Whether the bank offers indemnification against borrower default or other credit risks when the bank offers securities lending.

Operations and Controls Quality of Risk Management

Conclusion: The quality of risk management is (strong, satisfactory, or weak).

Board and Management Supervision

Objective: To determine whether the board and senior management have provided Asset Management operations with guidance on the organization's strategic direction and established an appropriate organizational structure for Asset Management operational and control activities.

1. Review minutes, resolutions, bylaws, or other documents to determine whether the board of directors or its designated committee has approved and periodically reviewed:

   - Strategic plan, strategic direction, and budgeting process for Asset Management operations.
   - Organizational structure of the Asset Management business, including delegation of the Asset Management operational activities to designated persons or committees.

2. Determine whether operational activities are consistent with the bank's overall mission and strategic goals.

Objective: To determine whether the board and senior management have provided effective oversight of major initiatives, such as mergers, conversions, and new product offerings affecting Asset Management operations.

1. Review regular board and committee minutes, as well as minutes for committees responsible for these initiatives.

Objective: To determine the extent to which the board of directors and management have developed policy guidance that enables the bank to effectively manage risk in Asset Management operations and meet its statutory and regulatory requirements.

1. Determine whether the board has adopted policies for Asset Management that incorporate internal controls, new product approvals, and audit.

2. Determine whether the bank's policies and procedures relating to Asset Management activities are in accordance with applicable law or regulation or OCC guidance. Examples include:

   - 12 CFR 9.5(e)—Policies and procedures, investment of funds held as fiduciary.
   - 12 CFR 9.8—Asset Management record keeping.
   - 12 CFR 9.10(b)—Pledging requirements.
   - 12 CFR 9.13—Custody of fiduciary assets.
   - 12 CFR 12—"Record-keeping and confirmation requirements for securities transactions."
   - 12 CFR 21—"Minimum Security Devices and Procedures, Reports of Suspicious Activities and Bank Secrecy Act Compliance Program."
   - 12 CFR 30, Appendix B—"Interagency Guidelines Establishing Standards for Safeguarding Customer Information."
   - 12 CFR 218, Regulation R—Definition of Terms and Exemptions Relating to the 'Broker Exception' for Banks.
   - 12 CFR 221, Regulation U—Free Riding.
   - 17 CFR 240.17f-1—Lost and stolen securities.
   - 17 CFR 240.14c-2, 17 CFR 240.14c-101, and 17 CFR 240.14b-2—Proxy processing and shareholder communications rules.

3. Determine whether the types and frequency of MIS reports provided to the board and management to oversee Asset Management operations are adequate. Consider the following:

   - Reconcilement exception reports (timeliness, extent to which exceptions are identified, aged, and escalated, and risks associated with any significant exceptions).

- Transaction exception reports (failed trades, missed corporate actions, etc.).
- Reports of counter-party credit exposure resulting from trade settlement and securities servicing.
- Reports that track volumes or measure productivity and efficiency, including reports related to staffing and expenses.
- Compliance exception reports. (BSA/AML, 12 CFR 9.10, 12 CFR 12, etc.)
- Reports of non-credit losses and fee concessions attributable to Asset Management operations errors, oversights, or client service issues.
- Asset pricing exception reports such as variance reports and stale pricing reports.
- Overdraft reports.
- Key Risk Indicator (KRI) and Key Performance Indicator (KPI) reports.

Objective: To determine the adequacy of the board of directors and management's oversight of information technology used by Asset Management operations.

1. Through discussion with management and a review of technology plans, evaluate the bank's strategies for controls and processes. Consider the following:

   - Whether critical applications, data, and service providers are identified and managed effectively.
   - Level of management's knowledge of the bank's Asset Management operations systems and of alternative systems available in the industry.
   - Appropriateness and completeness of management's evaluation of internal controls, security risks, and vulnerabilities.
   - Bank's internal expertise and technical training.
   - Management's knowledge and oversight of system security administration processes.
   - Management's knowledge of and compliance with applicable laws, regulations, and interpretations regarding IT oversight, information security and service provider oversight.
   - Effectiveness of the bank's backup process and contingency planning process as it relates to Asset Management operations.

Objective: To determine the effectiveness of the processes designed to evaluate and manage affiliated and non-affiliated third-party service providers.

1. Identify third-party service providers used by Asset Management operations. Examples include:

   - Asset Management accounting system providers.
   - Service providers performing Asset Management operations.
   - Depositories and third-party custodians.
   - Asset pricing service providers.
   - IRS reporting and tax preparation service providers.

2. Evaluate the bank's risk assessment process for outsourced services. Consider whether:

   - Outsourcing activity is consistent with strategic and business plans.
   - Senior management and the board of directors or a committee of the board are involved in the approval process for outsourcing decisions and servicer selection.

3. Evaluate the bank's due diligence process for gathering and analyzing information on the servicer prior to entering into a contract.

4. Evaluate the bank's contract review process for service providers used by Asset Management operations. Consider whether servicer contracts are reviewed to ensure that:

   - Responsibilities of each party are appropriately identified.
   - Service provider contracts require that servicers implement appropriate measures designed to meet the objectives of the standards of customer information security as set forth in 12 CFR 30—Appendix B.
   - For information technology systems, contracts are written and entered into in a manner consistent with the guidance provided in the "Contract Issues" section of the "Outsourcing Technology Services" booklet of the FFIEC's *Information Technology Examination Handbook*.

5. Determine whether the bank has an adequate process for ongoing evaluation and oversight of service providers used by Asset Management operations. Consider whether the:

   - Vendor oversight program meets the requirements of 12 CFR 30—Appendix B.
   - Servicer performance and service levels are monitored on an ongoing basis and service problems are properly escalated.
   - Bank has an adequate process to ensure that software maintained by the servicer is under a software escrow agreement and that the agreement is confirmed as current; see the "Outsourcing Technology Services" booklet of the FFIEC's *Information Technology Examination Handbook*.
   - Bank has an adequate process to determine when arrangements with affiliated third-party service providers are considered "covered transactions" under Section 23B of the Federal Reserve Act and Regulation W, and that such "covered transactions" comply with the "market terms" requirement of Regulation W.

Objective: To determine the effectiveness of the board and management's oversight of credit risk associated with Asset Management operations.

1. Assess the bank's process for monitoring and limiting credit exposure for client overdrafts.

2. Evaluate how effectively credit risk exposures associated with Asset Management operations are identified by management and considered as part of the bank's overall credit risk management program. For example, has the bank set specific credit limits and how are they monitored?

3. Evaluate the extent to which the bank considers credit risk when considering the use of third-party custodians or safekeeping assets with brokerage firms.

4. Assess whether counterparty credit limits, including daylight overdrafts, pre-settlement, and settlement lines, are appropriate and adequately reviewed by management.

Audit and Internal Controls

Objective: To determine the adequacy and effectiveness of the internal audit of Asset Management operations.

1. When the bank exercises fiduciary powers, determine whether the fiduciary audit committee or the board has arranged a suitable audit, as described in 12 CFR 9.9.

2. In coordination with the EIC, or examiner assigned to review audit at the enterprise level, evaluate audit's review of operational controls and processes within Asset Management operations. Determine how much reliance can be placed on the audit program by validating the adequacy of the audit's scope and effectiveness during each examination cycle. Review audit plans, work papers, and reports. Consider the following:

   - Whether audit scope covers significant activities and controls.
   - Expertise of the auditors.
   - When applicable, effectiveness of oversight over third-party audit resources.
   - Quality of the audit as evidenced by audit work papers and reports.
   - Whether audit scope covers BSA/AML compliance for Asset Management and specific BSA/AML functions within Asset Management operations.

   Note: Adequacy and scope of the audit coverage may affect the level of examiner testing and sampling of control activities. Whenever possible, evaluate the audit early in the examination process. Refer to the "Internal and External Audits" booklet of the *Comptroller's Handbook* for additional procedures.

Objective: To determine the effectiveness of the operational control processes.

1. Discuss with senior management its control process to gain an understanding of:

   - Control culture and structure.
   - Results of any control self-assessment.

- Control placed on high-risk processes (cash movements, asset movements, and corporate actions).
- Availability of any independent tests of the control structure—e.g., audits and/or SAS (Statement on Auditing Standard) 70 or similar reviews.
- Reviews of processes and internal controls performed by internal controls units (e.g. compliance, or risk management).
- Review of Key Risk Indicators.
- MIS processes used to control high-risk activities.
- Adequacy of facilities and records.

2. Review the internal audit findings and evaluate the nature of issues noted and corrective action taken.
3. Review the internal control self-assessment program and any compliance or other internal reviews, if applicable. Evaluate the coverage of the program, the nature of issues noted, and corrective action taken.

4. Review any external audit, SAS 70 or similar control reviews. Evaluate the coverage of the program, the nature of issues noted, and corrective action taken.

5. Determine whether the access control to the various computer systems used by Asset Management operations is adequate. Assess the process for monitoring access control to all systems to evaluate whether the process includes the following:

   - Appropriate approval prior to completion of requests to add or change user access.
   - Proper segregation of security administration function.
   - Timely and independent review of all changes to user access, including production and review of system administrator activity logs or audit trails.
   - Prompt removal of system access for terminated and transferred employees.
   - Appropriate authentication procedures for new password requests and for granting emergency access.
   - Review of system access levels that considers job requirements, appropriate segregation of duties, joint custody or dual control requirements, and appropriate delineation of authority.

- Extent to which system user access controls are used to accomplish the segregation of duties or joint custody or control, and extent to which any system weaknesses or gaps are documented and compensating manual controls are implemented.
- Availability of system user activity logs, audit trails, or similarly detailed reports.

6. Evaluate the bank's reconciliation processes for cash, asset, and other house/suspense accounts for monitoring the accuracy of the accounting controls for its Asset Management activities. Consider the following:

   - Timeliness and adequacy of reporting, aging, and escalation procedures for:
     - Asset Management operations demand deposit account and GL account reconciliations.
     - Reconciliation of Asset Management accounting system asset positions to depository and third-party custodian records.
     - Reconciliation of suspense (house) accounts.
   - Whether reconciliations are performed by individuals who do not have access to process transactions in the accounts that they reconcile.
   - Effectiveness of the bank's escalation and charge-off policy for Asset Management reconcilement exceptions.
   - Appropriate reconciliation or verification processes are in place for all asset locations.

7. Evaluate the bank's control process for house accounts (suspense accounts to handle various operation functions, e.g., sales, income, and purchases). Consider whether:

   - All house accounts have been identified and are being monitored.
   - New house accounts are established only after management approves their stated purpose.
   - House account activity is independently monitored.
   - House accounts are reconciled and reviewed by independent personnel, and aged items have trigger dates for escalation to senior management.

8. Assess the statement processing (printing, accuracy review, and mailing) procedures for adequacy. Determine whether management:

   - Closely monitors accounts that are not set up to receive statements, or for which recipients lack the capacity to review an account statement.
   - Prohibits administrators from mailing account statements to their clients.
   - Establishes appropriate controls over change of name or address and statement frequency fields within each account's records.

9. Review the bank's complaint file and determine whether there are any systemic operational risk issues that have not been properly addressed by management.

Objective: To determine the effectiveness of the processes designed to ensure compliance with applicable laws. Determine whether:

Pledge Requirements

1. Bank has adopted and implemented procedures to determine the amount of securities it is required to pledge for self-deposited fiduciary funds awaiting investment or distribution.

2. Bank has adopted and implemented procedures that require periodic review of the adequacy of collateral pledged.

3. Pledge calculations are accurate.

4. Adequate controls and procedures require that only designated fiduciary department employees are authorized to release securities from pledged status.

SEC Part 240—Regulation 13(d), Securities Ownership

1. Bank filed Form 13D or 13G as required.

SEC Part 240—Regulation 13(f), Institutional Money Managers

1. Bank filed Form 13 F as required.

Free Riding—Regulation U, 12 CFR 221

1. Bank's controls over free riding are appropriate. (Refer to Banking Circular 275, "Free Riding in Custody Accounts.")

Bank Secrecy Act—12 CFR 21.21 and 31 CFR 103 (future 31 CFR Chapter X)

1. An evaluation of Asset Management BSA/AML compliance is required and includes Asset Management operations. Discuss BSA/AML examination scope with the EIC. Refer to the FFIEC's *Bank Secrecy Act/Anti-Money Laundering Examination Manual* for applicable procedures.

Unclaimed Property

1. The process for unclaimed property within Asset Management is appropriate. Consider whether Asset Management operations:

   - Has an effective process identifying and complying with applicable laws for reporting and escheating abandoned property.
   - Has an effective process for aging outstanding checks, suspense account entries, house account entries, and matured bonds and bond coupons.
   - Has a due diligence process to attempt to identify the ownership of unclaimed property in accordance with applicable law.
   - Files reports with and remits abandoned funds to the proper jurisdiction (state).

Overdrafts, Regulation D—12 CFR 204

1. Asset Management overdrafts are monitored and reported to the bank's comptroller to ensure proper reporting under Regulation D for reserve requirements and accurate reporting for call report purposes.

Lost and Stolen Securities—17 CFR 240.17f-1

1. The bank has written procedures to comply with 17 CFR 240.17f-1, which covers lost and stolen securities. Consider whether the bank:

   - Is registered as a direct or indirect inquirer with the Securities Information Center (SIC).

- Has reported any lost or stolen securities to the SIC and followed SIC procedures.
- Makes inquiries to the SIC to determine whether securities received under certain circumstances are lost or stolen.

Other Applicable Laws

1. Through inquiry with senior management, determine whether the bank has a process to determine the laws applicable to Asset Management operations, including those applicable to any specialized products and services offered, and whether the bank has established processes to maintain compliance with them. Consider the following:

   - State and local laws in the United States.
   - Domestic and foreign laws for cross-border activities.
   - Foreign tax regulations and reclaim practices.

2. Through inquiry with senior management, determine whether the bank has an effective process to determine the applicability of new laws and regulations to Asset Management operations and to develop new compliance policies and procedures as appropriate.

Core Asset Management Operations Functions

Objective: To determine the effectiveness of the processes designed to ensure assets are properly safeguarded.

1. Evaluate asset custody and safekeeping processes and controls. Determine whether:

   - Fiduciary assets are placed in joint custody or control of not fewer than two fiduciary officers or employees.
   - Fiduciary account assets are kept separate from bank assets and other fiduciary account assets.
   - Third-party custodian or depository holds fiduciary assets; if so, determine whether such action is:
     - Subject to adequate board and management oversight.
     - Consistent with applicable law.
     - Supported by adequate safeguards and controls. (e.g., joint custody or control over free deliveries).
   - Fiduciary assets physically held by the bank are kept in a properly controlled vault under joint custody or control, under appropriate physical security measures (12 CFR 21), and subject to periodic vault counts.

   For additional guidance, refer to the "Custody Services" booklet of the *Comptroller's Handbook*.

Objective: To determine the effectiveness of the processes designed to ensure effective and efficient servicing of assets held.

1. Evaluate asset set-up and maintenance processes. Consider the following:

   - Use of independent sources and asset models for information on assets.
   - Verification of asset type, income type, and registration codes.
   - Internal-control processes to monitor new asset setup and modifications.

2. Evaluate asset pricing processes. Consider the following:

   - Adequacy of the bank's policies and procedures to determine asset pricing sources, methodologies, and frequency.
   - Adequacy of the bank's disclosure of pricing sources, methodologies, and frequencies to clients.
   - Effectiveness of the bank's processes to identify pricing errors and stale prices and to resolve exceptions.
   - Effectiveness of the bank's oversight of valuations for hard-to-value assets, especially in illiquid markets.

3. Evaluate the income collection process based upon a review of:

   - Methods and services subscribed to that provide information (or forecasts) on income from assets (look closely at assets with irregular payments, such as asset-backed securities).
   - Internal-control processes, including the use of accounting system MAPs of dividends and interest and suspense accounts to monitor and control income payments.
   - Process for aging items in the income suspense accounts. (Review for possible unclaimed property or escheatment issues.)
   - Process for monitoring, verifying, and posting reinvested income.
   - Whether dates on which income is paid to accounts is appropriate for the asset and payment type (i.e., actual vs. contractual payable date, or later dates based on funds availability).
   - Process for managing fixed income premiums and discounts.

4. Evaluate the bank's corporate actions process. For both mandatory and voluntary actions, consider whether:

   - Asset Management operations has access to accurate and timely announcements of stock dividends, stock splits, tender offers, mergers, called debt issues, and other corporate actions.
   - There is an effective process to ensure that, for each new corporate action, critical dates are tracked and monitored to ensure that action is taken in a timely manner.
   - Mandatory actions, such as bond calls, are processed promptly.
   - Appropriate parties are properly notified of voluntary actions and responses are adequately monitored and documented (electronically, in writing, or via voice recording).

- Voluntary responses are properly controlled and compiled, independently verified, and submitted to the issuer within required time frames.
- Systems are in place to block shares from trading if tender offers are accepted.
- Corporate action processing is automated to a degree that is appropriate given the nature and complexity of the bank's activities.

5. Determine whether the process for addressing tax reclaims on foreign securities is appropriate. Consider whether the bank:

- Obtains appropriate IRS determination letters to support employee benefit accounts' tax status.
- Provides its global custodian with appropriate account-level tax status documentation such as forms W-8 or W-9.
- Effectively monitors the reclamation efforts of its global custodian.

Note: If the bank is a global custodian, refer to the "Custody Services" booklet of the *Comptrollers Handbook for Asset Management* for more information about tax reclaims and related examination procedures.

6. Review the bank's procedures for handling class action lawsuits. Assess:

- Adequacy of the bank's class actions policy to address the review of notifications and the determination of when it is appropriate to notify clients or file on their behalf (including notifications received after an account has been closed); notification and filing procedures; monitoring and distribution of proceeds; and fees.
- Adequacy of sources used by the bank to obtain class action information.
- Extent to which the bank appropriately determines for which class actions and accounts a claim is filed.
- Extent to which the bank monitors class actions for which it has filed claims.
- Extent to which the bank properly controls and processes funds received from class action claims.

7. Review proxy voting and shareholder communication procedures. Review the distribution of proxy materials and the disclosure of information about shareholders whose securities are registered in a bank nominee name for compliance with SEC Rules 17 CFR 240.14b-2. Determine whether the bank:

   - Properly determines whether beneficial owners are considered objecting beneficial owners (OBO) or non-objecting beneficial owners (NOBO) under SEC Rule 17 CFR 240.14b-2 for purposes of disclosing their identity to issuers, and properly identifies beneficial owners and disclosure status on the Asset Management accounting system.
   - Either directly, or through third-party service providers, responds to issuers' requests for information in a timely manner and in accordance with disclosure status of the beneficial owners.
   - Either directly, or through third-party service providers, appropriately passes information and materials received from issuers, such as proxy mailings and annual reports, to beneficial owners.

Objective: To determine the effectiveness of processes and controls to ensure efficient and effective securities transaction processing.

1. Detailed trade records are maintained in compliance with 12 CFR 12.

2. Customer trade confirmation notices are sent, or alternate notification arrangements made, as required under 12 CFR 12.

3. Failed trades are promptly identified and effectively addressed.

4. Free deliveries are properly authorized and controlled.

5. Processes are in place to ensure that anticipated assets are either transferred to the bank's depository or sub-custodian account, or a properly controlled book-entry account.

6. Depository position changes are matched to changes on the bank's accounting system.

7. Bank has adequate controls over signature guarantee Medallions.

8. Bank procedures and system access controls provide appropriate segregation of duties and controls over the movement of securities.

Objective: To determine the effectiveness of the processes designed to ensure effective and efficient cash transaction processing.

1. Evaluate adequacy of input controls for entries posted to the Asset Management accounting system.

2. Determine whether there are controls to adequately segregate processing functions, such as posting transactions and making cash entries, from control functions, such as performing reconcilements or reviewing transactions.

3. Evaluate the bank's processes and controls over cash disbursements. Consider whether:

   - Approval and processing functions are appropriately segregated between administration and operations.
   - Controls over unissued checks and check facsimile devices are adequate.
   - Controls over the issuance of checks and the authorization of wire transfer and ACH transactions are adequate.
   - Disbursements are screened to identify any that might be prohibited by OFAC.
   - Wire transfers released by Asset Management operations comply with the BSA "Travel Rule," which requires that specific information is included on certain payment orders.

4. Evaluate the effectiveness of controls over fee processing. Consider the following:

   - Adequacy of procedures to ensure that fee schedules are properly set up and verified on the Asset Management accounting system.
   - Adequacy of procedures to identify fee schedule exceptions.
   - Controls over fee collection suspense/house accounts.
   - Past-due fee receivable exception reporting.

Objective: To determine the effectiveness of the processes used to evaluate and monitor overdrafts.

1. Evaluate the overdraft process. Consider whether:

   - Overdrafts are aged and have appropriate escalation processes based on size and age.
   - Reason for the overdraft is appropriate.
   - Procedures are in place to identify overdrafts that may be subject to Regulation O restrictions due to the relationship of an executive officer, director, or principal shareholder, and any of their related interests, to the account. (Refer to OCC Regulation 12 CFR 31.2 "Insider Lending Restrictions and Reporting Requirements.")
   - Procedures are in place to identify overdrafts that may violate the insider lending provisions of 12 USC 92a(h).
   - Overdraft process addresses free riding. (Refer to OCC Banking Circular 275.)

Objective: Review record keeping for compliance with 12 CFR 9.8, 12 CFR 12, and other applicable law. Determine whether the bank:

- Adequately documents the establishment and termination of each fiduciary account and maintains adequate records.
- Retains fiduciary account records for a period of three years from the termination of the account or the termination of any litigation relating to the account, whichever comes later.
- Maintains fiduciary account records separate and distinct from other records of the bank.
- Maintains minimum trading records (12 CFR 12.3).
- Provides customer notifications that are consistent with 12 CFR 12.4 and 12 CFR 12.5.

Note: Whether some of these records are housed in Asset Management operations or are maintained in the front office vary from bank to bank.

Objective: Given the size and complexity of the bank, determine whether bank management and personnel display acceptable knowledge and technical skills to manage its operational and control activities.

1. Using what you have learned from performing these procedures, evaluate the knowledge, communications, and technical skills of management and staff members. Consider the following:

    - Familiarity with applicable laws and regulations.
    - Familiarity with internal policies and with MIS reports produced for or by Asset Management operations.
    - Education, industry experience, and relevant industry certifications.
    - Familiarity with industry best practices.
    - Familiarity with processing systems used.
    - Involvement in industry working groups and system- and service-provider user groups.

2. Evaluate whether the staff size is sufficient to manage the volume of business conducted. Consider the following:

    - Cash and securities movement trends and volume (both by dollars and item numbers, such as wires in and out, ACH vs. checks, and securities received and withdrawn).
    - Employee overtime records and part-time vs. full-time trends.
    - Employee turnover ratios.
    - Management's plans for automation.
    - Strategic direction.

Operations and Controls Examination Conclusions

Objective: To communicate findings and initiate corrective action when policies, practices, procedures, objectives, or controls are deficient, or when violations of law, rulings, or regulations have been noted in the bank's administration of its operational activities.

1. Provide the EIC with a brief conclusion regarding the following:

    - Quantity of risk and quality of risk management associated with Asset Management operations.
    - Adequacy of risk management systems, including policies, processes, personnel, and control systems.
    - Adequacy of the bank's BSA/AML compliance program, including the policies, procedures, processes, and systems to manage the BSA/AML/OFAC risks associated with trust and Asset Management services.
    - Management's ability to implement effective due diligence, monitoring, and suspicious activity reporting systems used to manage BSA/AML/OFAC risks.
    - Internal control deficiencies or exceptions.
    - Bank conformance with established policies and procedures.
    - Significant violations of laws, rules, or regulations.
    - Corrective action recommended for identified deficiencies.
    - Adequacy of MIS.
    - Overall level of compliance with applicable law, accepted industry standards, and bank policies and procedures, to assist the EIC in determining the compliance rating.
    - Other matters of significance.

2. Assess the impact of Asset Management operations and controls on the bank's aggregate risks and the direction of those risks. Examiners should refer to guidance provided under the OCC's risk assessment program in the *Large Bank Supervision Handbook* or *Community Bank Supervision Handbook*.

    - Risk Categories: Operational, Reputation, Compliance, Credit, and Strategic.
    - Risk Conclusions: High, Moderate, or Low.
    - Risk Direction: Increasing, Stable, or Decreasing.

3. Determine, in consultation with the EIC, whether findings identified in the risk assessment are of enough significance to bring to the board's attention in the report of examination. If so, prepare items for inclusion in "Matters Requiring Attention" section of the report.

4. Determine, in consultation with the EIC, whether there are violations of law to be cited in the report of examination.

5. Discuss findings with bank management, addressing the:

   - Adequacy of risk management systems, including policies, processes, personnel, and control systems.
   - Violations of law, rulings, regulations, or significant internal-control deficiencies, emphasizing their causes and the potential for risks associated with operational activities.
   - Recommended corrective action for deficiencies cited.
   - Bank's commitment to specific actions for correcting deficiencies.

6. Prepare a memorandum or update the work program with any information that facilitates future examinations.

7. Update the OCC's electronic information system.

8. Properly dispose of any records/materials containing personally identified information and appropriately safeguard records that need to be retained.

9. Organize and reference work papers in accordance with OCC guidance. Work papers should clearly and adequately support the conclusions reached.

Operations and Controls — Appendix A

Sample Request Letter

(Date: Month day, year)

(Name)
(Title)
(Bank)
(Address)
(City, State Zip Code)

Dear (Bank Contact):

We plan to conduct a review of (bank department or activity) beginning (date). The review will be conducted at your (location) office and we will need space for (#) examiners. We expect this review to last (#) weeks.

In order for us to prepare effectively for this examination, please provide the information listed in the attachment to this request letter by (date). To protect the confidentiality of this information, all data should be transmitted to us in a secure manner. There are several methods by which this can be accomplished, including encrypted and password-protected media or use of OCC Secure Mail. To the extent possible, please provide the information in digital format. We will work with you to determine the most convenient method to exchange the information in a secure manner. Any hard copy documents that need to be returned at the conclusion of the examination should be marked accordingly. If you have questions about this request, you can contact me at (phone #) or by e-mail (e-mail address).

Sincerely,

Name
Title
cc:

Examination Request Letter Attachment

Examiners need the following information by (date). All information should be as of XXXX (date) unless otherwise indicated. Please provide as much information as possible in an electronic format. Any documents to be returned to management should be so marked.

General Information

1. Current Asset Management operations personnel. Include names, position titles, and phone numbers. Designate primary contact persons with whom we should coordinate examination activities.

2. Resumes of senior Asset Management operations officers hired since the last examination.

3. A copy of the current strategic and/or technology plan that addresses Asset Management operations.

4. List of committees that are involved in the oversight of Asset Management operations. Please include a description of the committee responsibilities and a list of current members.

5. Bank policies and procedures relating to Asset Management operations.

6. A list of major outside service providers used (such as depositories, sub-custodians, corporate action information providers, pricing services, etc.). Include specific DTCC services used such as Fund/SERV or ACATS. Include all automated systems used to perform Asset Management operations functions (in-house and outsourced). List any contractual or oral arrangements with another bank or non-bank firm for Asset Management support services involving operations. When applicable, provide most recent SAS 70 or external audit report for service providers.

7. Policies and procedures related to management oversight of service providers.

8. A list of operational losses of $______ or more for XXXX (current year) and XXXX (previous year). Please include amount and brief description of item; additional explanation will be requested as needed.

9. Current policy regarding operational gains and losses for both ERISA and non-ERISA accounts.

10. Pending or threatened litigation involving Asset Management operations. Include the account names and numbers, plaintiffs, defendants, date action commenced, basis for action, damages asked, bank's argument in defense, current status, and legal counsel's opinion of any probable loss.

11. Describe all instances in XXXX (current year) and XXXX (prior year) in which an officer, director, or employee is believed to have embezzled, misappropriated, or criminally misused fiduciary funds or property.

12. Key operations performance indicators (accuracy tracking to standards) and volume reports.

13. Copy of most recent quarterly and most recent end-of-year Schedule RC-T of the call report, and contact information for individual responsible for preparing the report.

14. Management information reports used to oversee Asset Management operations.

Control Functions

15. A copy of the internal Asset Management operations audit plan and audit program and/or external auditor engagement letter.

16. Copies of internal and external Asset Management operations related audit reports (including SAS 70 or similar reports, if applicable) for the current and previous year. Include management responses reflecting corrective action.

17. Access to internal audit work papers.

18. Copies of Asset Management-related compliance program and risk assessment plan/program for operations, if any.

19. Copies of all Asset Management compliance reports prepared by or applicable to Asset Management operations. Provide a list of any outstanding items.

20. Copies of any other reviews by internal control units (e.g. risk management) with respect to Asset Management operations. Provide a list of any outstanding items.

21. Access to the most recent operations business self-assessment(s). Please provide a list of any outstanding action items.

Systems and Processes

22. A copy of the Trust Accounting system codes list (administrators, portfolio managers, asset types, locations codes, etc.).

23. Security administration procedures for main accounting and depository systems. Include names, phone numbers, and e-mail addresses for security administrators for each system.

24. User access report for Asset Management accounting system and for any systems used by Asset Management operations to access depositories or third-party custodians, initiate wire transfers, or otherwise control the movement of funds or assets.

25. "Free delivery" procedures for depository and sub-custodian asset movement. Also provide the following lists: persons with free delivery capabilities on the depository or sub-custodian's systems; persons with free delivery capabilities on the Asset Management accounting system; and persons who can change location/registration codes.

26. The processes to ensure joint custody or control over money movement (i.e., checks, ACH, and wire transfer).

27. An overview of the workflow for incoming and outgoing wires, highlighting segregation of duties, and authorization/validation of money movements under various scenarios (repetitive/non-repetitive, incoming/outgoing, dollar limit authorizations, etc.).

28. Lists and authorization levels of individuals authorized to sign checks or approve wire transfers.

29. Description of any manual processes used by Asset Management operations to execute or settle trades.

30. A copy of the Asset Management business continuity plan, including operations. Provide the date it was last tested and the results of the test.

31. A copy of major service providers' business continuity plans. Provide the date it was last tested and the results of the test.

32. A list of all asset safekeeping locations, including depositories, third-party custodians and vaults. Describe the process used to reconcile safekeeping records to Asset Management accounting system records, and verify vault assets. Include process for resolving or escalating exceptions.

33. A list of demand deposit, suspense, house, and GL accounts used by the Asset Management division, indicating account name, number, type, and purpose, and name of person responsible for reconciliation.

34. Current demand deposit account, house and suspense account, GL and asset safekeeping reconciliations. List of reconciliation exceptions sorted by age of exception. Include status documentation for items more than 90 days old.

35. Description of the process for reconciliation of demand deposit account, suspense, house, and GL accounts to Asset Management accounting system records. Include process for resolving or escalating exceptions. Include key management reports used to oversee reconciliation process. Describe process for establishing new demand deposit account, suspense, house, or GL accounts.

36. An overview of data applications, procedures, and internal controls for corporate action and class action processing. Address both mandatory and voluntary actions.

37. Describe pricing sources, methodologies, oversight, and client disclosure. Provide reports that track/monitor stale prices and pricing errors.

38. Provide a list of overdrafts greater than $_______, which includes name, amount, and date the overdraft occurred. For any overdraft that has been outstanding more than five days, include account officer name, and a brief explanation of why the overdraft occurred and when and how it will be cleared.

39. Procedures addressing the management of overdrafts.

40. Describe procedures to ensure that appropriate collateral is set aside for self-deposited fiduciary funds awaiting investment or distribution. Provide a copy of most recent analysis, and a current depository or sub-custodian statement listing securities set aside for this purpose.

Operations and Controls References

Laws

12 USC 61, "Shareholders' Voting Rights; Cumulative and Distributive Voting; Preferred Stock; Trust Shares; Proxies, Liability Restrictions; Percentage Requirement Exclusion of Trust Shares."
12 USC 92a, "Trust Powers."
12 USC 161, "Reports to Comptroller of the Currency."
12 USC 371c, "Banking Affiliates."
12 USC 371c-1, "Restrictions on Transactions With Affiliates."
12 USC 1817(j), "Change in Control of Insured Depository Institutions."
12 USC 1842, "Acquisition of Bank Shares or Assets."
15 USC 78a et seq., "Securities and Exchange Act of 1934."
15 USC 80a-1 et seq., "Investment Company Act of 1940."
29 USC 1001 et seq., "Employee Retirement Income Security Act of 1974."
31 USC 5311 et seq., "Bank Secrecy Act."

Regulations

12 CFR 1, "Investment Securities."
12 CFR 3, Appendix C, "Minimum Capital Ratios; Issuance of Directives: Capital Adequacy Guidelines for Banks."
12 CFR 5.50, "Rules, Polices, and Procedures for Corporate Activities: Change in Bank Control; Reporting of Stock Loans."
12 CFR 9.5(e), "Fiduciary Activities of National Banks: Policies and Procedures."
12 CFR 9.8, "Fiduciary Activities of National Banks: Recordkeeping."
12 CFR 9.9, "Fiduciary Activities of National Banks: Audit of Fiduciary Activities."
12 CFR 9.10(b), "Fiduciary Activities of National Banks: Fiduciary Funds Awaiting Investment or Distribution."
12 CFR 9.13, "Fiduciary Activities of National Banks: Custody of Fiduciary Assets."
12 CFR 12, "Recordkeeping and Confirmation Requirements for Security Transactions."
12 CFR 21, "Minimum Security Devices and Procedures, Reports of Suspicious Activities, and Bank Secrecy Act Compliance Program."

12 CFR 30, Appendix A, Section II, "Safety and Soundness Standards: Interagency Guidelines Establishing Standards for Safety and Soundness, Operational and Managerial Standards."
12 CFR 30, Appendix B, "Safety and Soundness Standards: Interagency Guidelines Establishing Standards for Safeguarding Customer Information."
12 CFR 31.2, "Extensions of Credit to Insiders and Transactions With Affiliates: Insider Lending Restrictions and Reporting Requirements."
12 CFR 40, Regulation P, "Privacy of Consumer Financial Information."
12 CFR 204, Regulation D, "Reserve Requirements of Depository Institutions."
12 CFR 215, Regulation O, "Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks."
12 CFR 218, Regulation R, "Exceptions for Banks From the Definition of Broker in the Securities Exchange Act of 1934."
12 CFR 221, Regulation U, "Credit by Banks and Persons Other Than Brokers or Dealers for the Purpose of Purchasing or Carrying Margin Stock."
12 CFR 223, Regulation W, "Transactions Between Member Banks and Their Affiliates."
12 CFR 225, "Subpart B, "Bank Holding Companies and Change in Bank Control: Acquisition of Bank Securities or Assets."
17 CFR 240.13d-1, "General Rules and Regulations, Securities Exchange Act of 1934: Filing of Schedules 13D and 13G."
17 CFR 240.13f-1, "General Rules and Regulations, Securities Exchange Act of 1934: Reporting by institutional investment managers of information with respect to accounts over which they exercise investment discretion."
17 CFR 240.14b-2, "General Rules and Regulations, Securities Exchange Act of 1934: Obligation of banks, associations and other entities that exercise fiduciary powers in connection with the prompt forwarding of certain communications to beneficial owners."
17 CFR 240.14c-7, "General Rules and Regulations, Securities Exchange Act of 1934: Providing copies of material for certain beneficial owners."
17 CFR 240.17Ad-15, "General Rules and Regulations, Securities Exchange Act of 1934: Signature guarantees."
17 CFR 240.17f-1, "General Rules and Regulations, Securities Exchange Act of 1934:Requirements for reporting and inquiry with respect to missing, lost, counterfeit or stolen securities."
17 CFR 450, "Custodial Holdings of Government Securities by Depository Institutions."

26 CFR 1.6045A-1, "Statement of information required in connection with transfers of securities."
29 CFR 2550.412-1, "Rules and Regulations for Fiduciary Responsibility: Temporary bonding requirements."
31 CFR 103.33 (future 31 CFR 1010.410), "Financial Recordkeeping and Reporting of Currency and Foreign Transactions: Records to be made and retained by financial institutions."
31 CFR 103.100 (future 31 CFR 1010.520), "Financial Recordkeeping and Reporting of Currency and Foreign Transactions: Information sharing between Federal law enforcement agencies and financial institutions."

Comptroller's Handbook Booklets

"Asset Management" (December 2000).
"Community Bank Supervision" (January 2010).
"Conflicts of Interest" (June 2000).
"Country Risk Management" (March 2008).
"Custody Services" (January 2002).
"Internal and External Audits" (April 2003).
"Investment Management Services" (August 2001).
"Internal Control" (January 2001).
"Large Bank Supervision" (January 2010).
"Personal Fiduciary Services" (August 2002).
"Related Organizations" (August 2004).
"Retirement Plan Services" (December 2007).

OCC Issuances

OCC Banking Circular 196, "Securities Lending" (May 7, 1985).
OCC Banking Circular 275 "Free Riding in Custody Accounts" (September 3, 1993).
OCC Advisory Letter 2000-9 "Third-Party Risk" (August 29, 2000).
OCC Bulletin 2001-8 "Guidelines Establishing Standards for Safeguarding Customer Information" (February 15, 2001).
OCC Bulletin 2001-26 "Privacy of Consumer Financial Information" (May 25, 2001).
OCC Bulletin 2001-35 "Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information" (July 18, 2001).
OCC Bulletin 2001-47 "Third-Party Relationships: Risk Management Principles" (November 1, 2001).
OCC Bulletin 2002-16 "Bank Use of Foreign-Based Third-Party Service

Providers" (May 15, 2002).

OCC Bulletin 2004-20 "Risk Management of New, Expanded, or Modified Bank Products or Services: Risk Management Process" (May 10, 2004).

OCC Bulletin 2005-35 "Authentication in an Internet Banking Environment" (October 12, 2005).

OCC Bulletin 2005-44 "Small Entity Compliance Guide: Information Security" (December 14, 2005).

OCC Bulletin 2006-35 "Authentication in an Internet Banking Environment: Frequently Asked Questions" (August 15, 2006).

OCC Bulletin 2006-39 "Automated Clearing House Activities: Risk Management Guidance" (September 1, 2006).

OCC Bulletin 2007-42 "Bank Securities Activities: SEC's and Federal Reserve's Final Regulation R" (October 29, 2007).

OCC Bulletin 2008-10 "Fiduciary Activities of National Banks: Annual Reviews of Fiduciary Accounts Pursuant to 12 CFR 9.6(c)" (March 27, 2008).

OCC Bulletin 2010-37 "Fiduciary Activities of National Banks: Self-Deposit of Fiduciary Funds" (September 20, 2010).

U.S. Department of Labor Issuances

Prohibited Transaction Exemption 80-26 "Interest-free Loans (Overdrafts)" (Amended April 7, 2006).

Advisory Option 2003-02A "Overdraft Protection Services" (February 10, 2003).

Field Assistance Bulletin 2008-04 "Guidance Regarding ERISA Fidelity Bonding Requirements" (November 25, 2008).

Department of Labor Interpretive Bulletin 2509.08-2, "Interpretive Bulletin Relating to the Exercise of Shareholder Rights and Written Statements of Investment Policy, Including Proxy Voting Policy" (October 17, 2008)

Federal Financial Institutions Examination Council Issuances

Bank Secrecy Act/Anti-Money Laundering Examination Manual (2010).

"Business Continuity Planning" booklet, *Information Technology Examination Handbook* (March 2008).

"Information Security" booklet, *Information Technology Examination Handbook* (July 2006).

"Management" booklet, *Information Technology Examination Handbook* (June 2004).

"Operations" booklet, *Information Technology Examination Handbook* (July 2004).
"Outsourcing Technology Services" booklet, *Information Technology Examination Handbook* (June 2004).
"Instructions for Preparation of Form 031 and 041" (updated as needed) and "Quarterly Call Report Supplemental Instructions" (updated quarterly).